FÖRSVARSMAKTEN

Handbook
System Safety

2022

Swedish Armed Forces
System Safety Handbook 2022

H SYSTSÄK 2022

VIDAR reference: **FM2021-9449:4**

Decision establishing the System Safety Handbook 2022

The System Safety Handbook (H SystSäk 2022) revision 3 is set to apply from 2022-09-01.

The registered stock number of the publication is M7739-352031.

The following is to be repealed as of 2022-09-01:
M7739-352032 Handbook on System Safety 2011 part 2 - Methods applicable from and including 2012-01-01.

The publication is made available by publishing on the intranet emilia and www.forsvarsmakten.se.

The publication is distributed and stocked at FMCL/FBF.

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 made by Brigadier General Jonas Lotsne. In the final preparation Colonel Joakim Sellén has participated as rapporteur.

Jonas Lotsne
C RPE

Joakim Sellén

M7739-352031 H SYST SÄK E D1

Changes

Version	Change no.	Date when the version starts to apply/must become effective	VIDAR – document no.	Notes
1.0	0	1996-11-01	14 910:72214	Publication Year 1996
2.0	1	2011-01-01	14 910:60224	Publication Year 2011
3.0	2	2022-09-01	FM2021:9449:4	Publication Year 2022

Suggestions for improvements to the System Safety Handbook are to be sent to:
Swedish Armed Forces Headquarters
Materiel production
107 85 STOCKHOLM

e-mail: materielproduktion@mil.se; systemsakerhet.fmv@fmv.se
Write in the subject line: H SYSTSÄK E D1 - Amendment suggestions

Preface

This handbook contains instructions including explanations and descriptions of the Swedish Armed Forces' requirements for system safety activities for fundamental risk management, requirements for technical systems and products as well as the activities, tools and decisions that are part of the Swedish Armed Forces' system safety methodology.

The target group for the handbook is all officials who are involved in the supplying the Swedish Armed Forces with material.

The purpose of the handbook is to contribute to the Swedish Armed Forces' need for safe materiel, related research, technology development and services are met for all levels of readiness.

It is employees at the Swedish Armed Forces and The Swedish Defence Materiel Administration (FMV) who together manage Swedish Armed Forces' materiel from concept to decommissioning. This means that everyone involved in a material acquisition project must ensure that defence equipment is designed and adapted to fit in the Swedish Armed Forces' different environments and that it is safe to use. The handbook must provide natural support for all officials who are involved in supplying the Swedish Armed Forces with material. In addition to the Swedish Armed Forces' perspective, the handbook also outlines the contributions of other actors to the Swedish Armed Forces' system safety activities.

Both the development of defence capabilities and their perpetuation make for a more robust defence system. The materiel component is a load-bearing part in the growth process. Shorter delivery times should be sought and forced procurement may be necessary. In order to succeed in these actions, one aim should be to limit, among other things, the number of special requirements. Systematic requirement work must lay the foundations for a suitable supply of materiel.

The Swedish Armed Forces' system safety work aims to keep the risk of accident in the course of training, exercise, operation, material maintenance, transport, storage holding and disposal as low as possible. This is done through systematic occupational health and safety work to increase the safety awareness of the individual user and by imposing the right system safety requirements on the equipment to be acquired or modified.

The Swedish Armed Forces' system safety work collaborates with several different competence areas, for example environmental work, to protect our external environment. Usability and gender perspective so that the material is designed appropriately for all women and men.

In order to meet the Swedish Armed Forces' requirements for system safety, it is a prerequisite that all actors, within or outside the Swedish Armed Forces, during all of the life cycle stages of the equipment follow the principles described in the System Safety Handbook 2022.

The handbook applies in peacetime and the entire conflict scale.

The content of this publication is not covered by confidentiality.

Reading Guideline

The handbook is partly structured to be read in chapter order, partly divided block wise for the implementation of system safety activities for technical systems and products during all life cycle stages.

For those new to the system safety field, Chapters 1 to 4 and then Chapters 5 to 9 are proposed for study first. For those who are going to start system safety work, Chapter 10 onwards are recommended reading.

The handbook is divided as follows:

Chapters 1-4	Purpose, system safety activities, roles and responsibilities
Chapters 5-9	Legislation, standards, Swedish Armed Forces' regulations and languages
Chapters 10-12	Technical Systems, Route Selection Model, Selection of System Safety Activities
Chapters 13-16	Accident model, risk management methodology and system safety assessment
Chapter 17	Decision-making system
Chapters 18-19	Change (modification) and disposal
Appendix 1	EU law and Swedish legislation
Appendix 2	Standards
Appendix 3	System safety activities

Table of contents

1 Introduction

The purpose of this chapter is to describe the purpose, vision and basis of the system safety activities for technical systems and products that are procured, undergoing change (modification) and used by the Swedish Armed Forces.

1.1 Purpose

System safety activities aim to ensure that the accident risks identified are kept as low as possible throughout the life of the technical system or product. This includes development, use (training, practice and live usage), maintenance, storage, transportation, change (modification) and at the disposal of the materials.

In the first instance, legislation must be complied with without applying exemptions to military materiel. This applies to all levels of conflict. The system safety methodology is used to complement legislation where exemptions for military materiel are granted and justified or where additional safety enhancing measures are required for technical systems and products.

Vision for System Safety Operations

"No person (soldier, sailor, officer or civilian), property or external environment must be inadvertently damaged by Swedish Armed Forces' Technical Systems."

1.2 Background

The Working Group for Ammunition Safety (SAM, 1970-09-28) with representatives from the Swedish Defence Materiel Administration (FMV), the then Swedish Defence Research Institute (FOA) and the Swedish industry in the mid-1970s compiled a handbook based on experiences in the field of munitions, Ammunition Safety Handbook. In the handbook, which has since been progressively developed, there was a special section on safety methodology. In the early 1990s, the Swedish Armed Forces decided that the system safety methodology should be applied to all materiel.

In 1996, the Commander-In-Chief, (ÖB) established the first edition of the System Safety Handbook. The System Safety Handbook 2022 (H SystSäk 2022) is a further development of previous editions (1996 and 2011) and contains the Swedish Armed Forces' guidelines for implementing system safety activities.

This edition of H Systsäk has been prepared to provide better support for system safety activities in the Swedish Armed Forces, and presents a developed model for system safety evaluation, describe roles and responsibilities, and elements of MIL-STD-882E have been incorporated.

1.3 Basics

The main task of the Swedish Armed Forces is to defend Sweden by military means and promote the safety of society. To achieve success in combat requires the use of materiel that can put an opponent out of action. Users who use military materiel must be confident that the materials work in their intended way and do not harm themselves. This also applies to other personnel who handle the equipment in a variety of ways, for example during maintenance or transport.

The Swedish Armed Forces have to manage risks in all activities so that constitutional requirements for occupational health and safety of Swedish Armed Forces' personnel, as well as the requirements for the safety of third persons, property and the external environment are met. The work of the Swedish Armed Forces aims to keep accident risks in all activities as low as possible. This is achieved through a systematic occupational health and safety work to reduce the accident risks of the activities and increase the safety awareness of all personnel and by imposing demands on the equipment used in operations. This means, by extension, that the material must both comply with the legislation and have the necessary characteristics to protect and defend Sweden, but also for the conduct of organised armed combat. System safety activities are an aid so that the Swedish Armed Forces can assume its occupational health and safety responsibilities, as well as to prevent and take responsibility for risks affecting third persons, property and the external environment.

> The Swedish Armed Forces seek to reach society's accepted risk levels for technical systems and products by complying with the legislation with as few exemptions as possible for military materiel.

The Swedish Armed Forces have technical design responsibility for all materiel acquired (new or modified) and is responsible for managing the system safety activities so that the equipment can maintain a satisfactory level of safety throughout its lifespan. Therefore, before entering service, the equipment must have undergone the necessary system safety work and be determined to be sufficiently safe for its intended use and thus correspond to society's accepted safety levels.

The Swedish Armed Forces also have technical design responsibility for technical systems and products that are developed in-house or changed (modified) within their own organisation, for example at Swedish Armed Forces' workshops.

In its role as a support authority to the Swedish Armed Forces, FMV has a responsibility to hand over technical systems and products that comply with the legislation and system safety requirements laid down by the Swedish Armed Forces. The services provided by FMV to support the Swedish Armed Forces must also be quality-assured in order to comply with regulatory and system safety requirements.

The legislation provides for the safety characteristics of different types of equipment (which includes both equipment and consumables), working premises, etc., to be handed over, commissioned and marketed. The legislation can in some cases allow exemptions for military

materiel and military purposes, respectively. Military purposes can mean that the Swedish Armed Forces need different or more stringent system safety requirements for the materiel than the legislation mandates. This can be communicated, for example, through the Swedish Armed Forces' Internal Regulations (FIB), *Design Rules* (DR) or Objective Requirements.

A satisfactory level of safety is the accepted level of risk of society and is achieved by complying with legislation. *Tolerable Risk Level* (TR) is the Swedish Armed Forces' accepted risk level for accident risks that need to be assessed in a risk matrix and where the level of acceptance can be either higher or lower than the satisfactory level of safety.

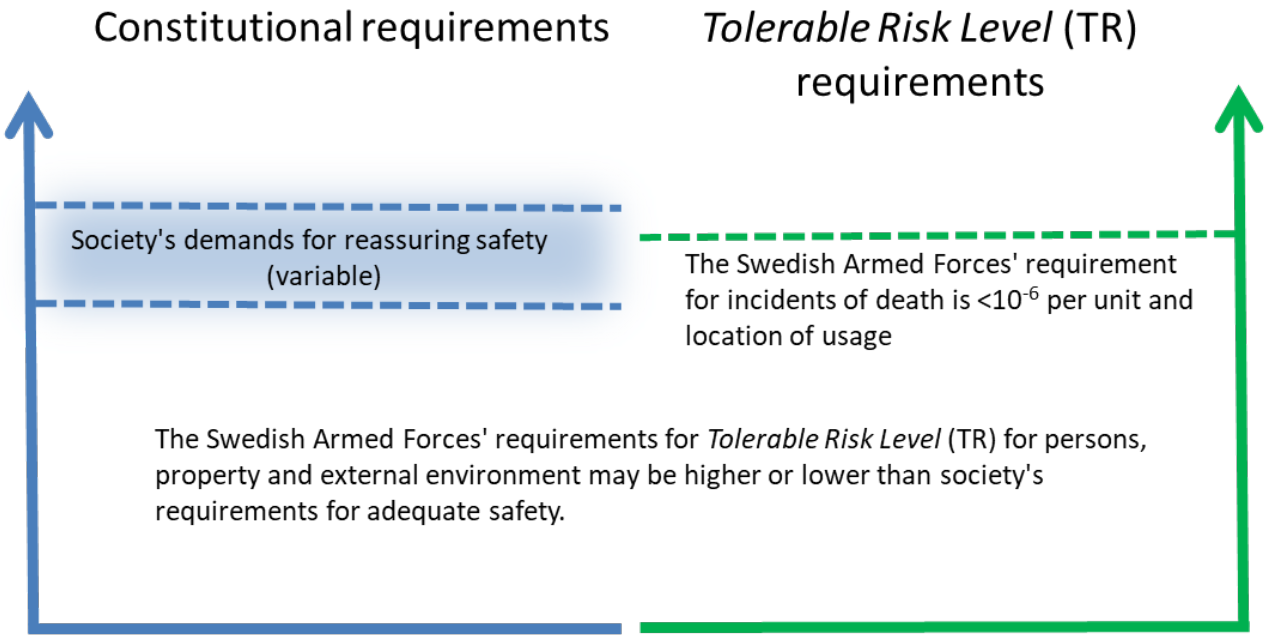


Figure 1.1 Society's demands for satisfactory level of safety may differ from the Swedish Armed Forces' requirements.

The Swedish Armed Forces seek as few exemptions as possible from the legislation for so-called military materiel. Partly for system safety reasons, partly for economic and timeline reasons for procurement.

Typically, the Swedish Armed Forces use technical systems and products integrated or in collaboration with other technical systems that requires additional system safety work to be carried out.

Technical systems often consist of several different products and components. System-of-systems consist of several technical systems, allowing system safety work for the whole to be based on the foundation developed through several different approaches. For example, different technical or system safety standards may have been applied in system safety work for different subsystems. In a statement on the overall safety of a system-of-systems, this needs to be highlighted.

If the system safety work is carried out based on an established system safety standard other than MIL-STD-882E, the system safety work may need to be complemented by, for example, the unique Swedish activities and by a cross-reference list between the different standards.

1.4 Concepts in the Field of System Safety

In the system safety field, the following descriptions of different concepts are used:

- **Operational safety** from a system safety perspective refers to the ability of the Swedish Armed Forces to manage accident risks in all activities so that the constitutional requirements for occupational health and safety of Swedish Armed Forces' personnel, as well as the safety of third persons, property and external environment is fulfilled.
- **System safety** is defined by the Swedish Armed Forces as:

> "The characteristics of a technical system not to inadvertently cause injury or damage to persons, property or the external environment"

Comment: Inadvertently causing personal injury refers to death, physical injury or ill health of one's own staff or a third party. By inadvertently causing property damage implies causing damage to the Swedish Armed Forces' own technical systems and facilities or other people's property such as real estate, vehicles and domestic animals. Inadvertently causing damage to the external environment refers to negative impacts on the environment, such as contaminated water and groundwater bodies or disturbances in the ecosystem. "Accidentally cause" implies an unintentional act.

- **Safety objectives** are the overall focus on the tolerable risk an activity can accept. The safety objectives define the risks to which the organisation and the environment are exposed when the engineering within a function chain is not working as intended. Safety goals are defined based on the most safety-critical functional chains within the respective technical arena (Army, Navy, Aviation, Command and Logistics) that the Swedish Armed Forces need to maintain in order to carry out the missions specified in the Ordinance with instruction to the Swedish Armed Forces.
- **System safety goals** are the objectives a product area or technical system has to fulfil in order to meet a *Tolerable Risk Level* (TR) in order to fulfil its part in a functional chain. The system safety requirements that follow then become dependent on whether the product area is included in a safety objective defined per arena.
- **Technical design responsibility** means that the defined design for permissible configurations of technical systems (including maintenance solutions) meets regulatory requirements, set objectives and other requirements including performance, function, information and system safety across the entire life cycle.
- **Military purposes** from a system safety perspective are military activities that are only permitted to be carried out by the Swedish Armed Forces during exercises and in operational scenarios.
- **Military materiel** from a system safety perspective has been designed and manufactured (also through integration into a system-of-systems) for military

purposes, where regulatory frameworks can allow exemptions or where civil standards are lacking.

Comment: Note that certain regulations allow exemptions for technical systems and products used by the Swedish Armed Forces. In the concept of *military materiel*, similar terms such as *military equipment* and *military product(s)* are included.

- **Military materiel specially designed and manufactured for certain military purposes** from a system safety perspective is when a technical system has been designed and manufactured (also by integration into a system-of-systems) to in its military function (organised armed combat) have a directly destructive effect**.**
- **Satisfactory level of safety** is the accepted level of risk of society and is achieved by complying with legislation.
- **Tolerable risk level (TR)** is the Swedish Armed Forces' accepted risk level for accident risks that need to be assessed in a risk matrix and where the level of acceptance can be either higher or lower than the satisfactory level of safety.

1.5 Application

The purpose of this section is to describe how the handbook will be applied in relation to other regulatory frameworks as well as to other authorities and organisations.

1.5.1 Status of the Handbook

The System Safety Handbook outlines the Swedish Armed Forces' system safety activities, which are to be carried out throughout the entire lifecycle of the materiel.

The handbook contains instructions with explanations and descriptions regarding system safety operations and describes the required administration and management. The handbook relates to EU law, Swedish legislation, standards, Swedish Armed Forces' regulations and other handbooks. The handbook also contains guidelines, processes, procedures, advice and recommendations with images for application, which should always be followed unless there are specific reasons for implementing system safety activities by other means.

The handbook describes roles, methods, and decision-making systems. Furthermore, the application of system safety methodology, activities and tools and how the results can be documented are described. The choice of activities and the documents described in the handbook to be used in the individual case must always be adapted to the current technical system, its function, complexity, use and assessed risk content.

If, in the application of the system safety methodology according to this handbook, there is conflict with EU law, Swedish legislation or other regulatory frameworks for ground, sea or air safety, then these will have precedence.

1.5.2 Inter-agency Application

The System Safety Handbook can be applied voluntarily and mandatorily by directives within an authority. In order for the contents of the handbook to be binding between two or more actors, contracts, agreements or agreements between the parties are required governing the scope of application, mutual liability and commitment, etc.

The Swedish Armed Forces impose demands on the scope of the system safety activities to be carried out together with various authorities. This can be done in coordinating agreements between the Swedish Armed Forces and the respective authorities or directly in an order.

Between the Swedish Armed Forces and FMV there is a Collaboration Agreement (SAMO FM - FMV). This states that FMV complies with the regulations and handbooks laid down by the Swedish Armed Forces in the field of system safety and is responsible for carrying out the corresponding activities at the developing industry and supporting authorities in materiel projects during the phases when FMV is the technical design responsible.

1.5.3 International Application

The development of this handbook has taken account of EU law and established standards used internationally, which is why the handbook is deemed to be applicable in its entirety even to international cooperation and procurement. When development assignments are placed with a foreign supplier (industry or state), system safety activities must be agreed and carried out according to the same level as for industries in Sweden.

2 The Swedish Armed Forces' Management of System Safety

The purpose of this chapter is to describe the Swedish Armed Forces' management of system safety activities so that technical systems and products can achieve and maintain a satisfactory level of safety over time. Furthermore, related areas are described and how these can affect the implementation of system safety work.

System Safety
"The characteristics of a technical system not to inadvertently cause injury or damage to persons, property or the external environment"

2.1 Safety Culture and Risk Awareness

The main task of the Swedish Armed Forces is to defend Sweden against an armed attack and thus assert Sweden's territorial integrity. The Swedish Armed Forces must be able to carry out their tasks independently or in collaboration with other authorities, states and organisations. The Swedish Armed Forces must, with the existing capabilities and resources of authorities and agencies, be able to promote the safety of society in the event of severe stress.

The Swedish Armed Forces conduct training and exercises, and in order to achieve success during live operations, the use of materiel that can contain large amounts of energy is required to put an opponent out of action. Users must have confidence that the materiel does not harm themselves. This also applies to other personnel who handle the materiel in a variety of ways, for example during maintenance or transport.

The Swedish Armed Forces are responsible for operational safety, where parts of it are linked to system safety activities. Operational safety refers to the Swedish Armed Forces' ability to manage risks in all operations so that constitutional requirements for the work environment and safety of the Swedish Armed Forces' personnel are met, and that requirements for safety for third persons, property and the external environment are taken into account. For this purpose, there are safety objectives and the concept of tolerable risk in order to be able to make appropriate trade-offs before different interventions. Operational safety work includes rulemaking, implementation of activities according to set regulations, and follow-up of this.

The Safety Management of Swedish Armed Forces is defined as all measures implemented by various organisational units, which aim to raise the safety culture and risk awareness of the organisation. Safety management must define, among other things, policies, the organisation's powers and resources, working methods, requirements definition, training, accident prevention, accident and incident reporting, follow-up and corrective actions, and supervision and inspection.

Society's concept *of safety culture* is defined as the collection of characteristics and attitudes in the organisation and in individuals that ensure that safety issues receive the attention needed. The organisation with its employees constantly strives for as high safety as possible.

The Swedish Armed Forces use the concept of *risk awareness*. A high level of risk awareness is a prerequisite for compliance with the Swedish Armed Forces' safety management, while at the same time responsible application can raise risk awareness within the organisation. For a high-risk awareness to develop, an atmosphere is required in which individuals are not punished or accused, or threatened with it, for their unintentional mistakes. However, an individual guilty of sabotage or deliberate negligence should of course not be released from the individual's responsibility.

A high level of risk awareness is characterised by the positive commitment and participation of the staff concerned. Only through good risk awareness are there conditions for continuous improvement in order to effectively take care of the accident risks identified during the implementation of the operation, and remedy these even before they cause accidents, incidents or deviations. A crucial success factor is to learn from accidents, incidents and mistakes, instead of demanding accountability.

As an example, the Swedish Armed Forces' aviation safety work was internationally recognised for its safety culture by focusing on openness, transparency and learning instead of primarily demanding accountability in the event of accidents, incidents and mistakes.

2.2 System Safety Activities

The goal of system safety activities is to strive to achieve the Swedish Armed Forces' vision for system safety. System safety activities are used to ensure, within the framework of legislation, that technical systems and products offer a satisfactory level of safety. The system safety methodology is used to complement legislation where exemptions for military materiel are granted and justified or where additional safety enhancing measures are required for technical systems and products.

The activities of the Swedish Armed Forces include personnel, technical systems and organisation. In civil terms, this is usually referred to as Human, Technology and Organisation (HTO). Accident risks exist if deficiencies exist within or in the interaction between these areas. Systematic system safety work for technical systems can eliminate or minimise these accident risks.

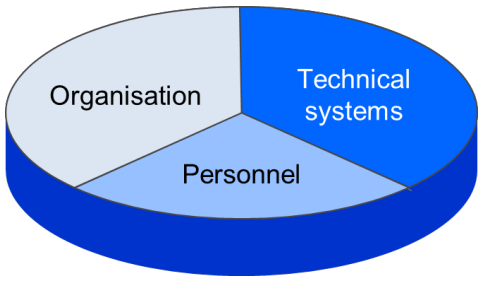


Figure 2.1 *The operational safety of the Swedish Armed Forces includes organisation, personnel as well as technical systems and products.*

The Swedish Armed Forces' system safety activities include methodology for achieving and maintaining the satisfactory level of safety of technical systems and products and their use in unit operations.

Based on the needs of the operations and previous experience of similar technical systems, the Swedish Armed Forces must formulate system safety requirements for new or changed (modified) technical systems, or for a change of field of use. The clearer and more precise the requirements placed on the intended use; the more comprehensive system safety work the supplier can implement. If the intended use is not specified or is vaguely described, the supplier's system safety work will mainly be based on the use that the supplier assumes the system will be subjected to and the Swedish Armed Forces will then need to carry out more extensive operational safety work linked to the use before the system can be put into use.

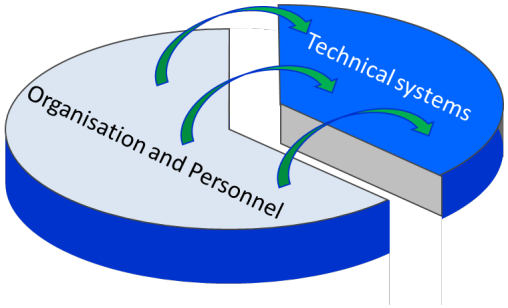


Figure 2.2 *Requirements for technical systems and system safety work from the organisation and personnel.*

The supplier's system safety work will never be more comprehensive than that described in various targeting documents. What has not been described can ultimately create restrictions that restrict the Swedish Armed Forces' intended use. The Swedish Armed Forces will have to manage residual accident risks through operational rules before systems can be put into service. When technical systems and products fail, it is the organisation and staff who have to compensate for these shortcomings within the framework of operational safety.

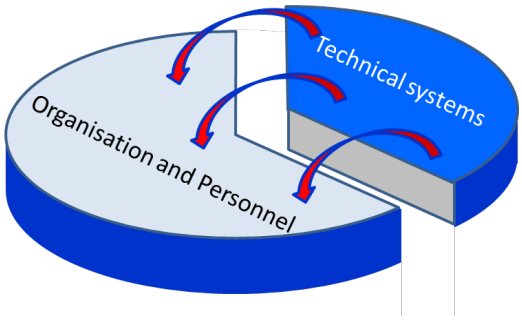


Figure 2.3 *The Swedish Armed Forces will have to manage the remaining accident risks of technical systems and products through operational rules.*

Safety targets provide general requirements regarding what tolerable risks an operation can accept. The safety objectives define the risks to which the organisation and the environment are exposed when the engineering within a function chain is not working as intended. Safety objectives are defined on the basis of the most safety-critical functional chains within each technical arena (army, navy, aviation, command and logistics) that the Swedish Armed Forces need to maintain. Based on the safety objectives, specific system safety objectives for a particular product area can be developed and specified in *the System Safety Management Plan* (SSMP). For technical systems and products, system safety requirements are set in the

current *System Objective* (SMS). These system safety objectives and requirements are then translated into a *Request for Proposal* (RFP).

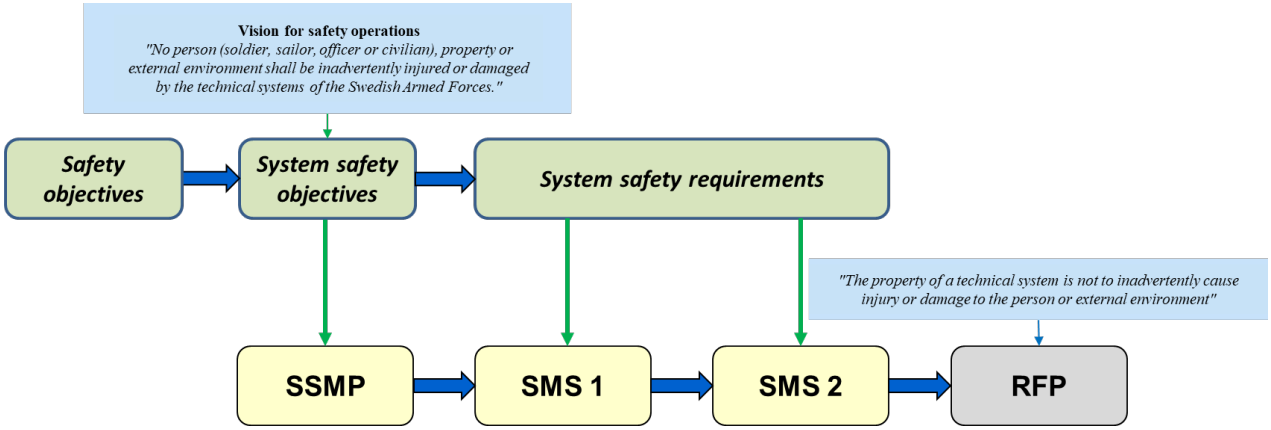


Figure 2.4 From safety targets to broken down requirements in Request for Proposal (RFP).

2.3 System Safety Work, Requirements and Decision Systems

The Swedish Armed Forces apply a requirements and decision-making system for technical systems and products. All actors in their different roles participate in different ways in the system safety work with new or changed (modified) technical systems and products. In the joint system safety work, the aim is to ensure that the remaining accident risks are few in number and tolerable.

Through a good safety culture and risk awareness within the Swedish Armed Forces, there are experiences that can be used in goal-setting work to make future technical systems even safer to use, maintain, store, transport and disposal.

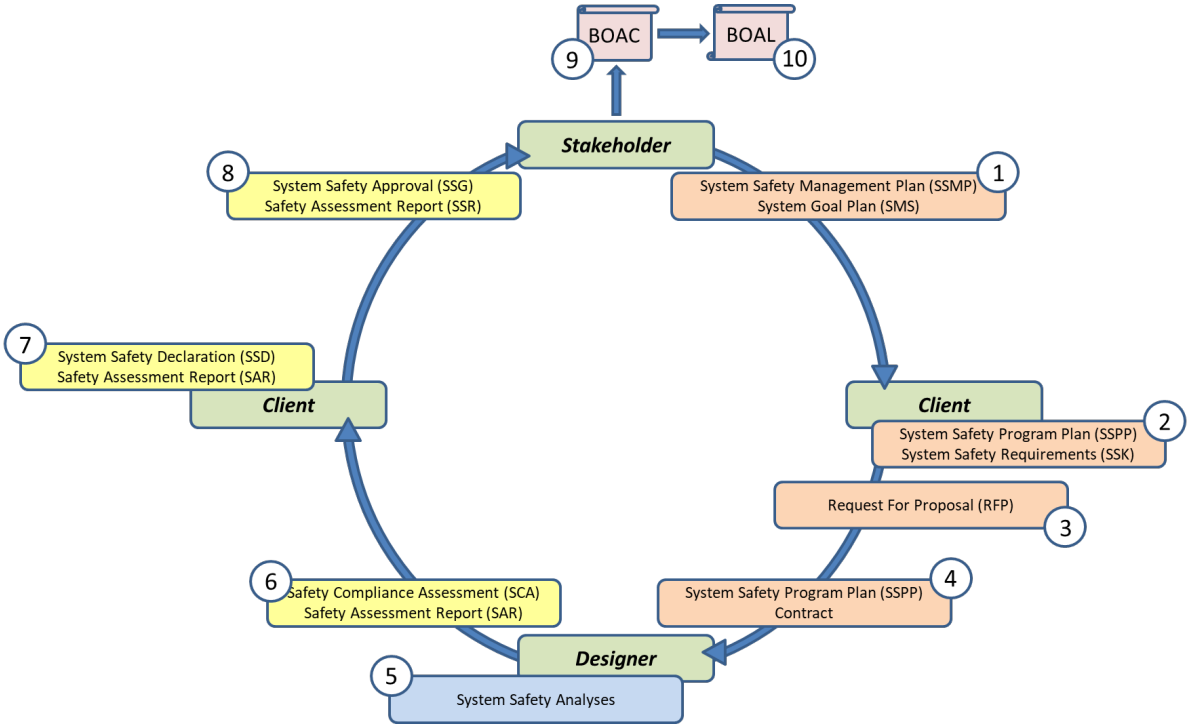


Figure 2.5 *The Swedish Armed Forces apply a requirements and decision-making system for technical systems and products.*

Below are explained the various points of the figure above.

1) The Swedish Armed Forces, in their role as *stakeholder* prepare a *System Safety Management Plan* (SSMP) for a product area and the required number of *System Objective* (SMS) for various technical systems and products. System safety requirements must be defined in the *System Objective* (SMS).
2) The Swedish Armed Forces or FMV in the role of *client* write a *System Safety Program Plan* (SSPP) for the system safety work that they need to carry out. Furthermore, System Safety Requirements (SSK) are implemented in order to identify EU law, Swedish legislation, standards, other regulations, *Design Rules* (DR) and design requirements.
3) Based on *System Safety Requirements* (SSK), technical requirements and business commitment requirements are formulated, which are distributed to different *Requests for Proposal* (RFPs).
4) The Swedish Armed Forces or industry in the role of *designer* receive a contract (or equivalent) and create a *System Safety Program Plan* (SSPP) as part of the agreement.
5) The *designer* carries out system safety work and the *client* continuously *monitors the designer's* system safety work.
6) The *designer* issues a *Safety Compliance Assessment* (SCA) with the required risk documentation, such as *Safety Assessment Report* (SAR) and *Risk Log* (RL).
7) The *client* reviews the *designer's Safety Compliance Assessment* (SCA). Thereafter, a *System Safety Declaration* (SSD) is issued with the required risk documentation, such as *Safety Assessment Report* (SAR) and *Risk Log* (RL).

8) The *stakeholder* reviews the *client's System Safety Declaration* (SSD). Thereafter, a *System Safety Approval* (SSG) is issued with the required risk documentation.
9) The *stakeholder's System Safety Approval* (SSG) is included in the decision gate *Decision on Use, Central Level* (BOAC) and after this decision, the technical system or product can be put into use at a central level.
10) *Head of Organisational Unit (*C OrgE*)* makes, if necessary, *Decisions on Use, Local Level* (BOAL) and the technical system or product can thus be put into service at the local level.

2.4 System Safety Work, Technical Systems and Products

System safety work for technical systems or products aims to identify, analyse, evaluate, classify and reduce the risk of identified accident risks. These accident risks may initially be diffuse, but through structured system safety work at the various actors, the accident risks are clarified and risk reduction measures can be taken.

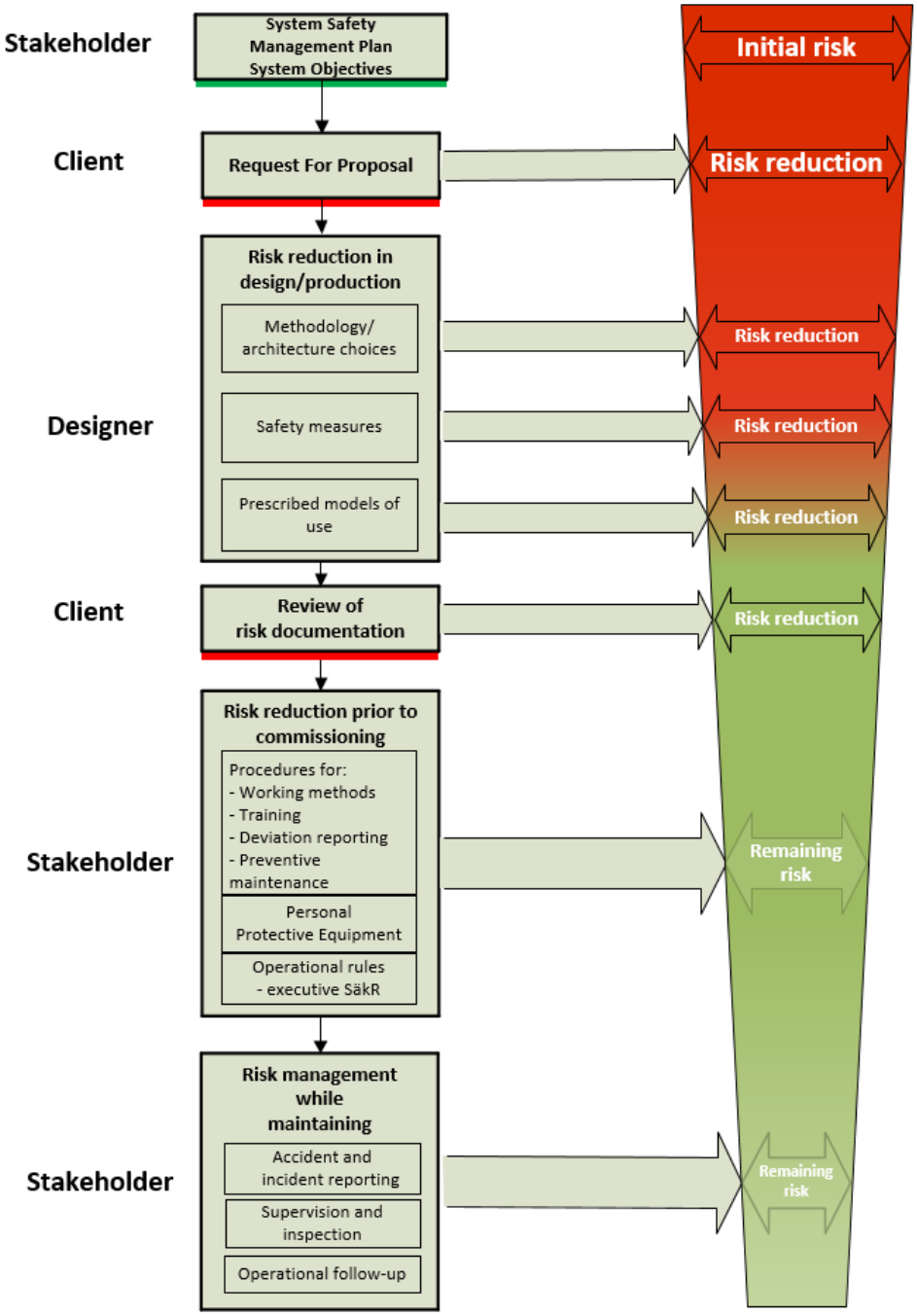


Figure 2.6 *The contribution of various actors in the work on risk elimination, risk reduction and management of residual accident risks.*

The Swedish Armed Forces' existing and future technical systems and products are included in various *System Safety Management Plans* (SSMP) at product area level. These include requirements for system safety activities, system safety objectives for a satisfactory level of safety based on EU law/Swedish legislation, and *Tolerable Risk Level* (TR) expressed in risk matrices for persons, property and the degree of negative impact on the external environment.

The *System Objective* (SMS) refers to the current *System Safety Management Plan* (SSMP). The *System Objective* (SMS) sets requirements for system safety work as well as specific system safety requirements for the technical system in question.

The system safety requirements in *the System Objective* (SMS) are realised into one or more different *Requests for Proposal* (RFP). *Requests for Proposal* (RFP) contain measurable requirements for the technical system, its intended use, as well as for expected system safety work and system safety documentation. Furthermore, requirements for satisfactory level of safety and *Tolerable Risk Level* (TR) are required as measures of acceptance level for any remaining accident risks.

The *designer's* choice of architecture, system solutions and sources of risk dimension the risk content of the technical system. Unfortunate or ill-considered choices can rarely be compensated for by various types of protective measures or prescribed modes of use. The *designer* advantageously uses different types of standards and *Design Rules* (DR) as these describe safe design principles.

Before the Swedish Armed Forces are to put new or changed (modified) technical systems into use, careful consideration needs to be given to the remaining accident risks. This means that any such risk of accidents by its nature must be known, rectified if necessary and that acceptance decisions have been made. The remaining accident risks can also be handled through operational rules.

Operational rules may include, for example, restrictions on use, requirements for the training of instructors and users, and edicts on the use of Personal Protective Equipment (PPE). When using technical systems in peacetime, special restrictions may apply during training and exercise. At higher levels of preparedness, restrictions may be affected.

The number of known accident risks in a technical system is not static but may increase or decrease over time. The increase may be due to the addition of new modes of use, the detection of materiel or production defects, the ageing or wear of the equipment in an unexpected manner, or incorrect or inadequate maintenance. The increase may also be due to changes in training, changes in modes of use (slippage of norms), both people and organisations become less vigilant or more home-blind over time, especially if no accidents or incidents have occurred for a long time. Reduction can for example be the result of safety deficiencies in the materiel being managed through changes (modification).

By working preventively with continuous improvements, accidents can be prevented. In all activities, deviations from planned implementation inevitably arise, such as deliberate or unintentional deviations from given rules, variation in user behaviour and changes from the expected performance of the materiel. In order to prevent and ensure that a satisfactory level of safety is maintained, the Swedish Armed Forces systematically collect information during the maintenance phase from use and maintenance. The information may consist of accident and incident reports, signals of changes in use (slippage of norms), fault outcomes, performance deficiencies or technical status surveys. Information can also be obtained through supervision and inspection. The system safety aspects from the collected data are evaluated and facts that are of importance for system safety are analysed so that correct measures can be taken in operations, through change (modification) of technical systems or in its use.

2.5 Areas Adjacent to System Safety

System safety has common interests with other areas of activity. Below is a description of some related areas that are not normally covered by the system safety methodology. Information created through system safety work, or by another related area, can therefore be transferred and put to use within or between other areas of activity.

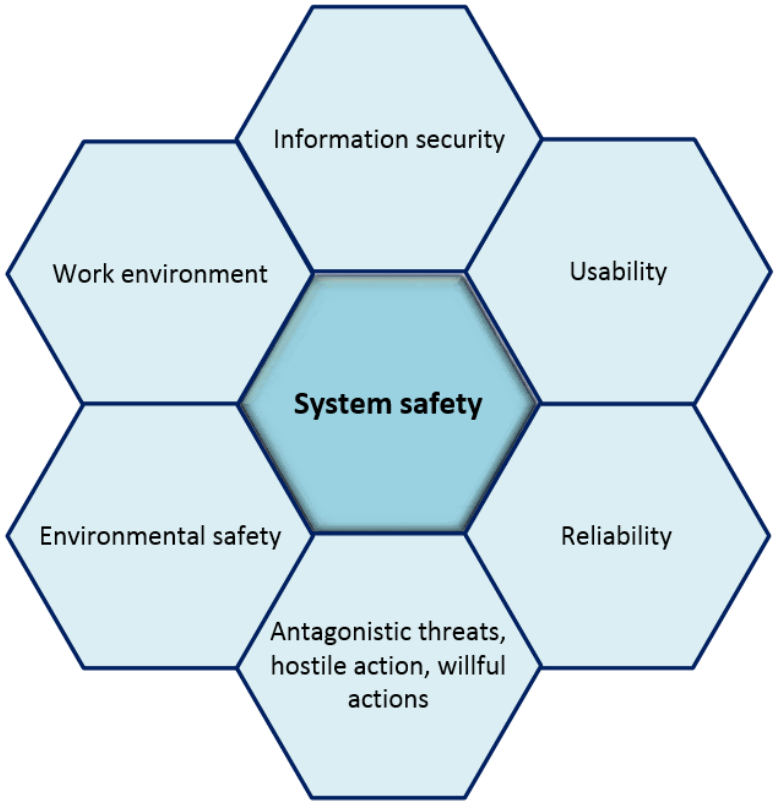


Figure 2.7 Examples of adjacent and sometimes overlapping areas to system safety.

2.5.1 Information Security

Information security refers to the protection of information assets so that the information is accurate and accessible only to the persons, systems or processes for which it is intended. The aim is to protect these assets against undesirable events such as physical or digital (cyber) intrusions. Protection may consist of technical safety and/or administrative safety. Based on the nature of the operations, some of these assets may be more worthy of protection and that the protection value of information may vary over time. From an information security perspective, the information must be:

- Correct
- Protected (against unauthorized access)
- Available (for those who at a certain point in time need the information)
- Traceable

If the protection of the information access is lacking so that it becomes inaccessible, inaccurate (corrupt) or spread to unauthorised persons (foreign powers), this can also affect system safety and lead to consequences in the operations for personnel, materiel and

facilities. A technical system can never offer a satisfactory level of safety unless information security is taken care of.

2.5.2 Usability

Usability refers to the degree to which a user can use a system in a given context to achieve specific objectives effectively, efficiently and satisfactorily for the user. Most technical and non-technical systems will in different ways communicate with users and maintenance personnel. If humans can increase or decrease their ability in this interaction, it has a bearing on ensuring that systems are perceived as secure, safe and useful.

Interaction design is about shaping systems, services and environments with a particular focus on their user qualities, that is, how they should be to use. When designing user interfaces, knowledge of human conditions and abilities is therefore required, but also knowledge of the physical and mental limitations of the human being as a user and as part of the system is required. Insight into how psychological, physiological, organisational and technical aspects interact in complex and stressful environments, creates conditions for achieving safe and useful systems.

If usability is lacking, for example through an excessively complex volume of information, recurrent false alarms, illogical controls or the choice of colour, this can also affect system safety and lead to consequences in operations for personnel, materiel, the environment and facilities.

2.5.3 Work Environment

The work environment refers to both the physical and the psychosocial work environment. The work environment includes biological, medical, physiological, psychological, social and technical factors that affect the user in the operation or in the workplace environment. When developing technical systems and products, it is the physical work environment that the user can make demands on, because there are detailed rules and measurable limit values for how our physical work environment should be designed.

Ergonomics is about adapting work and the environment to human needs and conditions. It can often concern how the workplace and the work environment should look purely from a technical point of view so as not to cause injuries or ill health. Examples of things to observe are posture, working position, working height, sound, light, ventilation, radiation and climate, but also that the body is used in a proper way, for example by pushing, pulling, lifting or carrying.

A good and healthy work environment increases the combat value of the user and does not have an acute or, in the long term, a negative impact on health. Long-term health impacts are managed through restrictions specified in the legislation and with the support of methods in the work environment area.

2.5.4 Reliability

Reliability refers to the ability of a system to perform a required function under given conditions in a certain time interval. Reliability at one system level can imply system safety

at another system level. Malfunctions can be both a contributing cause or a trigger for an accident to occur.

Reliability is a subset of operational availability and one way to measure it is through failure intensity. The intensity of error, as a function of time, can be decreasing, constant, or increasing.

If the components concerned that are to deliver their function do not have the correct reliability, accidents and incidents may occur. However, it is important to distinguish between system failures that have an impact on safety and system failures that affect or limit function and performance. The latter, by extension, as a consequence of insufficient functioning or performance, can cause damage to person, property or external environment. However, these are handled as a performance or quality issue.

Reliability can be maintained through preventive maintenance and/or early replacement of safety-critical components or by change (modification) of the technical system.

2.5.5 Environmental Safety

Environmental safety linked to technical systems refers to the management of aspects that have a negative impact on the external environment. The environmental work takes care of, for example, emissions and noise from a technical system during normal operation and which constitute a burden on the external environment. Emissions can be, for example, hazardous substances, air particles, light or radiation.

System safety work includes identifying and managing potential accident risks, i.e. individual accidental events that deviate from normal operation and that can have both long- and short-term environmental and health effects. Possible causes of accidents or incidents are investigated and possible consequences are reported within the framework of system safety work. Examples of such events may be tanker leaks or loss of noise protection. However, the actual environmental impact that is conditioned by the current physical location falls outside the scope of system safety work and is managed through restrictions specified in the legislation and with the support of other methods in the environmental field.

Results from system safety analyses such as measured noise or emissions can also be used in environmental work, for example when applying for a concession for activities subject to a permit.

2.5.6 Antagonistic Threats, Hostile Action, and Wilful Acts

Hostile weapons refer to the use of military means directly directed by a foreign power directly against a unit's assets worthy of protection, such as personnel, materiel and facilities. System safety operations do not deal with damage caused by hostile weapon action against their own technical systems or personnel. The exception is technical systems for ammunition or mine clearance in international operations and Swedish national ammunition clearance in peace. Accident risks arising from such sources of risk are disposed of within the framework of system safety work, since the main task of the technical system is to clear ammunition or mines.

Antagonistic threats refer to attacks without conventional weapons, but directed against a unit's information assets worthy of protection, for example through cyber-attacks. System safety operations do not deal with damage caused by hostile weapon action against their own technical systems or personnel.

System safety activities also do not include deliberate sabotage or intentional acts by own personnel in order to harm own personnel or deliberately destroy technical systems and products.

3 System Safety Activities in the Life Cycle

The purpose of this chapter is to describe the Swedish Armed Forces' life cycle model for technical systems and products from a system safety perspective.

3.1 Research and Technology Development

Research and Technology Development (R&TD) activities mean the work that is carried out before a technical system is to be realised.

Research and Technology Development (R&TD) activities are usually governed by the Swedish Armed Forces' future need for new capabilities to meet future military threats. The purpose of the work is partly to develop new cross-platform technology, partly to analyse what opportunities and threats may arise from new technology, and partly to identify new areas of application for already known technology. The goal of the system safety work within the Research and Technology Development (R&TD) business is to acquire sufficient knowledge about different technologies and their potential uses, for a *System Safety Evaluation* (SSB) of different alternatives to be possible to carry out.

3.2 The Swedish Armed Forces' Life Cycle Model

The Swedish Armed Forces' life cycle and decision model for technical systems and products is based on the ISO/IEC/IEEE 15288 standard, *Systems and software engineering - System life cycle processes*.

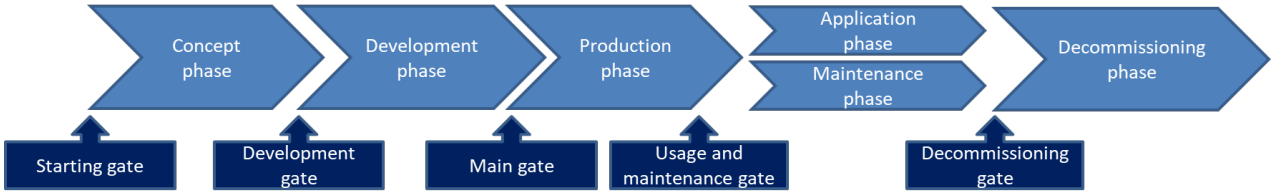


*Figure **Error! Reference source not found.Error! Reference source not found.Error! Reference source not found.**.1 The Swedish Armed Forces' life cycle model with decision gates.*

The Swedish Armed Forces' use of the life cycle model and associated decision gates are primarily described in the materiel production process. The *Collaboration Agreement (SAMO FM - FMV)* uses both stages and phases, which are italicised below. Stages are used to describe the life cycle of a technical system and phases derive from the Government's investment planning directives. In order to describe what system safety work needs to be carried out within the framework of the different life cycle stages, the term "work" is used instead.

- Concept work *(Concept stage, Concept phase)*
- Development work *(Development stage)*
  - Preparatory work *(Preparatory phase)*
  - Procurement work *(Procurement phase)*
- Production work including work for BOAC/BOAL *(Production stage)*
- Maintenance work *(Maintenance stage, Use stage/Maintenance stage)*
- Decommissioning work *(Decommissioning stage)*

The figure below shows system safety work in relation to the Swedish Armed Forces' decision gates. In order to move a technical system or product between life cycle stages, necessary system safety documentation is required, among other things.

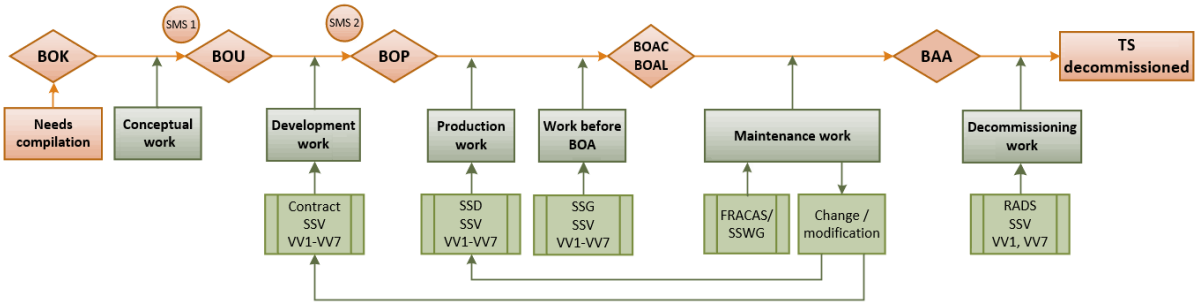


*Figure **Error! Reference source not found.**.2 System safety work in relation to the Swedish Armed Forces' decision gates.*

3.3 The Life Cycles of the Actors

The life cycle phases of the other actors are staggered against each other. The *stakeholder's* Concept and Development stage is carried out before the *client* can begin their work. The Swedish Armed Forces' Decision Gate BOP *(Decision on Production)* releases funds to begin serial procurement, which means that the *client* can only then begin the procurement of technical systems. In cases where the *client's* offer to the *stakeholder* must rest on a binding offer from the *designer,* the *client's* procurement work begins already during the Development Phase of the Swedish Armed Forces. The work of the *designer* begins as soon as a contract has been concluded with the *client*.

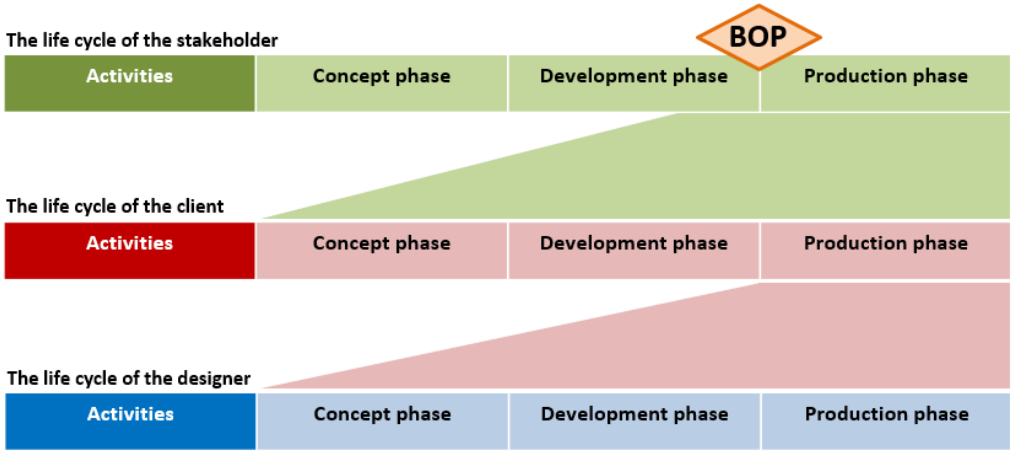


*Figure **Error! Reference source not found.**.3 Staggered life cycles of actors*

3.4 Compilation of Needs

The *Compilation of needs* activity means that the Swedish Armed Forces, in their role as *stakeholder* produce documentation such as reports prepared under Research and Technology Development (R&TD), Perspective Planning (PerP), business intelligence, market analysis and experiences from previous technical systems. Controls and input values that are to form the basis for being able to describe abilities, functions, benefits, properties and limitations are obtained. Information on stakeholders to the envisaged technical system and dependencies to other systems and activities, as well as evidence on which existing technical systems are intended to be replaced are produced.

No system safety work is carried out in the Compilation of needs activity.

3.5 Concept Work

The Swedish Armed Forces' Concept Stage is initiated through the Decision Gate BOK *(Decision on Concept)* which is normally taken at the military-strategic level. The purpose of the Concept Stage is that the Swedish Armed Forces, in their role as *stakeholder* investigate various alternative possibilities to meet the needs for functionality in future technical systems. This functionality can be realised through the changes (modification) of existing materiel or through the acquisition of new technical systems or products or a combination of new materiel, existing materiel and changed (modified) materiel. The concept work is based on the Compilation of needs.

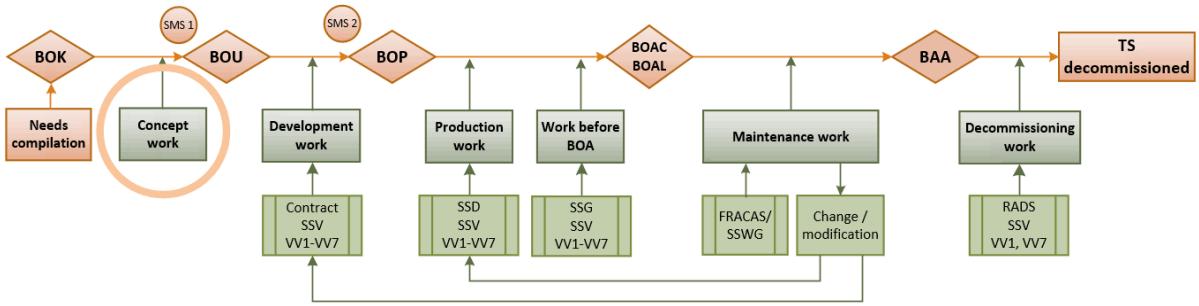


*Figure **Error! Reference source not found.**.4 System safety work in the Swedish Armed Forces' Concept Stage.*

The concept stage does not need to be carried out if the most suitable product can be identified without deeper analysis. In those cases, *System Objective* (SMS 1) is not elaborated.

In cases where a given supply solution is missing, a *System Objective* (SMS 1) needs to be worked out. Alternative supply solutions are investigated and evaluated on the basis of various aspects such as system safety, information security, international cooperation, the user environment and commercial aspects. Furthermore, approaches to facilities and their basic resources need to be described. At the Concept stage, a check is made that the intended technical system falls within the framework of current legislation for military materiel, if not, then the concept must be reworked.

The system safety work focuses on the degree to which it is possible to base the intended technical system on society's requirements and approvals through route selection (VV1), on other state approval route selection (VV2) or whether it is a proven system route selection (VV6). These choices are preferable as it means that already completed system safety work can be used. If the technical system is intended to be changed (modified) or used in a way other than that required for route selection (VV1, 2, 6), other routes also need to be applied.

Approval issued by another State in compliance with a route selection (VV2) refers primarily to a foreign defence authority. In the *System Objective* (SMS 1), the conditions should be specified for being able to accept other states' approvals and, if possible, also which states' approvals can be accepted.

With a proven system according to route selection (VV6), this means a start from a technical system that is already in use and is well known. The prerequisite for being able to rely on the provenance of the technical system is that its execution or use does not change.

3.6 Development Work

The Swedish Armed Forces' Development Phase is initiated through the Decision Gate BOU *(Decision on Development)* and is carried out by the Swedish Armed Forces in the role of *stakeholder*. The purpose of the Development Stage is to describe in *System Objective* (SMS 2) a system solution that meets the Swedish Armed Forces' needs for a future technical system.

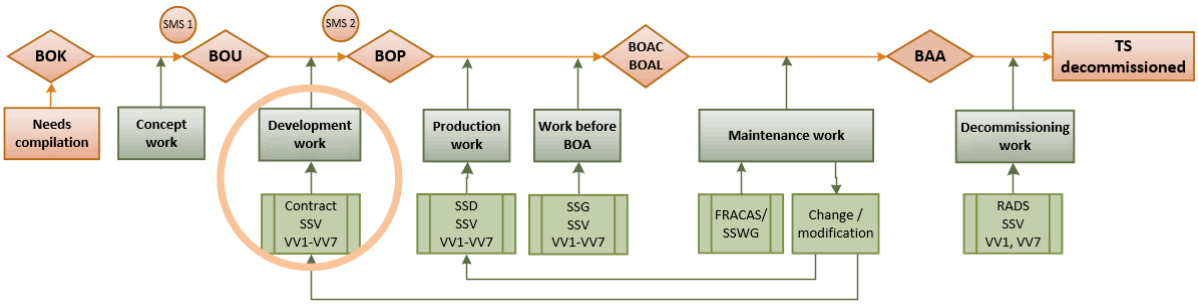


*Figure **Error! Reference source not found.**.5 System Safety Work in the Swedish Armed Forces Development Stage.*

3.6.1 The Swedish Armed Forces' Development Stage as a Stakeholder

If the existing *System Safety Management Plan* (SSMP) and *System Objective* (SMS 2) is valid and sufficient, there is no need to implement a Development Stage.

For new technical systems, *the System Safety Management Plan* (SSMP) may need to be updated. *The System Safety Management Plan* (SSMP) is based on the safety objectives and the Swedish Armed Forces' vision for system safety, which are translated into system safety objectives. The *System Objective* (SMS 2) specifies the system safety requirements.

In cases where an applicable system objective is missing, a *System Objective* (SMS 2) needs to be developed. If *System Objective* (SMS 1) exists, it forms the basis for the preparation of new *System Objective* (SMS 2).

This functionality can be realised through the changes (modification) of existing materiel or through the acquisition of new technical systems or products or a combination of new materiel, existing materiel and changed (modified) materiel. Alternative supply solutions are investigated and evaluated on the basis of various aspects such as system safety, information security, international cooperation, the user environment and commercial aspects. Furthermore, approaches to facilities and their basic resources need to be described.

The architecture of the system solution identifies how a system-of-systems is most appropriately built up of different system elements (technical systems, subsystems, products and integration products). The system architecture at the overall level is defined as far as necessary, for example with regard to adaptation to the organisation or use of existing materiel.

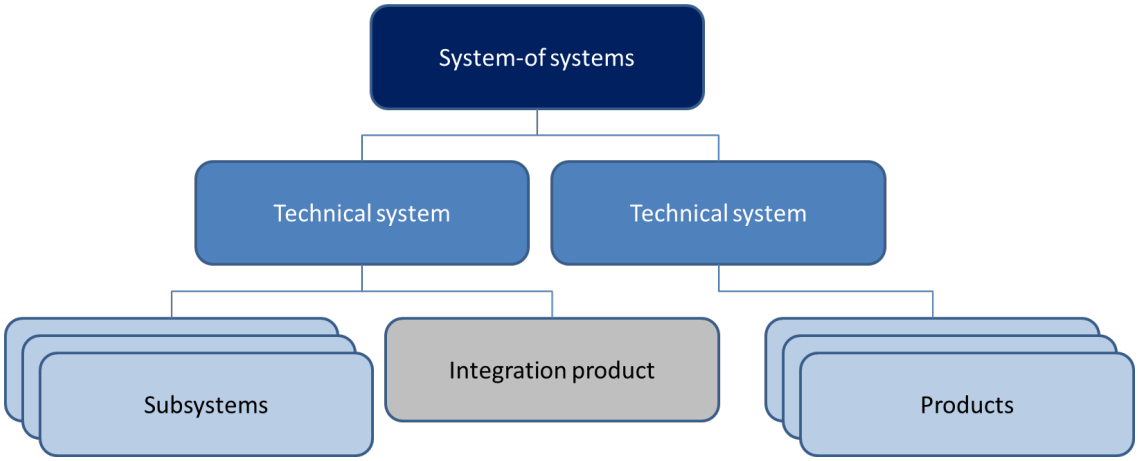


*Figure **Error! Reference source not found.**.6 System-of-systems can consist of optional combinations of technical systems, subsystems, products and integration products.*

Each of these system elements can demonstrate a satisfactory level of safety through different Route Selections (VV). The different system elements must provide a basis for the entire technical system to demonstrate a satisfactory level of safety and also, where appropriate, as one of the systems in a system-of-systems.

System safety work is carried out for the technical system with the aim of clarifying the worst credible consequences in the event of accidents for persons, property and the external environment. This is done in order to be able to determine which Route Selections (VV) may be relevant in the upcoming work. With the support of the system safety work, the *Route Selection Model* (VVM) is applied with a focus on the route selections (VV1 – VV6):

- Route Selection 1 (VV1) - Constitutional requirements
- Route Selection 2 (VV2) - Approved by another State
- Route Selection 3 (VV3) - Approved by another party
- Route Selection 4 (VV4) - Other standards
- Route Selection 5 (VV5) - Design Rules
- Route Selection 6 (VV6) - Proven system

3.6.2 The Development Work of the Swedish Armed Forces or FMV As a Client

The Swedish Armed Forces or FMV in the role of *client* develops a *System Safety Program Plan* (SSPP) that describes how the internal system safety work is to be carried out. Furthermore, it describes how the system safety requirements against the *stakeholder* are to be met and what system safety requirements are to be imposed on the *designer*.

In the *Client's* system safety work, the dimensioned accident risks are determined, which form the basis for the preparation of the *Request for Proposal* (RFP). The system solution is adapted to enable suitable choices even at lower system levels and to provide the opportunity for different procurements. The *client* ensures the collaboration of the coherent technical system with its subsystems, and products from different *designers,* i.e. makes an appropriate distribution between different suppliers based on different aspects. Based on the system safety work, the acceptance criteria for the specified route selections are determined. In the *Request for Proposal* (RFP), requirements can also be made for principled design solutions to the technical system or product.

The *Request for Proposal* (RFP) sets out the criteria for using the route selections (VV1 – VV7) in subsequent system safety valuations during production work:

- VV1: What constitutional requirements must be applied?
- VV2: What documentation must be presented in order to accept an approval from another state?
- VV3: What documentation must be presented in order to be able to accept an approval from another party?
- VV4: What established standards in the field of technology can be applied?
- VV5: What *Design Rules* (DR) and *Technical Rules of Practice* (THR) can be applied?
- VV6: What criteria and requirements can be accepted for a proven system?
- VV7: What *Tolerable Risk Level* (TR) including Risk Matrices must be applied?

3.6.3 Industry Development Work as a Designer

When the industry in the role of *designer* has received a contract, the *designer* creates a proposal *for a System Safety Program Plan* (SSPP) and a more detailed concept for the intended technical system. The *designer* describes in his *System Safety Program Plan* (SSPP) how the choices will be applied for the system with its constituent subsystems and products, as well as based on all existing accident risks for persons, property and the external environment. The *designer* proposes how the choices can be applied to the detailed concept in order to achieve a satisfactory level of safety for the intended technical system. This forms the basis for the contract review.

At the contract review, there are opportunities for the *client* to provide alternative proposals for design and route selections. The *client* and the *designer* may agree on changes to the proposed route selections within the framework of the contract. This is documented in a protocol and then transferred to the contracted *System Safety Program Plan* (SSPP).

Reconciliations with the *client* take place during the design work so that the *System Safety Program Plan* (SSPP) is complied with.

During the development work, prototypes may need to be developed in order to evaluate different technology solutions during testing and trials. Prototypes are normally developed by the *designer*. In the case of prototyping, the *designer* must declare that the technical design measures taken, together with instructions for use, subject to any restrictions, provide a satisfactory level of safety for the intended test or tests.

After completed system safety work, the *designer* compiles the risk documentation by making a system safety evaluation for the technical system. Furthermore, a *Safety Compliance Assessment* (SCA) is issued with a *Safety Assessment Report* (SAR) and *Risk Log* (RL).

3.7 Production Work

The Swedish Armed Forces' Production Phase is initiated through the Decision Gate BOP *(Decision on Production)* and is carried out by the Swedish Armed Forces in the role *of stakeholder*. Decision gate (BOP) means that *System Objective* (SMS 2) is established and that the *client* can thus begin their procurement. The purpose of the production stage is to procure, verify and validate (VoV) and deploy technical systems and products in the unit operations.

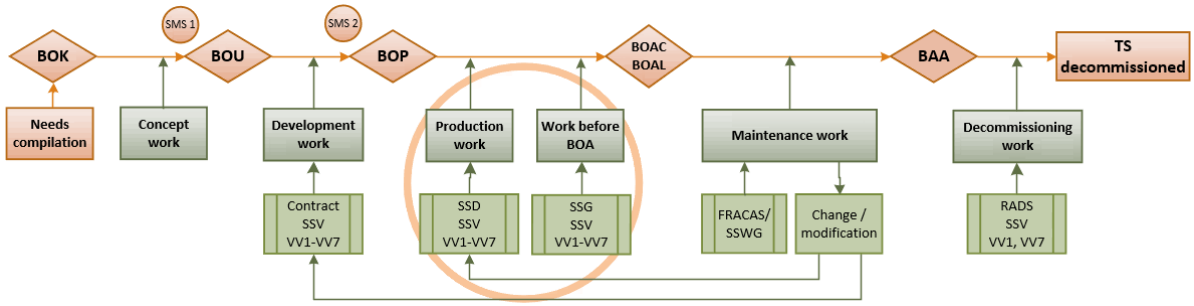


*Figure **Error! Reference source not found.**.7 System safety work in the Swedish Armed Forces' Production Stage.*

The *stakeholder* follows up that the Swedish Armed Forces or FMV in the role of the *client* has managed and interpreted the requirements of the *System Safety Management Plan* (SSMP) and *the System Objective* (SMS 2). This work can be coordinated, agreed upon and quality assured in the *System Safety Working Group* (SSWG).

The *client* carries out procurement in accordance with the controls developed in the previous life cycle sections. Controls regarding system safety can be found in *System Objective* (SMS 2) and in this referenced *System Safety Management Plan* (SSMP).

The *client* ensures that the *designer* works in accordance with the contract and the agreed *System Safety Program Plan* (SSPP). The *client* reviews the *designer's* work before delivery takes place. Furthermore, a *Safety Compliance Assessment* (SCA) is issued with a *Safety Assessment Report* (SAR) and *Risk Log* (RL).

The *client* carries out verification and validation (VoV), which means that compliance with the *System Objective* (SMS 2) can be displayed with sufficient confidence. An independent review as an internal review is carried out and, if necessary, evaluation is obtained from FMV's Advisory Groups in Weapons and Ammunition Safety before System Handover (SÖL) can be carried out. Through its system safety evaluation, the *client* must be able to demonstrate that a satisfactory level of safety has been achieved for the entire technical system. If an already existing technical system is used, its system safety dossier may need to be re-evaluated and, to the extent necessary, reworked based on changes in the intended use of the technical system and in conjunction with other subsystems and products. The *client* issues a *System Safety Declaration* (SSD) with associated system safety declaration.

3.7.1 System Safety Approval (SSG)

The *System Safety Approval* (SSG) confirms that the technical system meets the requirements of the *System Safety Management Plan* (SSMP) and *System Objective* (SMS 2) for its intended use. Furthermore, it is certified that the necessary operating rules exist for managed accident risks and that any proposed restrictions on remaining accident risks are reasonable and that the technical system can thus be brought into operations in a satisfactory manner.

3.7.2 Decision Gate BOAC

Decision on Use, Central Level (BOAC) ensures from a system safety perspective that the technical system as it is actually constituted meets the vision for system safety and that the conditions exist for putting the technical system into use in the Swedish Armed Forces.

The *Decision on Use, Central Level* (BOAC) governs what is to be managed in the *Decision on Use, Local Level* (BOAL). If *Decision on use, Local Level* (BOAL) is not necessary, the corresponding documentation and positions must be reported in *Decision on Use, Central Level* (BOAC).

3.7.3 Decision Gate BOAL

In *Decision on use, Local Level* (BOAL) it is reported that all points are managed that are the responsibility of C OrgE according to the *Decision on Use, Central Level* (BOAC).

3.8 Maintenance Work

The Swedish Armed Forces' Maintenance Stage is carried out by the Swedish Armed Forces in the role *of stakeholder*. The purpose of the system safety work during the Maintenance Stage is to identify conditions in the use of the technical system and its function that means that the system safety evaluation in *the System Safety Approval* (SSG) that forms the basis for *the Decision on Use, Central Level* (BOAC), may need to be supplemented or reworked as applicable. This may also be caused by changes in current legislation, regulations or changed conditions for the previously made Route Selections (VV).

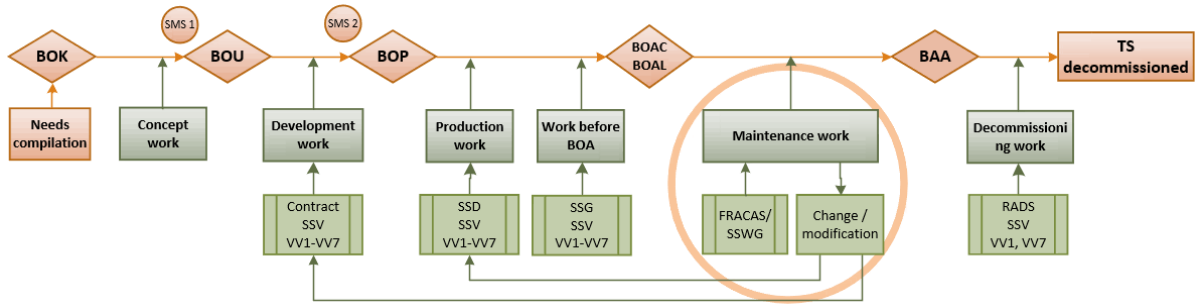


*Figure **Error! Reference source not found.**.8 System safety work in the Swedish Armed Forces' Maintenance Stage.*

Information is systematically collected from use, maintenance and storage (transportation). The information may consist of accident and incident reports, user experience, fault outcomes, performance deficiencies or technical status surveys. The system safety aspects from the collected data during the *Failure Reporting System* (FRACAS) activity are evaluated by the *System Safety Working Group* (SSWG). FMV or industry can be given the task of carrying out more detailed analyses to the extent needed.

Data that are of importance for system safety are analysed and new system safety evaluations are carried out that aim to ensure that a satisfactory level of safety continues to be contained. This may partly mean the need for changes (modifications), partly changes in handling including norm slippage, and partly maintenance. Changes that affect previously made system safety valuations mean that system safety work must be carried out in accordance with the development and/or production stage. Based on such facts, the *System Safety Working Group (SSWG)* provide documentation for new system safety decisions.

In the *System Safety Working Group (SSWG)*, it can be difficult to identify normal slippage from the data collected and therefore this must be monitored in particular. Norm slippage means that there are changes in use that have not been based on renewed analysis or decisions. It is a common phenomenon that occurs when materiel has been used for a long time and without perceived major problems. Norm slippage is problematic because experience is not obviously applicable to the changing use. It may also be the case that the design is neither formally nor in reality intended for, or meets, the requirements of the changed use. This must be continuously monitored and changes in use must be preceded by system safety and conscious decisions. Otherwise, the equipment may be used outside of what it has been shown to be safe for, which may entail not tolerable accident risks.

3.9 Decommissioning Work

The Swedish Armed Forces' Decommissioning Stage is initiated through the Decision Gate BAA *(Decision on Decommissioning)* and is carried out by the Swedish Armed Forces in the role of *stakeholder*. The purpose of the system safety work during the disposal phase is to identify accident risks that may occur during the physical settlement of the technical system.

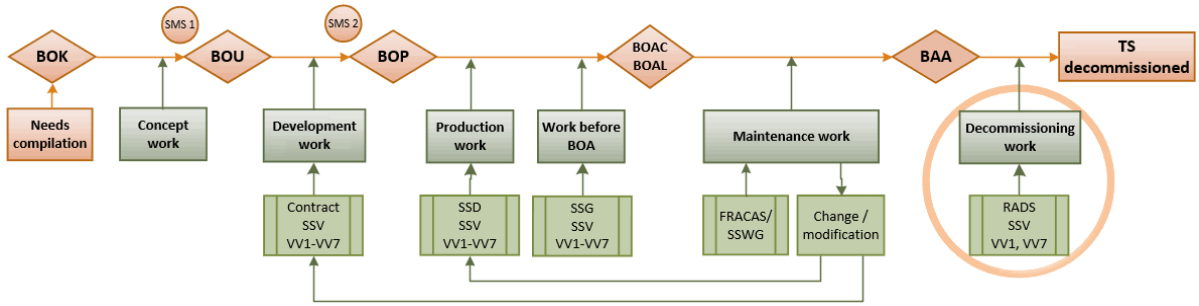


*Figure **Error! Reference source not found.**.9 System Safety Work in the Forces' Decommissioning Stage.*

Decommissioning may be caused, inter alia, by the fact that the technical lifetime of the system has been exhausted or because there is no longer a need for the system. In some cases, an identified safety deficiency in the technical system or product may lead to disposal.

The disposal work aims to investigate different possibilities to get rid of technical systems and products in a safe and sustainable way according to current environmental legislation. Producer responsibility may be invoked on the basis of contract or legislation. New legislation, directives or regulations that did not exist during the production phase can, for example, affect the handling of hazardous substances.

Settlement methods such as transfer, reuse, sale and destruction are evaluated. In the disposal work, financial, legal and practical aspects also need to be taken care of. Decommissioning methods are decided by the Swedish Armed Forces.

Decommissioning needs to be taken into account throughout the life cycle of the equipment. Prior to the physical disposal of technical systems and products, the *Risk Assessment Prior to Disposal of Systems* (RADS) developed during the production phase must be analysed and, if necessary revised. The renewed system safety analysis must identify new accident risks and, if necessary, re-evaluate the previously identified ones that may occur during the physical disposal. It is important that also reserve equipment, maintenance equipment, support systems and Basic and Management Data (BaM) and information regardless of the form in which and the actor is subject to disposal in order to avoid the emergence of unclear responsibilities regarding the system safety status of the materiel and security of the information concerned.

Feedback that the technical system or products are physically decommissioned and that management data has been removed is based on the application decision according to the Decommissioning Assessment.

4 Actors, Roles and Responsibilities

The purpose of this chapter is to describe the roles and responsibilities of the different actors. The various organisations such as the Swedish Armed Forces, FMV, the Swedish Fortification Agency and industry all have different responsibilities, tasks and functions within system safety operations.

4.1 Description of Roles

From the perspective of the Swedish Armed Forces, a few principled roles that carry out system safety activities are described below. Each actor can hold additional roles, but these are managed within their own organisation based on the main descriptions below.

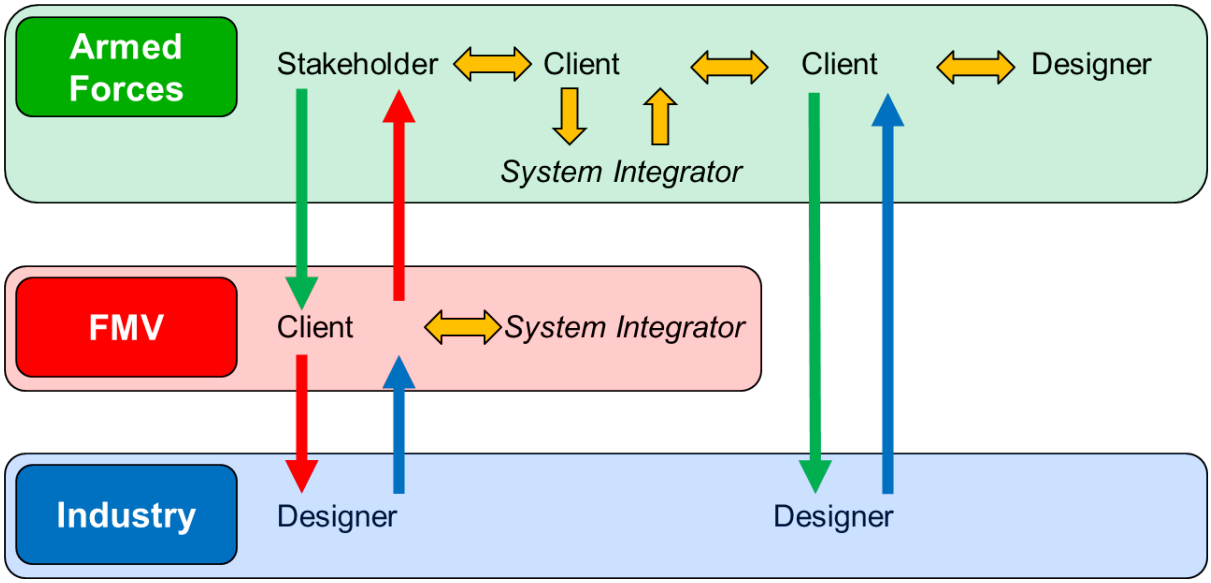


Figure 4.1 The roles of the different actors with order/procurement order and delivery routes.

The stakeholder is the one who, based on the need for abilities and functions, places demand on materiel (system-of-systems, technical systems or products). Furthermore, the *stakeholder* issues *System Safety Approvals* (SSG), follows up the equipment during the maintenance stage and decommissions them.

The *client* is the one who, based on *System Objective* (SMS), places demand on and orders the design and manufacture of the actor or actors who carry out the realisation of technical systems or products, or alternatively gives a special task to a *System Integrator*. Furthermore, the Client issues *System Safety Declarations* (SSDs) and if necessary, carries out the requested tasks during the maintenance and disposal phases.

The *designer* is the one who, based on contracts, realises, designs and constructs technical systems or products. Furthermore, it issues the *Safety Compliance Assessment* (SCA).

The *system integrator* ensures the collaboration of technical systems to a system-of-systems and thus provides the required capability or functionality in cases where confidentiality exists or that a *designer* cannot assume this responsibility.

4.2 Roles of the Swedish Armed Forces

The Swedish Armed Forces have the entire spectrum of roles in system safety operations, and can thus perform tasks in the four roles *of Stakeholder, Client, System Integrator* and *Designer.*

The Swedish Armed Forces hold the roles of *Stakeholder*, *Client*, *System Integrator* and *Designer*.

4.2.1 The Swedish Armed Forces in the Role of Stakeholder

The Swedish Armed Forces in the role of *Stakeholder* have to be responsible for and make decisions on:

- Design Rules (DR) and Technical Rules of Practice (THR)
- System Safety Management Plan (SSMP)
- System Objective (SMS)
- System Safety Approval (SSG)
- Decision on Use, Central Level (BOAC)
- Decision on Use, Local Level (BOAL)
- System Safety Working group (SSWG)
- Risk Assessment prior to Disposal of Systems (RADS)

The Swedish Armed Forces have technical design responsibility for all materiel and impose operational and system safety requirements on units, functional chains, technical systems and products that are to be included in the war organisation and that are thus to be used for training, exercises and operations. This is done through the elaboration and establishment of *System Objective* (SMS) at different levels. These contain, among other things, system safety requirements. The same also applies to equipment used in other operations/activities.

Design Responsible (DesignA) is a role in the Swedish Armed Forces that bears technical design responsibility within the assigned product area. This means coordinating and directing design within those stages of the materiel life cycle where the Swedish Armed Forces bear technical design responsibility. The DesignA role exists at different levels and within different parts of the Swedish Armed Forces' activities. Examples of different levels of the DesignA role are Technical Director and Technical Manager. The role is assigned responsibilities, tasks and mandates through the Swedish Armed Forces rules of procedure (ArbO) including delegations, directives and other decisions.

The Technical Director of the Swedish Armed Forces is responsible for common *Design Rules* (DR) and *Technical Rules of Practice* (THR) and leads the Swedish Armed Forces' technical design activities by identifying, defining, and allocating responsibility for all levels of technical systems and their co-functionality (system-of-systems) as well as making overall

design decisions. The *Technical Manager* (TM) is responsible for *Design Rules* (DR) and *Technical Rules of Practice* (THR) within their own field of activity and leads the technical design activities by identifying, defining and allocating tasks and mandates for underlying levels of technical systems and their co-functionality (system-of-systems) as well as making design decisions in their own field of activity.

Appointed officers in accordance with the Swedish Armed Forces' Rules of Procedure and Delegation (ArbO) establish overall guidelines governing system safety activities described in various *System Safety Management Plans* (SSMP). These guidelines can be found at different levels of the business such as arena, composite system levels and individual system level.

The Technical Manager is technical design manager for the assigned product portfolio. Tasks and mandates for underlying areas within the product portfolio can be distributed via delegation to different levels and executives. The Technical Manager establishes *System Safety Management Plans* (SSMP) for the product area (or certain technical system) and establishes *System Safety Approvals* (SSG) within his own product portfolio.

SÄKINSP and FLYGI carry out inspections. SÄKINSP signs consultations on *System Safety Approvals* (SSG) and FLYGI does this if necessary.

This provides input to the *Decision of Use, Central Level* (BOAC).

C OrgE has an employer and delegated work environment task and is thus responsible for all activities conducted locally and for all materiel used in that operation. C OrgE makes *Decision on Use, Local Level* (BOAL) of centrally determined materiel where necessary, and reports back on operational experiences such as accidents, incidents and deviations.

4.2.2 The Swedish Armed Forces in the Role of Client

The Swedish Armed Forces in the role of *Stakeholder* have to be responsible for and make decisions on:

- Contracts (or equivalent) for the acquisition or changes (modification) to technical systems or products

The Swedish Armed Forces follow up the system safety work by checking the fulfilment of requirements against contracts (or equivalent) based on *System Safety Management Plans* (SSMP) and *System Objective* (SMS). Furthermore, received system safety documentation from *the Designer* or *System Integrator* is reviewed and prepares *System Safety Approval* (SSG) for decision.

4.2.3 The Swedish Armed Forces in the Role of System Integrator

The Swedish Armed Forces in the role *of System Integrator* carry out system safety work to ensure interoperability between technical systems to a system-of-systems. A system-of-systems provides demanded capability or functionality through new combinations of physical products or software. The system safety work is documented in a *Safety Assessment Report* (SAR) with *Risk Log* (RL).

4.2.4 The Swedish Armed Forces in the Role of Designer

The Swedish Armed Forces in the role of *Designer* have to be responsible for and make decisions on:

- System Safety Program Plan (SSPP)
- Safety Compliance Assessment (SCA)

The Swedish Armed Forces in the role of *Designer* basically corresponds to the role of industry below, which means design and production responsibility. The *designer* responds to internal *Request for Proposal* (RFP) documentation by developing a *System Safety Program Plan* (SSPP) for system safety work. Furthermore, a *Safety Compliance Assessment* (SCA) is issued with a *Safety Assessment Report* (SAR) and *Risk Log* (RL).

4.3 The Roles of FMV

FMV procures technical systems and products from various actors (suppliers) such as developing industry, another state, the Swedish Armed Forces' workshops or the Swedish Fortification Agency.

FMV holds the roles of *Client* and *System Integrator*.

FMV manages the technical design responsibility until the approved handover has taken place to the Swedish Armed Forces. Furthermore, FMV can, upon order, participate in the Swedish Armed Forces' development, maintenance and disposal stages, for example by participating in the Swedish Armed Forces' *System Safety Working Group* (SSWG).

FMV in the role of *Client* develops a *System Safety Program Plan* (SSPP) that describes the system safety work to be carried out for the technical system or product in question. Based on *System Objective* (SMS 2), FMV produces a *Request for Proposal* (RFP) for procurement. The *Request for Proposal* (RFP) includes the necessary technical system safety requirements and requirements for system safety activities. In connection with System Handover (SÖL), the *System Safety Declaration* (SSD) is submitted with the *Safety Assessment Report* (SAR) and *Risk Log* (RL).

FMV in the role of *System Integrator* carries out the system safety work that needs to be carried out to ensure interoperability between technical systems to a system-of-systems. The system safety work is documented in a *Safety Assessment Report* (SAR) that is handed over to the *Client*. In connection with System Handover (SÖL), the *Client* submits the *System Safety Declaration* (SSD) with *Safety Assessment Report* (SAR) and *Risk Log* (RL).

4.4 The Roles of the Swedish Fortification Agency

The Swedish Fortification Agency constructs and maintains facilities of various kinds for the needs of the Swedish Armed Forces. Facilities can encompass the environment in which technical systems are installed, connected, stored or used. Installations can, in addition to protection, also provide certain basic civil engineering resources such as electricity, power,

heating, cooling, ventilation, water and sewage. The development of this type of resources is handled by order from the Swedish Armed Forces to the Swedish Fortification Agency, or by order from FMV. The Swedish Fortification Agency submits facility documentation.

In cases where the Swedish Fortification Agency installs technical systems and products such as computer equipment or alarm devices in facilities, the same requirements are imposed on system safety decisions and system safety documentation as if FMV had carried out equivalent work.

4.5 The Role of Industry

The main role of the industry is as *Designer*. The role of *Designer* also includes other roles that may be managed within their own organisation.

The industry holds the role of *Designer*.

Industry that develops, designs and manufactures technical systems and products takes product safety and product responsibility (if legally applicable). Industry responds to internal *Request for Proposal* (RFP) documentation by developing a *System Safety Program Plan* (SSPP) for system safety work. Furthermore, a *Safety Compliance Assessment* (SCA) is issued on delivery with a *Safety Assessment Report* (SAR) and *Risk Log* (RL).

Industries that only carry out series production submit a Delivery Certificate (DC) that certifies that they have followed the production documentation and verified this through quality assurance documentation.

An economic actor, such as a distributor within the EEA area, is responsible for ensuring that only legal products are purchased and sold. An importer in the EEA is responsible for ensuring that only legal products are imported from manufacturers outside the EEA, to be placed on the market. The importer has a greater share in product safety responsibilities compared to the distributor.

5 EU Law and Swedish Legislation

The purpose of this chapter is to account for EU law and Swedish legislation, which impose requirements on the system safety characteristics of technical systems and products so as not to inadvertently cause injury and/or damage to persons, property or the external environment.

5.1 Background

In its capacity as an employer, the Swedish Armed Forces have a legal responsibility for the safety of its employees, but also for those belonging to the Civil Defence, officer cadets, recruits in training, conscripts and for those who are part of a voluntary defence organisation. The Swedish Armed Forces also have legal responsibility for the safety and property of third persons in connection with the activities the Swedish Armed Forces conduct. The tasks of the Swedish Armed Forces must be resolved within the framework of current legislation.

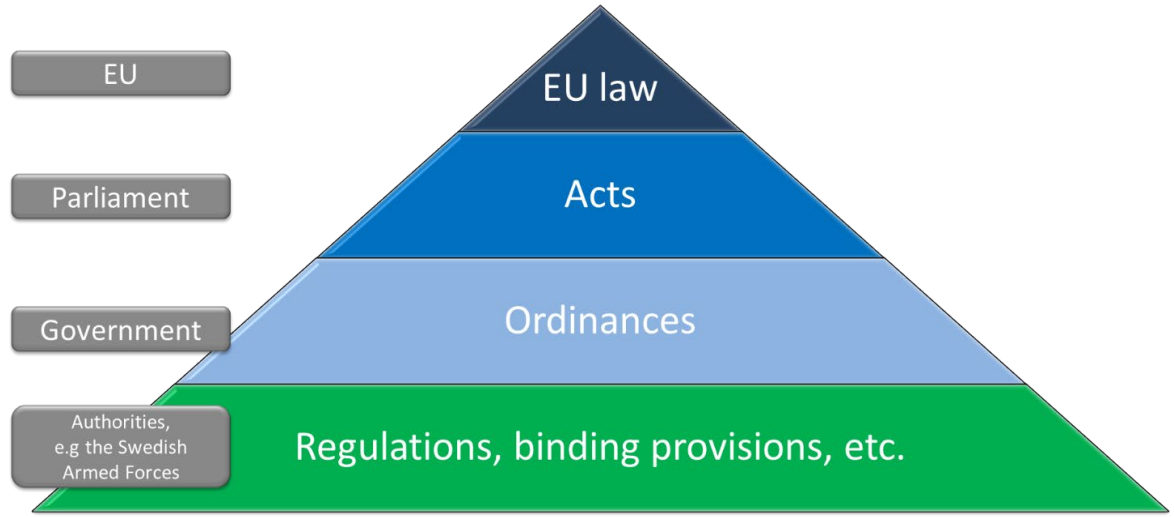


Figure 5.1 Hierarchy of EU law, acts, ordinances, regulations, etc.

A technical system may consist of several different subsystems and products. It is to identify the rules applicable to the respective technology area. Some rules govern the design and technical characteristics such as pressure, energy or electrical voltage levels. In other cases, function/impact or intended use may govern whether the rules apply or not.

Manufacturers or *systems integrators* must ensure that the interoperability between different subsystems and products (including system-of-systems) is fully analysed in terms of applicable EU law and Swedish legislation for the complete technical system. It should be noted that the rules usually place liability on the legal/liable manufacturer, that is, the economic operator who puts a new product on the market in its name.

Formulations in EU law and Swedish legislation are often written technology-neutral, which means that the requirements are expressed in such a way that it does not matter what technology the systems are built with. Safe functions can be realised with various technologies such as mechanics, pneumatics, hydraulics, pyrotechnics, electrical circuits, electronics, radio communications or software. The important thing is that the manufacturer

has carried out its system safety work and then used techniques and methods to avoid errors in design and manufacture, that is, failures that can lead to accidents or incidents. This work also includes managing accident risks during use and maintenance.

In the handbook, references and document designations are those that were current at the handbook's completion. In cases where the references need to be applied, it is recommended to use the current version of the reference.

5.2 EU Regulations, EU Directives and Harmonised Standards

Within the European Union (EEA area for freedom of the *Single Internal Market*), it is sought to harmonise legislation in several areas in order to enable mobility on the internal market without additional compelling requirements while ensuring a high level of safety. Therefore, EU/EC Directives/Regulations are issued, which are addressed to the Member States and to interested parties respectively. EU Directives must be incorporated into the legislation of the respective Member States. In Sweden, it is usually done through acts, ordinances and regulations.

> This handbook will from here on use the term EU Directive, even though an EU/EC Directive´s Swedish transfer to acts, ordinances and regulations is referred. The term EU Directive is used even if the legal act is an EU Regulation.

An EU Directive is binding on the result to be achieved, but leaves it to the Member State to determine the approach to the transfer. An EU Regulation, on the other hand, operates directly in each Member State.

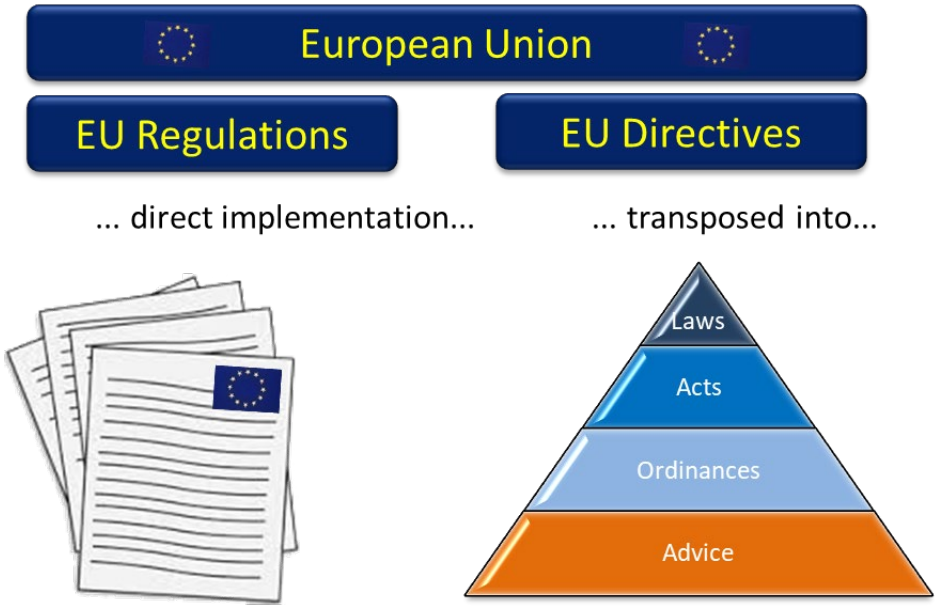


Figure 5.2 Adoption of EU Regulations and EU Directives in Sweden.

EU Directives and EU Regulations set out basic health and safety requirements for design and manufacture, for the protection of persons, domestic animals, the environment and, to a

certain extent, property. The basic health and safety requirements are minimum requirements that must be met for products to be sold/distributed/used within the EU/EEA. Often there are requirements for the conduct of risk analyses. The products must also withstand reasonably foreseeable misuse without becoming hazardous. The requirements must be met by each individual product in order for it to be placed on the common internal market with the intention it being put into service/to be used on this market, for example in Sweden.

Detailed requirements for technical design are in practice referred to Harmonised Standards. These impose verification requirements according to specified test methods. Technical design requirements are sometimes imposed, but the principle is that a Harmonised Standard must not lock-in a design solution or hinder development. This method of working means that EU Directives and EU Regulations offer stability and do not need to change at the same rate as today's level of technology changes.

The applicability of the respective EU Directive varies as to how and when it must be applied to different products.

For certain areas of technology, EU Regulations are issued for immediate operation in EU Member States. They are thus not transferred to Swedish regulations, although they are often supplemented by an ordinance from the Government or by authority regulations. Examples include EU Regulations for road vehicles, Personal Protective Equipment (PPE) and Medical Devices (MDs).

EU Regulations are part of Swedish legislation and some instruments can come into force as early as 20 days after they have been published within the EU. EU Directives are normally to be transposed and applied into Swedish law within 18 months of publication. EU Directives provide for CE marking of the products whereby the manufacturer demonstrates and verifies that the product complies with the regulatory requirements of safety, health and the environment.

CE

Figure 5.3 Example of CE marking.

Standards can include both normative and informative parts. The normative parts constitute the claims or requirements of the standard. It is the normative elements that must be complied with in order for a product to be considered to conform to the standard. The informative parts may be made up of notes and explanatory appendices to the normative parts.

A client may impose higher or more precise safety requirements than specified in a particular EU Directive or a Harmonised Standard based on the environment of use and under the conditions in which the product is to be used. Such higher requirements are set in the *Request for Proposal* (RFP) and managed by CE marking.

Harmonised Standards are European standards drawn up in accordance with guidelines agreed between the European Commission and the European Standardisation Bodies, which follow a mandate from the Commission. When a product meets the normative requirements of listed (i.e. current) Harmonised Standards, the product is also assumed to meet the corresponding basic safety requirements of the current EU Directive for the product according to the so-called *principle of presumption*.

The Harmonised Standards giving presumption are set out in the Commission's Decision published in the *Official Journal of the European Union* (OJ). It also indicates if there are restrictions on the standard and when the presumption of an old Harmonised Standard expires. In some special cases there remain standards that are mandatory, for example in the road vehicles area.

A Harmonised Standard is voluntary to follow. Several, but very rarely all, of the requirements of the EU Directive are covered by one (1) Harmonised Standard. Most often, several standards need to be applied. The requirements of the EU Directive that the standard is considered to meet are set out in an Appendix Z/ZA of the respective standard. Note that the requirements of an EU Directive which the presumption of the Harmonised Standard does not cover, the manufacturer must take care of separately. However, if the manufacturer does not comply with a harmonised standard, it will be more difficult and more cumbersome to verify compliance with the basic health and safety requirements.

One advantage of common rules on product safety responsibility and product responsibility is that a product can be placed on the market in several Member States in a single embodiment, without a repeated approval procedure in each individual Member State. The basic health and safety regulations are the same in all EU Member States. The requirements of national legislation transferring the directives are mandatory and must be met in order for the product to be placed on the market. For products with moderate accident risks, EU Directives rely on the manufacturer's own verification that safety requirements are met. For products with greater risks, third party certification requirements, known as a Notified body, are required.

5.3 Health and Safety Legislation

The purpose of the Work Environment Act is to prevent ill health and accidents at work and also to achieve a good working environment. The Work Environment Act regulates the obligations of the employer as well as the employee. The term workers in the Swedish Armed Forces refers to all personnel, i.e. employed personnel, those belonging to the Civil Defence, officer cadets, recruits in training, conscripts and for those who are part of a voluntary defence organisation, where they participate in activities within the Swedish Armed Forces.

5.3.1 Basics

The Work Environment Act is a framework law supplemented by regulations, which are communicated by virtue of the law. The Work Environment Act assigns that the employer is responsible for ensuring that the safety of staff is satisfactory. The supervisory authority for the Work Environment Act is the Agency for Health and Safety at Work, except on board ships, including warships, where the Swedish Transport Agency is the supervisory authority.

According to the Work Environment Act, the health and safety and aspects must be adequate, taking into account the nature of work and social and technical developments in society. Working conditions should be adapted to the different conditions of people in physical and mental terms.

In situations where raised readiness levels are called upon, the Government may announce specific regulations.

5.3.2 General Responsibilities of the Employer

The employer's responsibility means that the employer must take all the precautions necessary to prevent the employee from being exposed to health hazards or accident risks. The employer must systematically plan, direct and control activities in a manner which leads to the working environment meeting the prescribed requirements for a good working environment. The employee must not only know what accident risks may exist, but also have knowledge of how to avoid them. In addition, work injuries must be investigated, the operational risks must be continually investigated, and measures that result from this must be taken. When changes to the activity are being planned, the employer must assess whether the changes entail risks of ill-health or accidents which may need to be remedied.

Technology, work organisation and job content must 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. The distribution of working hours must also be taken into account. Closely controlled or restricted work must be avoided or limited. Machinery, implements and other technical devices must be designed, positioned and used in such a way as to provide a satisfactory level of safety against ill-health and accidents.

5.3.3 General Responsibilities of the Supplier

Any person manufacturing, importing, delivering or providing a machine, implement, protective equipment or other technical device must ensure that the device provides a satisfactory level of safety against ill-health and accidents when it is placed on the market, delivered to be used or displayed for sale. Instructions for the device's assembly, installation, usage and maintenance as well as other information about the device which is of significance to prevent ill-health and accidents (product information) must be enclosed upon delivery through clear marking, in form of documentation or in other manner. Information of particular significance for the work environment must be submitted for the device.

Any person manufacturing, importing or delivering a substance that can cause ill-health or accidents must take the measures necessary in order to prevent or counteract any safety hazards entailed by the substance when used as intended. Product information must be supplied at the time of delivery by means of clear marking, in the form of documents or otherwise.

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

5.3.4 Regulations Issued Under the Work Environment Act

The Work Environment Act is a framework law that gives Government the right to empower a specific authority, in this case the Work Environment Authority (Arbetsmiljöverket - AV) and the Swedish Transport Agency, to provide supplementary regulations to the act if necessary, something which is carried out on a continuous basis

The Work Environment Authority has issued a number of regulations with detailed requirements and rules. The majority of these are general and always apply. Regulations should be well known and applied by those who receive assignments for the production of materiel for the Swedish Armed Forces. Regulations AFS 2008:3 on Machinery, which transpose EU Directive 2006/42/EU, are central as much materiel falls under these rules.

In some of the regulations (AFS) issued by the Work Environment Authority, 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.

5.3.5 Exemptions for Military Use and Military Materiel

Some regulations allow certain exemptions for military use and/or military materiel. Examples of such regulations include AFS 2020:1 Workplace design, the Radio Equipment Directive (RED) through the Post and Telecommunications Agency's regulations on requirements for radio equipment PTSFS 2016:5, and AFS 2008:3 Machinery respectively. Note, however, if the product (or a similar product) can be of dual-use, i.e. can be used both in civil and military scenarios, then the military exemption cannot be invoked, but the product must be CE-marked.

Through the exemption for military use, the legislator intends to grant the Swedish 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 the Work Environment Act. In order to use the intended freedom of action in a responsible manner, the Swedish Armed Forces are required to produce its own application instructions with guidelines, limit values etc., which the Swedish Armed Forces define as tolerable for Swedish military personnel.

The Work Environment Authority's Regulations AFS 2008:3 Machinery, excludes machinery that is *specially* designed and manufactured for *military* or *law enforcement purposes*. The background of this exemption for certain military materiel is that certain military purposes impose requirements for advanced materiel, often based on new technologies and specific applications, which, if possible, must not be disclosed to a potential adversary. If such technologies or applications are safety classified data (defence confidentiality), CE marking cannot be implemented.

Where legislation allows exemptions for certain military materiel or military use and, if necessary, specifies requirements for limit values, the Swedish Armed Forces need to provide a detailed specification of the requirements for a similar purpose within the Swedish Armed Forces in order to provide protection for the military personnel that will be using the technical system (for example AFS 2020:1 Workplace design).

The fact that a regulatory framework allows exemptions for certain military materiel does not mean that the requirements of the regulatory framework should nevertheless be applied to the extent possible.

6 Standards

The purpose of this chapter is to describe civil and military standardisation and to present the most common international standardisation bodies.

6.1 General Description of Standards

Standardisation takes place both in the civil and in the defence field, both nationally and internationally. In the Swedish Public Procurement Act (LOU) and in the Act on Public Procurement in the Field of Defence (LUFS) there is an order of priority that determines the order in which standards are to be used. Where exemptions need to be made, they must be proportionate and the reasons need to be well described. The priority is designed to avoid, as far as possible, national special requirements between the different member states within the EU.

It is voluntary to follow a standard until someone refers to its fulfilment, for example in regulations or in a contract, but the requirement of an authority in both cases under the Public Procurement Act (LOU) must always be followed by the words *"... or equivalent"*. Exceptions to this requirement may be dealt with on a case-by-case basis.

> It is optional to follow a standard until someone indicates that it must be fulfilled. In most cases, standards still need to be followed when in practice there are no other alternatives to meet the regulatory safety requirements.

There are many benefits to using standards such as interoperability, functionality, technology coordination, common components, safety, operational reliability, reliability, and compatibility with general logistics systems, total cost of ownership and other similar defence-related requirements.

The term *Standards* in this handbook refers to both formally established standards issued by standardisation bodies and standard-like documents in the form of guidelines and handbooks issued by trade associations.

> The user of a particular standard should always obtain it from the publisher. Partly to have access to the latest edition, partly due to possible copyright.

6.2 Civil Standards

Civil standards are used by both military and civil authorities, other technical organisations, as well as by industry.

Sweden participates in international standardisation through the three state-recognised standardisation bodies:

- Swedish Electricity Standards (SEK)
- Swedish Institute for Standards (SIS)

- Swedish Information and Telecommunications Standardisation (ITS)

SEK is a member of the international standardisation organisations CENELEC (European) and IEC (global), SIS is a member of CEN and ISO and ITS is a member of ETSI.

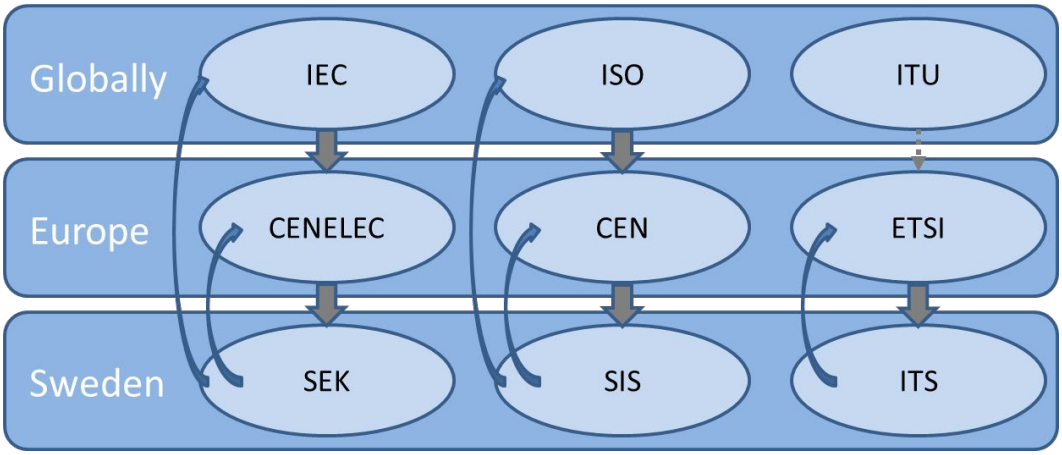


Figure 6.1 Simplified chart of the relationship between different recognised standardisation bodies.

6.3 Defence Standards

Defence standards are used by both military and civil authorities, other technical organisations, as well as by industry. Defence standards have different information safety classifications, which need to be taken into account when defining requirements between different actors, as some are covered by defence confidentiality.

Defence standards can generally be divided into operational standards, capability standards and technical standards. NATO standards are unofficially assessed by both the EU and the UN as international defence standards. These standards are used voluntarily by NATO member states and partners. However, the use of NATO standards may be influenced by agreed partnership goals within the framework of the *Partnership for Peace Planning and Review Process* (PARP). NATO directs the use of the standards that partner countries should implement when interacting with NATO units.

The technical standards are more nation-specific and include, for example, standards for colour, ballistic protection and the quality of electrical power for weapons on ships. There are a large number of Government agencies and Government organisations that in different ways create defence standards independently of each other.

6.4 The Function of Defence Standardisation organised at FMV

Defence standardisation was established in 1944, when the Defence Standardisation Delegation was formed for joint standardisation purposes. In 1976, the Government abolished the Defence Standardisation Delegation and decided that responsibility for standardisation in specific areas would be allocated to the authorities respectively under the Ministry of Defence. Furthermore, the Swedish Government decided that FMV would keep together common standardisation issues and provide agency-wide secretariat functions in consultation

with the authorities under the Ministry of Defence. In addition, FMV would be responsible for the Swedish Defence Standards (FSD).

FMV holds together issues of standards in the field of defence through Swedish Defence Standards (FSD). The FSD is tasked with administering and providing both international and national defence standards as well as providing civil standards to the constituent authorities. FSD also provides Government-wide standardisation services to the agencies under the Ministry of Defence and their suppliers. Employees of defence agencies can find facts about FSD on their website. The authorities covered today are:

- Swedish Armed Forces (FM)
- Swedish Defence Materiel Administration (FMV)
- Swedish National Defence Radio Establishment (FRA)
- Swedish Coast Guard (KBV)
- Swedish Civil Contingencies Agency (MSB)
- Swedish Defence Research Agency (FOI)
- Swedish Defence University (FHS)

Other authorities, Government agencies such as the Civil Aviation Authority (LFV) and the industry also apply certain Swedish Defence Standards (FSD) in their operations.

7 Swedish Armed Forces' Regulations

The purpose of this chapter is to describe the Swedish Armed Forces' internal regulations and handbooks. These need to be taken into account when defining requirements as internal regulations may differ from, or be more detailed than, equivalent civil requirements.

7.1 The Swedish Armed Forces' Statute Book (FFS) and the Swedish Armed Forces' Internal Regulations (FIB)

The Swedish Armed Forces decide on regulations in the form of statutes that are published in the Statute book of the Swedish Armed Forces (FFS) and in the Swedish Armed Forces' Internal Regulations (FIB). Furthermore, there is the General Council of the Swedish Armed Forces (FAR). FFS, FIB and FAR are decided by the Commander-in-Chief or by the person authorised. Some FFS are decided by the Defence Inspector for Health and Environment (FIHM).

FFS contains provisions that are also aimed at other authorities such as the Swedish Fortification Agency, the Swedish Defence Research Agency (FOI) and FMV, but also at companies or for individuals. This depends on what authority the Swedish Armed Forces have to issue regulations in a particular area, such as the Rules for Military Aviation (RML).

The FIB contains provisions that may include regulatory requirements that must be met in order for a technical system or product to be used in the Swedish Armed Forces. In *System Objective* (SMS 2), all applicable FIBs need to be specified, for example those within the Rules for Naval Operations (RMS).

The content of FIB and FAR may need to be transferred to requirements in the *Request for Proposal* (RFP).

7.2 Rules for Military Aviation (RML)

All activities that are considered aviation activities are subject to a permit in accordance with the Aviation Act (SFS 2010:500). In accordance with the Aviation Ordinance (SFS 2010:770), the Swedish Armed Forces have been authorised to issue regulations and supervise military aviation. The Swedish Armed Forces regulate this through the Swedish Armed Forces' regulations on military aviation FFS 2019:10, FFS 2020:4 and their designated regulations, handbooks and implementation regulations SE-EMAR *(European Military Airworthiness Requirements)*, collectively referred to as the Rules for Military Aviation (RML). For civil aviation, as well as for air navigation services for both civil and military aviation, the Government has authorised the Swedish Transport Agency to decide on regulations and to act as a supervisory authority.

The European Commission, through EASA (*European Aviation Safety Agency*), is responsible for the regulation and supervision of the more important parts of civil aviation. In military aviation, EU countries cooperate within the framework of the European Defence Agency (*EDA)* and have created common requirements for airworthiness etc. in the form of EMAR *(European Military Airworthiness Requirements*) which have been translated into national implementation rules SE EMAR.

The military aviation system includes air operations, airports and air bases, and airspace. The three systems include, within their respective sub-areas, operators including personnel, aeronautical systems and other aeronautical products, airport and air base systems, ground, facilities and premises, aviation-related devices and equipment on board seagoing ships and other installations, and the airspace that meets the need for aircraft manoeuvring.

The Swedish Armed Forces must conduct military aviation on the basis of a tolerable risk that may vary depending on current conditions and tasks. The Commander-in-Chief, or the deputy the Commander-in-Chief decides on, determines what a tolerable risk is. This is applied within the Swedish Armed Forces (Rules for Military Aviation, RML) in the form of aviation safety risk that covers what affects flying, that is, all the different services and activities that are affected. The concept of tolerable risk is thus not consistent with the concept of *Tolerable Risk Level* (TR) in system safety.

Rules for aircraft are contained, through RML, in implementation rules SE EMAR and relate to airworthiness, which means that people and property must not be harmed in, or in direct connection with, flight. This means that additional system safety requirements need to be imposed on technical systems covering aircraft or other aeronautical products in order to achieve a satisfactory level of safety for the entire technical system.

7.3 Rules for Naval Operations (RMS)

The Swedish Armed Forces regulate military maritime safety through the Rules for Naval Operations (RMS). RMS will in due time be replaced by the Swedish Armed Forces' Internal Regulations (FIB) for naval operations. The concept of military maritime safety includes both ship safety and diving safety.

In order for a warship to be used in the Swedish Armed Forces, there must be a valid certificate of seaworthiness. For diving systems, there must be a valid dive safety certificate. Such evidence, together with the other certificates and documents regulated in the Rules for Naval Operations (RMS) and other applicable regulations, proves that the applicable regulations are met.

The Rules for Naval Operations (RMS) include rules on, among other things, supervision, maritime safety systems, manning and qualifications, design and equipment requirements (for both warships and diving systems) and anti-pollution measures. In practice, this means that the Swedish Armed Forces, through the Military Maritime Safety Inspectorate (SJÖI), partly formulate Rules for Naval Operations (RMS) and partly exercise the Swedish Armed Forces' internal supervision of compliance with these rules.

7.4 The Swedish Armed Forces' Operational Safety Regulations (SäkR)

The Swedish Armed Forces' Operational Safety Regulations (SäkR) contain provisions for the operations to be carried out safely, i.e. with a tolerable risk to personnel and third parties, and to minimise damage to materiel, property and the external environment. Provisions must apply to training and exercises, as well as to operations in peace, at heightened readiness and to operations that do not involve combat action. SäkR is aimed at senior officers of Organisational Units (C OrgE), exercise leaders, troop commanders and other personnel involved in the Swedish Armed Forces' activities.

Documentation for SäkR is obtained from *System Safety Approvals* (SSG), *System Safety Announcements* (SSM) and from experiences of technical systems during use and maintenance.

7.5 Other Regulations and Handbooks

For certain legislation, the Swedish Armed Forces issue regulations and supplementary handbooks, such as:

- The Swedish Armed Forces Handbook for Storage and Transport of Ammunition and Other Explosives (H IFTEX)
- The Swedish Armed Forces Handbook for measures against fire and explosion hazards, water pollution and chemical health effects from flammable goods (H BVKF)
- Handbook for Basic maintenance of Vehicles (FAG F)

8 Design Rules and Technical Rules of Practice

The purpose of this chapter is to describe the intention and application of design rules (technical requirements) and technical rules of practice (administrative requirements) of different actors.

8.1 General Information about Design Rules and Technical Rules of Practice

Design rules (DR) intend to govern the design of technical systems and products in order to meet requirements for characteristics such as performance, availability, interoperability between systems, finances and information and system safety.

Design rules (DR), from a system safety perspective, may include requirements for certain designs or requirements for principles for such design so that known accident risks are reduced or avoided. The aim is to indicate, for proven technology, appropriate ways of preventing or reducing the effect of known accident risks.

Technical Rules of Practice (THR) aim to govern administrative procedures related to the design of technical systems and products, as well as to facilitate use, maintenance, storage (transport) and disposal (reuse). *Technical Rules of Practice* (THR) specify how administration surrounding technical systems and products is to be carried out and do not have a direct influence on the design.

8.2 Swedish Armed Forces' Design Rules and Technical Rules of Practice

Military activities may imply that the Swedish Armed Forces need stricter system safety requirements for the equipment than the legislation stipulates in order to achieve a satisfactory level of safety. The Swedish Armed Forces can then establish these stricter system safety requirements such *as Design Rules* (DR) so that certain design or design principle is applied, or that a certain stricter limit value is contained.

For military equipment that is specifically designed and manufactured for certain military purposes, or for other military activities, exceptions to the requirements of the regulations are sometimes allowed, for example regarding limit values in the Swedish Work Environment Act's various regulations. If necessary, the Swedish Armed Forces can develop their own *Design Rules* (DR) with guidelines and limit values that the Swedish Armed Forces define as tolerable for Swedish military personnel. Other types of controls can also be developed by the Swedish Armed Forces. These can, but do not need to, be translated into *Design Rules* (DR).

Managing accident risks by staying within established limits is recommended over evaluating the corresponding accident risk against a *Tolerable Risk Level* (TR) expressed in a risk matrix. The limit value is linked directly to current accident risks, while the tolerable risk level is general. An explicit requirement for limit values leaves less room for interpretation and subjective judgement and can also be used for different technical systems and products. If such limit values have not been established, the issue is instead treated as a risk of certain

harmful effects and is evaluated against the tolerable risk level of the relevant technical system expressed in a risk matrix.

The Technical Director of the Swedish Armed Forces establishes the *Swedish Armed Forces' common Design Rules* (DR) and *Technical Rules of Practice* (THR) and the respective Technical Managers establish *Design Rules* (DR) and *Technical Rules of Practice* (THR) within their own field of operation. In addition to the above, the Technical Director of the Swedish Armed Forces may adopt directives, instructions within the framework of the Swedish Armed Forces' design activities. The Swedish Armed Forces maintain a list of established common and domain-specific *Design Rules* (DR) and *Technical Rules of Practice* (THR).

> What Design Rules (DR) and Technical Rules of Practice (THR) can be applied to the technical system or products must be specified in System Objective (SMS 2).

Information can also be collected systematically from use and maintenance. The information may consist of accident and incident reports, user experience, fault outcomes, performance deficiencies or technical status surveys. When following up on accidents, incidents and deviations, new knowledge about the accident risks of technical systems normally arises. It is important that this information, including the risk reducing measures taken, is brought to the attention of FMV and the manufacturer (industry).

The *Design Rules* (DR) adopted by the Swedish Armed Forces apply, where applicable, to the assignments and orders that FMV carries out for the Swedish Armed Forces.

8.3 FMV's Design Rules and Technical Rules of Practice

FMV maintains a list of established *Design Rules* (DR), handbooks (Design Rule Collections) *and Technical Rules of Practice* (THR) to be applied in the procurement and change (modification) of technical systems and products.

If the Swedish Armed Forces identify a safety deficiency during the use or maintenance of a technical system, FMV, on request from the Swedish Armed Forces, develops design solutions with the aim of eliminating the risk of accidents or reducing the probability of repeated accidents and/or reducing its consequences if the accident nevertheless occurs. The new design solution introduced could be applied in the future use of the corresponding technology. Experience from such design changes can be transformed into general design requirements into a *Design Rule* (DR). Knowledge that has emerged through external analyses or through new/revised standards can also be included in the *Design Rule* (DR).

Handbooks (design rule collections) are either produced because technical systems in a certain area are judged to have higher risks, or that there is already general knowledge of the system area's accident risks. In several cases, new *Design Rules* (DR) for an entire system group have been documented and started to be applied after investigations of actual accidents that have shown that deficiencies in a technical system have been contributing causes to the accident's occurrence.

FMV's handbooks (design rule collections) in the field of system safety are:

- FMV Weapons and Ammunition Safety Handbook (H VAS)
- FMV Handbook for Software in Safety Critical Applications (H ProgSäk E)
- FMV Handbook on Safety (H FordonSäk)
- FMV Handbook for Safe Electrical Products and Systems (H SEPS)
- FMV Handbook for Safe Field-based Workplaces (H SFAPL)

There are also other handbooks published by FMV that place demands on technical systems and products, such as the EMMA handbook (Handbook Electromagnetic Environment).

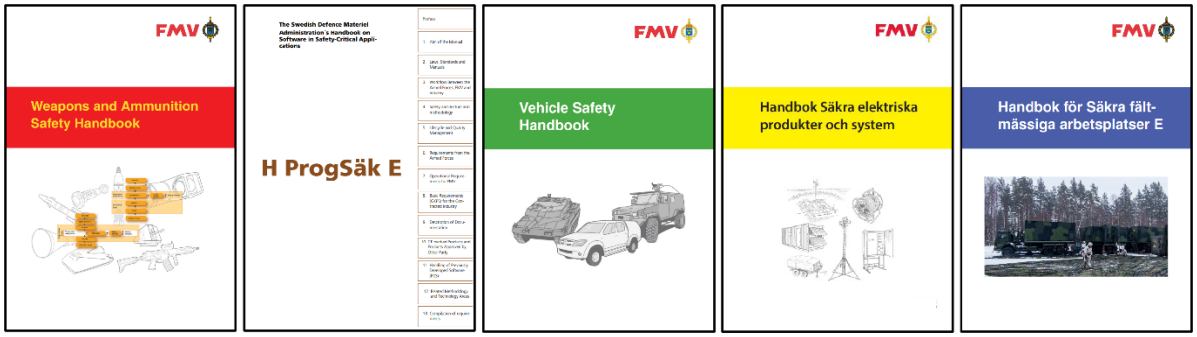


Figure 8.1 FMV's handbooks (design rule collections) in the field of system safety.

In cases where area-specific handbooks (design rule collections) exist, these are applied in parallel with the System Safety Handbook. If the technical system includes weapons and/or ammunition, the FMV Weapon and Ammunition Safety Handbook (H VAS) must be used in conjunction with this handbook. The same applies to other product safety areas where the technical system includes, for example, platforms, software and electrical products.

FMV's area-specific handbooks can be applied voluntarily and made mandatory by directives within an organisation or by contract (or equivalent) to another actor (authority) or a manufacturer (industry).

Technical Rules of Practice (THR) may exist for technical systems to comply with specific rules, carry out certain tests or undergo independent review prior to use in a particular field of technology. Furthermore, there may be rules for, for example, requirements for management data.

The individual requirements that will apply to the technical system or product in question must be taken from the *Design Rules* (DR), the handbooks (Design Rule Collections) and the *Technical Rules of Practice* (THR). These requirements are stated in the Technical Specification (TS) of the technical system and in the Business Commitment Specification (VÅS) if the requirement is of an operational nature.

Design Rules (DR), handbooks (Design Rule Collections) and *Technical Rules of Practice* (THR) do not have the same status as Harmonised Standards and thus do not confer a presumption of conformity with the essential requirements of an EU Directive.

Requirements taken from Design Rules (DR), handbooks (Design Rule Collections), and Technical Rules of Practice (THR) for technical systems and products must be specified in the Request for Proposal (RFP).

8.4 Manufacturer's Design Rules

The manufacturer's design rules are primarily aimed at complying with EU law, Swedish legislation and technical standards.

The manufacturer is often found in one or more competitive markets. In order to maintain or increase their market share, the products marketed must offer an adequate level of safety and have competitive performance and good availability. Furthermore, products are required to comply with international standards in order to avoid technical barriers to trade on the global market.

9 Language

The purpose of this chapter is to outline the requirements of EU law and the Swedish Armed Forces on languages for technical information. It is vital that information can be understood by the user and especially important that safety regulations are not misunderstood due to substandard language ability. The Swedish Armed Forces therefore need to impose language requirements for different user interfaces and materiel documentation.

9.1 Languages for Different User Interfaces

A graphical user interface is a form of information carrier that allows the user to interact through graphical symbols and alarms, instead of text-based user interfaces or text navigation. User instructions, in addition to being in the form of a printed instruction handbook, can be displayed on push buttons, on pressure-sensitive screens, or as projected information in a *Head-up display* (HUD). Text on push-buttons and on pressure-sensitive screens are normally also subject to the language requirement of EU Directives. The same language requirements also apply in cases where the product speaks/reads instructions for handling.

9.2 Language of Technical Information for Swedish Armed Forces

The right, obligation and responsibility to issue the necessary governing and informative documents for technical systems comes with the technical design responsibility.

Technical information for defence materiel refers to materiel documentation and technical data. Materiel documentation is the documentation required for safe use, maintenance, handling, supply and modification. Technical data refers to matters/items to be accounted for in different management systems. An example of this is *Safety Data Sheets* (SDS) for chemical products.

Materiel documentation is a collective term for both printed matters (hardcover or loose-leaf) and electronic documents dealing primarily with function, handling, operation and maintenance. It can also be warning labels such as signs and stickers attached to technical systems and products.

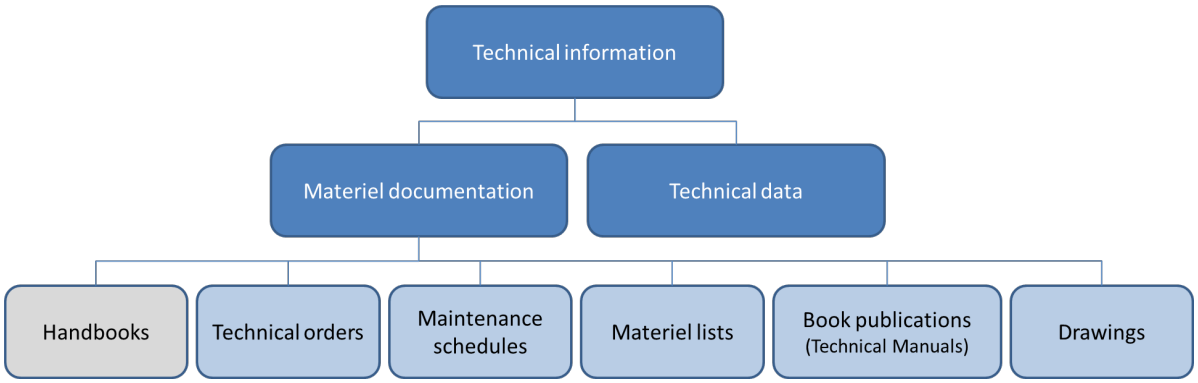


Figure 9.1 A simplified view of technical information within the Swedish Armed Forces.

For technical information for defence materiel, a different nomenclature is used at FMV.

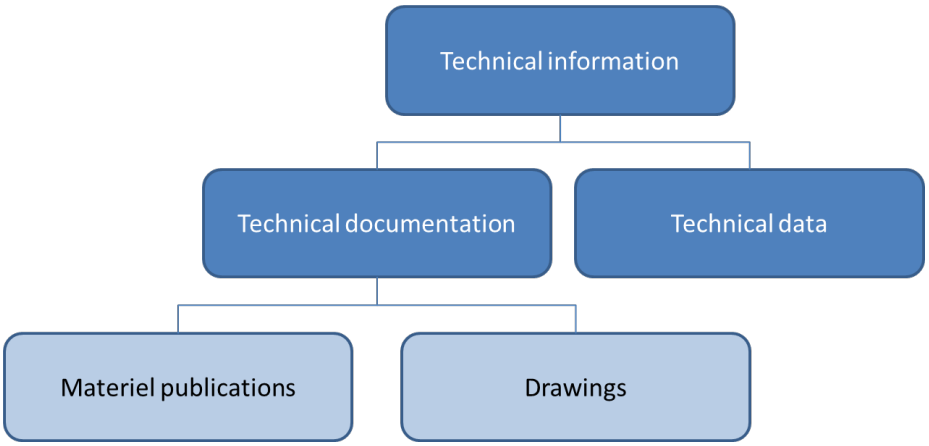


Figure 9.2 A simplified view of technical information at FMV.

Language for the materiel documentation is specified in the *System Objective* (SMS 2). In some areas there are regulatory requirements (EU law, Swedish legislation, Internal Swedish Armed Forces' Regulations (FIB) or design rules/technical rules of practice) that specify that safety instructions should be written in Swedish. Normally, all materiel documentation intended for the user should be in Swedish, while other technical documentation and technical data may be in English.

In some areas, such as the aviation area, English is the main language and translation into Swedish is not applicable. In cases where the technical personnel tasked with maintaining materiel, such as a helicopter or a road ambulance, have the required knowledge of technical English, English may be chosen as the language for the materiel documentation.

In cases where the manufacturer's instructions for use and maintenance instructions and warning labels such as signs and stickers are to be translated into Swedish, the manufacturer of the technical system is responsible for this translation. The System Safety Decision must state that the technical information constitutes a translation and from which language it is made. The foreign version of the text must be included in the supplied product documentation.

If the Swedish Armed Forces or FMV provide signs and stickers for safety markings to the manufacturer, it is the responsibility of the Swedish Armed Forces or FMV that these comply with Swedish legislation and that any text is correct.

9.3 Language of Technical Information for CE-marked Products

The manufacturer (the legal manufacturer) who CE marks a product must comply with Swedish legislation including EU Directives in the field. In connection with the CE marking, the manufacturer must create technical documentation for the product and issue a *Declaration of Conformity* (DoC). The technical documentation *(Technical file)* is compiled by the manufacturer and is intended solely for market surveillance authorities and not for the user of

the product. The technical documentation *(Technical file)* is a subset of the total design and manufacture documentation of the product and must be available in an EU language, such as English.

Both EU Regulations and EU Directives transferred to Swedish law, stipulate that documentation intended for the everyday user such as safety instructions and markings, as well as instructions for assembly, installation and daily maintenance by the user must be in one of the official languages (excluding minority languages) of the country where the product is to be used, i.e. Swedish. Maintenance instructions (service manual) for technical personnel are intended for those who will maintain, repair or calibrate the product. Technical personnel may exist within the manufacturer's own organisation or at another actor, for example the Swedish Armed Forces. Maintenance instructions should be in an EU language, such as English, which technical personnel are usually expected to understand.

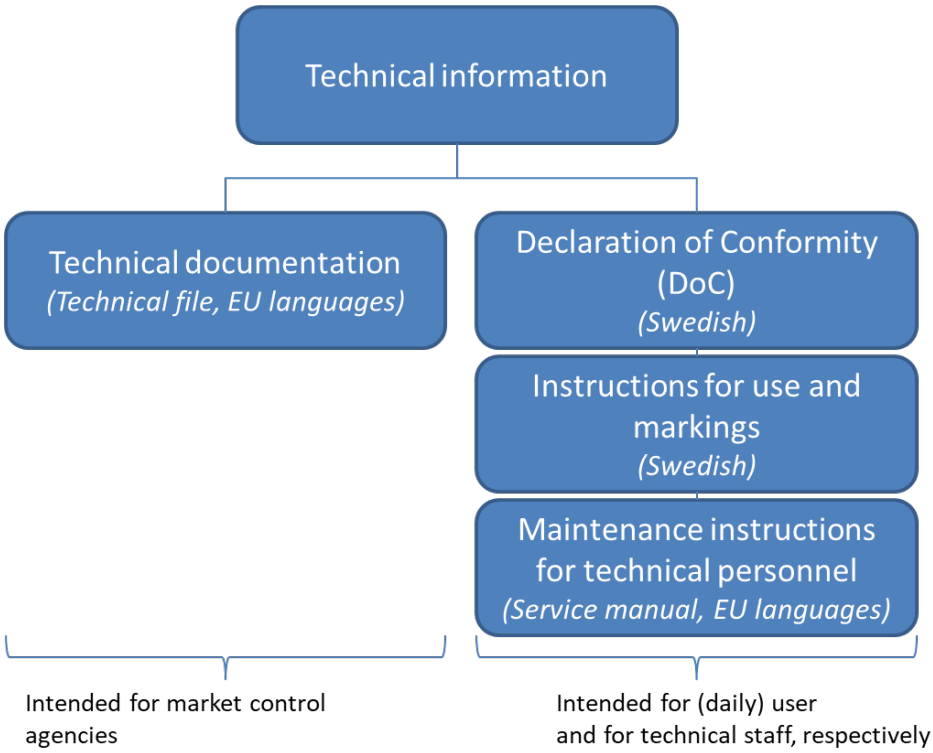


Figure 9.3 Technical information related to CE marking.

In the case of a CE-like process for products exempt from an EU Directive, and which are instead specifically designed for a specific military purpose, authorisations and other accounting documents may be written in the contracted language, preferably Swedish or English. Requirements for accepted languages for technical information are specified in the *System Objective* (SMS 2).

9.4 Languages under EU Regulation REACH

The EU Regulation REACH (*Registration, Evaluation, Authorisation and Restriction of Chemicals*) specifies that Safety Data Sheets for chemical products are to be provided in an official language of the Member State where the dangerous product is placed on the market. Therefore, Safety Data Sheets should be written in Swedish for chemical products placed on the Swedish market.

9.5 Languages in the Acquisition of MOTS

In the case of procurement of *Military Off the Shelf (*MOTS*)* products and in international cooperation with organisations or another State, approvals and other accounting documents may be written in the contracted language, preferably English. Requirements for accepted languages for technical information are specified in the *System Objective* (SMS 2).

9.6 Languages in Accounting and Decision Documents

System safety decisions such as *System Safety Declaration* (SSD), *System Safety Approval* (SSG) and *System Safety Announcement* (SSM) must be written in Swedish.

In export trades, system safety decisions and other system safety documentation are issued in the language agreed in contracts with the relevant state.

The manufacturer must write accounting and decision documents such as *System Safety Program Plan* (SSPP), *Safety Compliance Assessment* (SCA), *Safety Assessment Report* (SAR) and the *Risk log* (RL) in Swedish or in the language agreed in the contract. Other documents must be in Swedish or English, or in the language agreed in the contract.

10 Procurement of Technical Systems

The purpose of this chapter is to provide guidance on how system safety work can be adapted depending on legislation, categories of technical systems or products and whether these should be procured, re-acquired or changed (modified).

10.1 General Information on the Procurement of Technical Systems and Products

Based on EU law, Swedish legislation and the complexity, nature and risk content of the technical system, the scope of system safety work needs to be adapted.

All materiel that is to be included in a military unit or that is to be used in the Swedish Armed Forces' unit operations, needs to undergo well-balanced system safety work.

Standard products without exemption for military equipment, for example CE-marked products, which are procured for *other activities* and used in accordance with the manufacturer's instructions can be put into service without undergoing system safety work. Note, however, that all forms of co-function in another technical system need to be analysed from a system safety perspective.

Technical systems and products that are re-acquired and that are already registered in the Swedish Armed Forces' management system do not require renewed system safety work as long as they are used and maintained in accordance with previously issued system safety decisions. Please note, however, that if EU Directives or Harmonised Standards have been amended, a new *Declaration of Conformity* (DoC) is required. If serial production resumes, a new verification may be required.

10.2 Interfaces between Technical Systems and Facilities

Facilities are one of several different environments in which it should be possible to install, connect, store or use the technical system. Facilities as such must not be included in system safety decisions.

Facilities may, in addition to protection, also provide certain basic technical resources such as electricity, power, heating, cooling, ventilation, water and sewage to maintain both the function and safety of the equipment. The interfaces of facilities, alternatively with the basic resources included, against technical systems and products can be handled in different ways depending on how these are defined. The choice of model as below should be stated in the *System Objective* (SMS 2):

- Alternative 1:
  The requirements of the technical system for the **interfaces of basic technical resources**, as well as their performance and quality, must be included in the system safety decisions.
- Alternative 2:
  The technical system, together with the **basic technical resources** must be included in the system safety decisions.

The term *facilities* is sometimes applied to materiel, such as an arms caisson, which in this handbook is referred to as technical systems or products.

10.3 Construction of Technical Systems and Products

The architecture of the system solution identifies how a system-of-systems is most appropriately built up of different system elements (technical systems, subsystems, products and integration products).

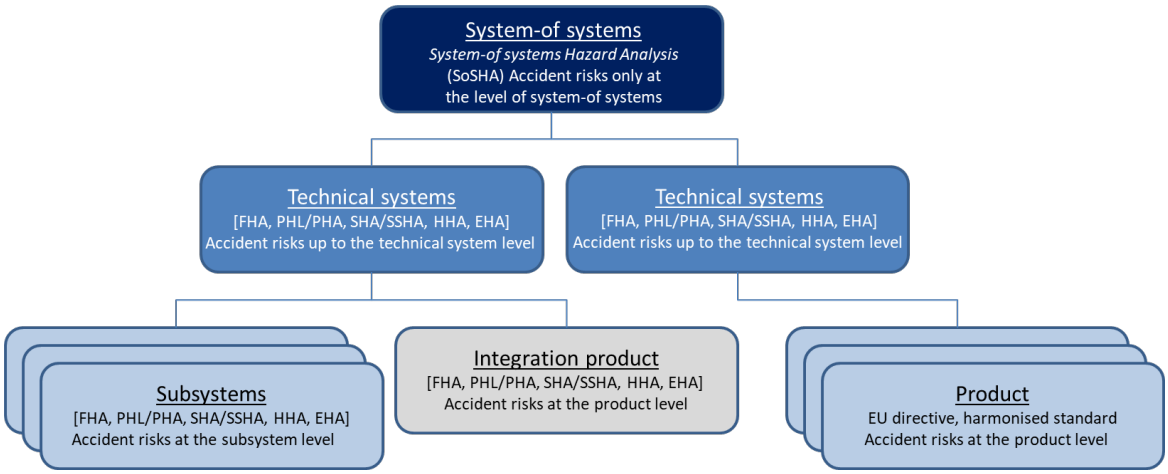


Figure 10.1 System-of-systems can consist of optional combinations of technical systems, subsystems, products and integration products.

The architecture of the system solution can also include specific system elements (subsystems, products or integration products) that can be handled in different ways from a system safety perspective.

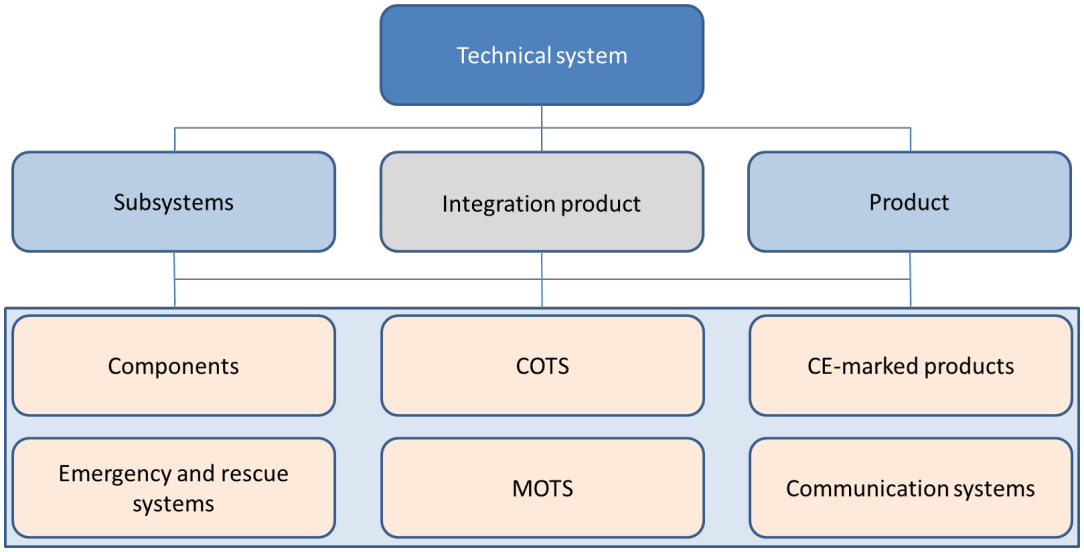


Figure 10.2 Examples of system elements that can be handled in a special order.

10.4 Different Categories of System Elements

Below are listed different categories of system elements for the construction of system-of-systems, technical systems and products. For each of these categories, the focus is given for the system safety work and how to reason about these.

10.4.1 Standard Products for Other Activities

Standard products procured for *other activities* such as offices, school and canteens as well as other types of staff quarters and used there in accordance with the manufacturer's operating instructions may be put into service without carrying out system safety work or decisions. The same applies to products without exemption for military equipment, which are used in, for example, workshops and hangars.

Note, however, that any form of collaboration in other technical systems that is outside the manufacturer's operating instructions needs to be analysed from a system safety perspective.

10.4.2 Spare Equipment

Products (spare equipment, replacement units) that are re-procured normally do not require any renewed system safety work unless the product is modified or other environmental requirements are specified.

10.4.3 Components

To this category belong components of civil or military origin. These components do not have their own function and may be adapted to be mounted. The components are meant to be assembled in a specific location, often in a platform to fulfil a specific purpose, but without the intention of being deployed as a single functional unit. Thus, the components (singly or in groups) cannot be used or function independently and these do not require any system safety work or system safety decisions.

Examples of components can be racks for radios, cable ducts and holders for loose equipment, but also include "meter goods" that are adapted to a custom length, such as wires, pipes and electrical cables.

10.4.4 Devices With or Without a Source of Risk

To this category of materiel belong simple products (trivial) that cannot be attributed to the previously presented categories. The products may have a single source of risk that is thus easy to understand with regard to system safety, or alternatively they are products that lack specific sources of risk.

It is the manufacturer's (or importer's) responsibility to ensure that the product complies with Swedish legislation and may be placed on the market. The products are intended to be used alone or together with other products based on the manufacturer's instructions for use. The intended use within the Swedish Armed Forces must not differ significantly from civil use.

If technical standards for design and verification are lacking, a less comprehensive, but well-balanced system safety effort needs to be carried out. In some cases, the *client* can already

indicate in the *Request for Proposal* (RFP) which accident risks the manufacturer is to analyse and in relation to these risks report what risk reducing measures have been taken.

For chemical products, a safety data sheet is sufficient.

Examples of materiel with or without a source of risk are articles for the soldier, thermos jugs and paint.

10.4.5 COTS Products

COTS (*Commercial off the shelf*) products include products that are already on the market and that may be approved by an accredited body against international standards.

It is the manufacturer's (or importer's) responsibility to ensure that the product complies with Swedish legislation and may be placed on the market. This category includes products that have been assigned different markings, such as wheel marking of marine equipment. However, a very large part consists of CE-marked products, which are dealt with in their own sections.

The products are intended to be used alone or together with other products based on the manufacturer's instructions for use. If the intended use within the Swedish Armed Forces deviates from the manufacturer's instructions, the use needs to undergo special system safety work.

The product must not be changed (modified). If the product is changed (modified) so that it no longer meets the essential requirements, the manufacturer's product safety and product liability become invalid and the certificate/marking (if applicable) of the accredited/Notified body is thus no longer valid.

If the product fits the above description, the system safety work can be reduced to checking that the accredited body, if it has participated in conformity assessment, is authorised for approval (certification) of the product in question and that the intended use within the Swedish Armed Forces fits within the approval, the manufacturer's instructions and any markings.

Examples of COTS products are wheel-marked products, whole vehicle type-approval of road vehicles and CIP-marked ammunition (hunting and sport shooting).

10.4.6 Emergency or Rescue Systems

This category includes safety products and systems used in emergency or rescue situations. These can be constantly active (monitoring is done with sensors and are activated automatically) or passive (activated by the user).

An emergency or rescue system can contain or generate large energies and can thus be relatively dangerous for the user if not used or handled properly. System safety work needs to demonstrate that the benefits of an emergency or rescue system are always greater than the consequences that may arise from its use, malfunction or in the event of an unsafe discharge. For emergency or rescue systems can under certain conditions, such as availability and performance, a higher tolerable level of risk be accepted than for the platform in question.

The design and performance of safety products are often governed by regulations. For example, a seat belt or airbag may cause some damage (hearing damage, impacts, etc.) when activated because its benefits in saving lives or avoiding serious personal injury outweigh hearing loss and bruising.

A life jacket must have certain characteristics regardless of the technical system in which it is included. The number of life jackets on board a ship or in an aircraft is governed by international regulations and therefore does not affect the safety architecture of the platform. Adding twice as many life jackets does not mean that a poorer seaworthiness of the ship can be accepted. Installing an effective fire extinguishing system also does not imply the allowance of more fires.

Examples of emergency or rescue systems are hand-held fire extinguishers, fire extinguishing systems, life jackets, lifeboats, airbags, seatbelt tensioners and seatbelt cutters.

10.4.7 CE-marked Products

CE-marked products include technical systems and products that have already been released on the market or have not yet been released on the market and where the Swedish Armed Forces will be the first user. The CE-marked product is most often used independently, which means that the manufacturer's operating instructions are followed regarding fastening, installation, power supply and connection to various technical and information systems.

10.4.7.1 The product is released on the open market ready for use

If the product is placed on the market and ready for use, it is the manufacturer's (or importer's) responsibility to ensure that the CE-marked product complies with current legislation and is correctly CE-marked to be put into service in Sweden.

The intended use within the Swedish Armed Forces must not differ from the manufacturer's stated (intended) mode of use. The product must not be changed (modified). If the product is changed (modified) so that it no longer meets the basic requirements or if its instructions for use are changed, the legal manufacturer's product safety and product liability becomes invalid and the CE marking is thus no longer valid.

If the product is CE-marked as above, the system safety work can be reduced to checking that the *Declaration of Conformity* (DoC) is complete and that EU Directives and Harmonised Standards are specified and applicable to the product. *The client* may need to ask which requirement levels have been used in the standards and review that these are sufficient for the procured product, for example regarding EMC requirements.

Furthermore, the presence of operating instructions in Swedish including CE marking and any other marking is checked and that the intended use within the Swedish Armed Forces fits within the CE marking.

If the CE-marked product requires a registration or certificate (other concepts may also occur) from a third-party body, such as a Notified body, it is audited that the person issuing the certificate is competent for the relevant product category and used test methods for verification and that the CE-marked product is covered by the certificate. Furthermore, the Harmonised Standards applied by the manufacturer and the third-party body in the

verification and whether they are deemed to be applicable for that purpose should be examined.

Where other standards, only parts of Harmonised Standards or repealed Harmonised Standards have been applied (as the presumption no longer exists), the examination should cover how the manufacturer has complied with the corresponding essential safety requirements in the EU Directives. In some cases, it may be desirable to also take part of the performed risk analysis that forms the basis for the CE marking.

In addition to operating instructions in Swedish and the *Declaration of Conformity* (DoC)*,* it must be possible to identify the manufacturer, importer, address, type designation and, if necessary, individual marking through a permanent marking (sign, engraving, casting) on the product.

The manufacturer's *Declaration of Conformity* (DoC) with references to EU Directives, standards and, where possible, parts of technical documentation *(Technical file),* must be annexed to the system safety decisions.

Examples of already CE-marked products are work machines, generators, pressure vessels, tailgate lifts, lifting devices, rubber boats, snowmobiles and telecom equipment.

10.4.7.2 The product is not yet released on the market

If the product has not yet been released on the open market and the Swedish Armed Forces become the first user, contractual requirements can be set for transparency in the manufacturer's system safety work and how it is to be carried out. However, it is the manufacturer's (or importer's) responsibility to ensure that the CE-marked product complies with current legislation and is correctly CE-marked to be put into service in Sweden.

The system safety work, including the CE marking, must be based on the Swedish Armed Forces' requirements for the operational environment and operational conditions (including technical performance). The military standards and the main Harmonised Standards to be applied are set out in the *Request for Proposal* (RFP).

The product must be CE-marked in accordance with all applicable EU Directives and this is done before delivery to the Swedish Armed Forces or FMV. If the Swedish Armed Forces have requirements in addition to the minimum requirements of the EU Directives in terms of basic health and safety, these must be stated in the *Request for Proposal* (RFP) and included in the CE marking. *The client* may request that these requirements also be verified separately and reported in a test report or in a *Safety Assessment Report* (SAR). The *client* checks that the set requirements are met.

EU Directives may require that the product and/or the manufacturer's quality system need an approval/certificate from a Notified body.

In cases where the EU Directives allow freedom to engage a third-party body or laboratory, any requirements for this need to be stated in the *Request for Proposal* (RFP). Such a body must be accredited for the relevant product category and for verification test methods.

The product must comply with Harmonised Standards giving presumption with requirements in the EU Directives. In cases where parts of Harmonised Standards, or military standards, for example, are used, the manufacturer must specifically disclose how the requirements of the EU Directives have been taken care of. In the absence of applicable standards, it may be necessary to combine requirements from different standards.

The client may specify that certain military standards should be followed. These standards often have higher or much higher safety and protection requirements compared to the corresponding Harmonised Standards. *The designer needs to compare the* requirements, and any differences in the level of requirements, between the standards and assess whether the requirements of the Harmonised Standards are met or whether additional testing and verification are required. Compliance with the requirements of the Harmonised Standards must be declared as part of the technical documentation *(Technical File)*.

In addition to operating instructions in Swedish and the *Declaration of Conformity* (DoC), it must be possible to identify the manufacturer, importer, address, type designation and, if necessary, individual marking through a permanent marking (sign, engraving, casting) on the product.

The manufacturer's *Declaration of Conformity* (DoC) with references to EU Directives, standards and technical documentation *(Technical file)* must be appended to the system safety decisions.

Examples of products that have been CE-marked with the Swedish Armed Forces as the first user are functional containers.

10.4.8 Products Undergoing a CE-like Process

The few technical systems and products that are exempted from a CE marking from a given EU Directive, can instead undergo a *CE-like process.* Note, however, that some EU Directives do not allow any exemptions to CE marking.

For example, products that have been procured from another state and that fall under classified information (defence secrecy) may mean that CE marking cannot or may not be carried out, for example for a signal protection device. Often, however, such products already meet more stringent requirements based on military standards.

Machines that are *specially designed and manufactured for military purposes* are exempted from CE marking and must (may not) not be CE-marked according to the current EU Machinery Directive. However, other EU Directives may be applicable in parallel and still require CE marking, such as the EMC Directive. A few additional exceptions may exist in other EU Directives, but they are defined in other ways. Note, however, if the product (or a similar product) can be of dual-use, i.e. can be used both civilly and militarily, then the military exemption cannot be invoked, and the product must be CE-marked.

The *CE-like process* means that the same process and requirements apply as for CE marking of products according to a certain EU Directive. The difference is that the product that follows the *CE-like process* must not (may) be CE-marked for this particular EU Directive.

For particularly risky products, there is also no certificate issued by a Notified body. However, the product may need to be CE-marked according to other EU Directives.

The *client* should in the *Request for Proposal* (RFP) require that certain methods and standards, including Harmonised Standards, be followed. Any requirements for the use of third-party bodies (accredited certification body or laboratory, other than Notified body) must be specifically stated. *The client* may also specify that certain military standards should be followed.

Examples of products where CE-like process can be applied are MOTS, radio equipment used exclusively by the Swedish Armed Forces and for certain additions on road vehicles.

The manufacturer does not have the right to modify a product solely to avoid CE marking.

10.4.9 Integration Products

To this category of materiel belongs civil and military products. These products can be integrated into other technical systems, often platforms, or can be used standalone. For integration products, system safety work is carried out and system safety decisions are issued.

Ammunition is always to be regarded as a stand-alone technical system while often being the integration product into one or more technical systems. For ammunition, system safety decisions must always be issued.

Examples of integration products can be ammunition, weapon stations, BT-46, adjustable dozer blade for working machinery and CE-marked power supply units.

10.4.10 Partly Newly Developed Technical Systems

A partly newly developed technical system can be characterised by the merging of existing known subsystems and products into a new technical system. Alternatively, a known basic design can be further developed with another alternatively with additional functionality or changed performance. Thus, there is knowledge and experience in subsystems and basic designs.

Previous system safety work and experience from use and maintenance can be relied upon, but needs to be reconsidered based on the new means of usage and the current requirements for system safety. Operational experience can show weaknesses in design and any safety deficiencies that need to be taken care of in the new technical system.

If older subsystems or basic designs are used, documentation and previous system safety work may be missing or incomplete for the new means of usage. In these cases, it is not enough to simply analyse the integration with other subsystems. System safety work may need to be carried out separately for the older subsystems or the basic design before the integration to the new technical system is analysed.

For the partly newly developed technical system, the legislation must be met, but exemptions for military equipment can be applied. For subsystems and basic designs, there are normally standards and *Design Rules* (DR) to follow. The system safety work must include the

integration between the different subsystems, as well as the new functionality and changed performance. Therefore, more comprehensive, but still well-balanced system safety work may need to be carried out on the new complete technical system.

Examples of partly newly developed technical systems are the Grenade Launcher Armoured Personnel Carrier 90 (*GRKPBV90).*

10.4.11 Newly Developed Technical Systems

A completely newly developed technical system is often preceded by both Research and Technology Development (R&T) and concept work when new technical solutions for technical systems or subsystems need to be developed.

The legislation must be complied with, but exemptions for military materiel may be applied. Technical standards and *Design Rules* (DR) may be missing or not fully applicable. Therefore, more extensive system safety work may need to be carried out.

Examples of newly developed technical systems are submarines (type Blekinge).

10.4.12 System-of-Systems

A system-of-systems refers to technical systems and products that each already have their own system safety decisions issued, but which in common behaviour create new capabilities and functions. This means that none of the technical systems are integrated into the other system, but that they only interact.

In system-of-systems, function is achieved, for example, by sharing or transferring available information from one system to another. These common information assets have an impact on the system safety of the cooperative system-of-systems as they affect the system containing the sources of risk. The integrity and accuracy of the information means that requirements definition must handle requirements at a certain level of criticality in the constituent subsystems. If the system safety-critical information assets cannot be kept separate from other functionalities, this requires a common requirements definition regarding the level of criticality of all constituent subsystems of any new system-of-systems.

In system safety work, the critical information assets must be identified so that failures in these do not lead to a hazardous event in the subsystem that constitutes the executive part.

System safety decisions for system-of-systems must cover the new accident risks arising in the common conduct. The constituent systems may need to be re-designed to manage accident risks that arise when the systems interact.

Examples of system-of-systems can be that a helicopter should be able to land on a ship or that a platform can act as a fire control site and provide information to a firing unit.

Another example is the command and control system that will convey fire missions to different gun groupings over a large grouping area where both the position of the protected object and the target as well as the time for joint effort become system safety critical information assets.

10.4.13 Communication Systems

This category includes systems in which interconnected products transmit information only in the form of spoken or written messages between people, without the information in turn being transmitted or used in another technical system, for example to control dangerous energies such as weapons or autonomous systems.

> Communication systems used to control or influence safety-critical technical systems belong to the category of system-of-systems.

The composite system consists of relatively simple products in terms of system safety. The products may be approved by another state (MOTS), parties (accredited bodies against international standards) or CE-marked by the manufacturer. It can also include products (COTS) that from a functional point of view lack a specific source of risk, such as cabling, connectors and holders.

From an information security perspective, a communication system can be a complex integrated system and consist of a variety of products, such as computers, monitors, speakers and printers. From a system safety perspective, the same system can be considered trivial where the products have no impact on system safety. From a system safety perspective, the interconnected system can be considered harmless, but at the same time from an information security perspective (safety) may need to be managed as a critical system.

For communication systems used to warn others, for example on board a ship, their reliability will be safety critical as failure to function in the long run can lead to serious consequences, for example if personnel do not escape from certain places in the event of a fire. Such accident risks are managed in the system-of-systems category.

Accident risks contained in the stand-alone MOTS, COTS and CE-marked products for communication are managed at the product level according to any of the categories above. These accident risks should therefore not be escalated to the category of communication systems.

Examples of communication systems are radio or wired systems for speech or text messages.

10.4.14 MOTS Products

Military off the shelf (MOTS) products *include technical systems, products and spare parts designed for special military purposes.* These are in use by at least one state and can thus be available to defence authorities.

For MOTS products where contracts are signed between states, such as *Foreign Military Sales* (FMS), or between defence authorities and other organisations, such as *the NATO Support and Procurement Agency* (NSPA), special conditions apply. The Swedish Armed Forces or FMV in the role of *client* must ensure that the MOTS product complies with Swedish legislation and can thus be placed on the market to be put into service by the Swedish Armed Forces.

For MOTS products where contracts have been signed between states, the intended use of the MOTS product within the Swedish Armed Forces may not differ from the instructions of the foreign defence authority. Neither may the MOTS product be changed (modified). If the MOTS product is changed (modified) or used otherwise than as directed by the foreign defence authority or previous purchases, their approval may expire.

For MOTS products where contracts have been signed between states, system safety work can be reduced to checking that Swedish legislation is met and that the intended use fits within the approval and is in accordance with the foreign defence authority's instructions. Furthermore, contact should be made with states that use the MOTS product. These states have already reviewed and approved the MOTS product as well as have operational experience. Traceable and credible operational experiences can be evaluated and invoked in system safety decisions.

Examples of MOTS products are Off-Road Vehicle 16 (contract with manufacturers), Helicopter 16 (FMS) and Camouflage Net (NSPA).

Anyone procuring a MOTS product must fully analyse the meaning and the extent of the approvals obtained from another State.

10.4.15 Training Systems and Training Materiel

Most technical systems and products are used in both training, exercises and operations. However, hazardous components can be exchanged for less dangerous ones in the live systems during training and exercises to reduce the consequences should an accident nevertheless occur. For example, blank or blind ammunition can be used in a weapon.

Training systems and training materiel procured for use solely in training and exercises must normally comply with the legislation without exemption for military equipment. This is because this materiel is not intended for certain military purposes and thus has no destructive effect. Training systems and training materiel can be attributed to several of the categories above such as CE-marked products or MOTS.

However, training systems and training materiel may need to be evaluated individually on a case-by-case basis if any exemptions for military materiel need to be used.

Training systems and training materiel must normally comply with legislation without exemption for military materiel.

If the purpose of the training is to teach proper handling, the training system or training materiel and the live system need to be fully compliant. In system safety, accident risks arising from the use of the live system as a result of the training system deviating from the live system in some context need to be managed. These accident risks can occur when the users, who have completed their training with the training system, manage the live system in a habitual and potentially incorrect way, which can lead to accidents. Differences between

training systems and training materiel and the live system are considered as potential contributors to accidents. This must always be investigated by *the client of the* training materiel.

If the purpose of the training is to teach tactical behaviour or data, design and function, then the training materiel from a system safety perspective does not have to reflect the real technical system purely in terms of handling. However, there must be no doubt for the user carrying out the training that the training materiel does not fully reflect the live system in terms of handling. Such training materiel is not considered to entail any accident risks in the live system as a result of incorrectly learned handling.

If the purpose involves some form of exercise in handling, training systems and training materiel can be divided into different categories. For each of the categories, the scope of system safety activities required for the system is proposed:

Type of training system or training materiel	Required system safety work	Examples of training materiel
The training materiel consists of the live system and is used in the same user environment as for the live environment, but its use is adapted for training.	A system safety analysis is carried out in accordance with the requirements of the Swedish Armed Forces. Accident risks associated with learning errors resulting from possible deviations from a live system must be identified and assessed in the system safety work.	Weapons with blanks, lose or practice ammunition. CBRN materiel with alternative or diluted active substances (agents).
Training materiel is used in a different user environment but contains the same functions and is subject to or control the same energies as its live counterpart.	Compliance with legislation through CE marking. In addition to the legislation, an initial assessment and documentation of possible accident risks associated with learning errors as a result of deviations from the operator environment of the live system is required. If such accident risks are identified, these must be managed in accordance with the system safety methodology.	Diving chamber Electric bridge layer

Type of training system or training materiel	Required system safety work	Examples of training materiel
The training materiel is used in a different user environment and contains only simulated functions equivalent to those found in the live system. The difference from the live system is that the energy is not generated by the function. However, the system can generate some energy to mimic the live system.	Compliance with legislation through CE marking. In addition to the legislation, an initial assessment and documentation of possible accident risks associated with learning errors as a result of deviations from the operator environment of the live system is required. If such accident risks are identified, these must be managed in accordance with the system safety methodology.	Driving training simulator g-force centrifuge Simulators of operator systems Dummy for cardiopulmonary resuscitation Ammunition effects that simulate live explosions Target towing equipment
Special cases, the training materiel does not match any of the above descriptions or is a combination of these.	Compliance with legislation. A system safety analysis is carried out in accordance with the requirements of the Swedish Armed Forces. Accident risks associated with learning errors due to deviations from the live system must be assessed in the system safety work.	Battle in built-up areas CBRN Indoor Training Facility

Table 10.1 Examples of the classification of training systems and training materiel.

The possible differences between training systems and training materiel and the live system needs to be taken into account in the system safety work.

10.5 Provided Materiel to Developing Industry

Government Furnished Equipment (GFE) refers to products that are already in the *Swedish Armed Forces' management system or otherwise provided by the Swedish Armed Forces or FMV*. It can be bulk materiel such as shovels, axes and crowbars, but also specific subsystems, such as appliances and other devices for assembly and integration.

The designer is responsible for the integration and functionality between the materiel provided and the technical system. *The designer* should also be responsible for ensuring that the technical system together with the materiel provided is safe to use. Note that in cases where *the designer* is not responsible for the whole design (technical system including provided equipment), the *client* becomes the integration manager from a system safety perspective.

The client who lends materiel, live or blanks, to *the designer* is also responsible for handing over the required system safety documentation for the materiel.

11 Route Selection Model

The purpose of this chapter is to explain the Route Selection Model (VVM) and to describe how requirements for ensuring a satisfactory level of safety and acceptance criteria can be imposed on this basis.

11.1 Description of the Route Selection Model

The *Route Selection Model* (VVM) is an iterative method that can be used both in the procurement and in change (modification) of technical systems and products. It is used when determining requirements to allow, target and limit different route choices. During design and integration work, the permissible route choices regarding the possibilities of meeting acceptance criteria for them are tested. During the system safety evaluation, arguments and evidence are verified to confirm compliance with the system safety requirements.

The first moment when the VVM is used is when the Swedish Armed Forces start work on *System Objective* (SMS). *The Route Selection Model* (VVM) is used by various actors during the different life cycle events.

The Route Selection Model (VVM) is applied to all materiel with or without exemption of military materiel. It also demonstrates how military materiel can be credited with compliance with legislation, standards and *Design Rules* (DR) as well as approvals by another party or state.

The *Route Selection Model* (VVM) is applied to both technical systems, subsystems and products and to individual accident risks. This can be done, for example, through a whole vehicle type-approval (CoC) for a truck (technical system) or through a *Declaration of Conformity* (DoC) for a CE-marked pressure vessel (component) integrated into a technical system. Further, individual accident risks can be managed such as barrel explosion (technical flaws) or misdirection of weapons (human mishandling).

The technical system needs to be broken down into an appropriate system structure with a sufficient level of detail to apply the different route selections.

> The Route Selection Model (VVM) is applied to both technical systems and components as well as for individual accident risks.

The Route Selection Model (VVM) includes the following Route Selections (VV):

- Route Selection 1 - Constitutional requirements
- Route Selection 2 - Approved by another State
- Route Selection 3 - Approved by another party
- Route Selection 4 - Other standards
- Route Selection 5 - Design Rules
- Route Selection 6 - Proven system
- Route Selection 7 - Risk matrices

The route selections are normally tested in numerical order, i.e., VV1 before VV2, before VV3. Sometimes a combination of route selections may be necessary, such as VV1, VV4 and VV5 to demonstrate a satisfactory level of safety together. For accident risks that have not been managed in previous route selections, Route Selection (VV7) is applied.

If military materiel exemptions are used, more route selections may be required in the *Route Selection Model* (VVM) in order to demonstrate a satisfactory level of safety.

Route Selection (VV1) is always applied because the constitutional requirements must always be met. Route Selection (VV1) includes, for example, CE marking. If Route Selection (VV1) is not sufficient to ensure the satisfactory level of safety of the technical system or product, then proceed to Route Selections (VV2 - VV6). If there are accident risks that could not be handled in these route selections, proceed to Route Selection (VV7) with assessment against risk matrices.

The system safety evaluation constitutes the overall result and consists of arguments and evidence from the different route selections and which, together with a position, are presented in the current system safety decision.

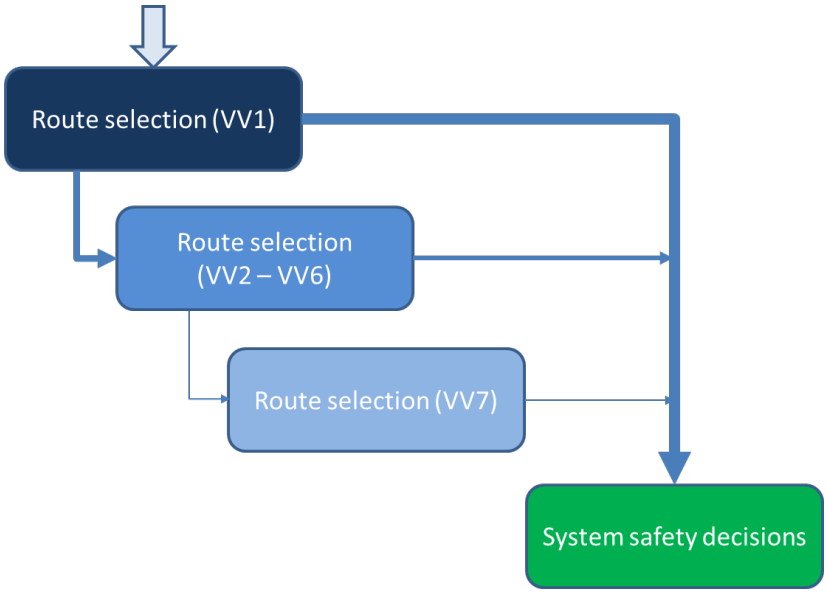


Figure 11.1 Principled application of the Route Selection Model (RMS).

11.2 Description of the Different Route Selections

The purpose of this section is to describe, based on the different route selections, how these can be applied to requirements in *System Objective* (SMS) and *Request for Proposal* (RFP).

The System Objective (SMS) sets out the focus and acceptance criteria for the permitted route selection. The Request for Proposal (RFP) spells out requirements and acceptance criteria for the different route selections.

11.2.1 Route Selection 1 - Constitutional Requirements

The purpose of Route Selection (VV1) is to ensure that technical systems and products can meet the constitutional requirements.

Constitutional requirements refer to EU law and Swedish legislation with its ordinances and regulations. This also includes the Harmonised Standards which, when their more detailed requirements are met, are presumed to meet the corresponding requirements of the Constitutions.

Constructing a product directly against the basic requirements of an EU Directive is very demanding and cannot in practice be implemented as the requirements are too general. From a system safety perspective, the Harmonised Standards of EU Directives are therefore considered important and, in principle, absolutely necessary to comply with. In the absence of Harmonised Standards, other established international standards may be used, however (NB) without the presumption principle being applicable.

Some constitutions include *General Advice* (GA) on how something can or should be carried out. However, these are not compelling but indicate the appropriate mode of work or interpretation.

Route Selection (VV1) is about opening to, alternatively determining, whether the technical system or product should be:

- Military materiel (MOTS)
- Materiel with a civil or military background *without* the exemption of certain military materiel
- Materiel with a civil or military background *with* the exemption of certain military materiel

The intended technical system or product must fall within the framework of current legislation. This also applies to military materiel.

For certain materiel, such as road vehicles specifically designed and manufactured for certain military purposes, the Swedish Armed Forces have a legal right within the space provided by law. For other technical systems and products, for example in the case of machinery, the Swedish Armed Forces have interpretive precedence as to whether these technical systems or products can be considered *military materiel or military materiel specially designed and manufactured for a particular military purpose*. If the Swedish Armed Forces do not use its interpretive precedence, materiel without military exemption is primarily procured.

The Swedish Armed Forces have interpretive precedence regarding the possibility to use exceptions in the legislation for military materiel and for materiel which is specially designed and manufactured for certain military purpose(s). *The client* has always better right than *the designer* to interpret the legislation.

For many technical systems and products, the civil regulatory requirements for safety and protection may be considered sufficient if the intended use is provided within the manufacturer's operating instructions and maintenance regulations. This may also apply to subsystems and components that are later assembled into military materiel. For example, all or part(s) of the technical system(s) may be subject to CE marking requirements, such as the EU's Electromagnetic Compatibility Directive (EMCD) and the Machinery Directive (MD) or wheel marking.

Compliance with the technical requirements of the legislation for technical systems and products must be sought, for example by means of CE or wheel marking. For materiel that may have an exemption to, for example, the CE marking, a satisfactory level of safety can be achieved in alternative ways. This can be done, for example, by complying with the regulatory framework's technical requirements including risk analysis and Harmonised Standards, as far as possible, even if formal labelling of the product is not carried out. In this handbook, this is termed a *CE-like process*.

For certain types of technical systems and products, specific decisions or certificates from authorities outside the Swedish Armed Forces may be required to bring the systems into service. For example, approval may be required from:

- The Swedish Civil Contingencies Agency (MSB) regarding the classification of explosives
- The Swedish Radiation Safety Authority (SSM) for the use of radiation sources
- The Swedish Environmental Protection Agency (NV) for the use of depleted uranium
- The Swedish Food Agency (LMV) for veterinary certificates for the handling of foodstuffs
- The Swedish Delegation for the International Law Review of Weapons Projects

The *System Objective* (SMS 2) should list the approvals needed to enable the technical system or product to be put into service. *The Request for Proposal* (RFP) must require the approvals for which *the designer* is responsible.

For remaining accident risks not dealt with by the constitutional requirements of Route Selection (VV1), Route Selection (VV2) must primarily be tested.

11.2.2 Route Selection 2 - Approved by Another State

The purpose of Route Selection (VV2) is to ensure that technical systems and products already approved by another State can also meet the Armed requirements for satisfactory level of safety for their intended use.

Approval issued by another State refers primarily to a foreign defence authority. If another State has approved (or equivalently designated) the technical system, a system safety report or other corresponding system safety documentation should also be called for.

Note, however, that normally only one defence authority, such as the Swedish Armed Forces or FMV, can procure technical systems from a foreign defence authority.

System safety work from another state should have followed an established system safety standard such as MIL-STD-882 or DEF STAN 00-056. Whoever procures technical systems or products from another State must fully analyse the meaning and extent of the approvals on which the system safety evaluation intends to support. The review also involves ensuring that the approval is correct and accommodates the intended use of the Swedish Armed Forces.

In the *System Objective* (SMS 2), there should be a list of which states whose approvals can be accepted. From the State from which the procurement takes place, access to the system safety documentation on which the authorisation is based should be requested.

For remaining accident risks not taken care of by the constitutional requirements of Route Selection (VV1) and through the approval of another State in Route Selection (VV2), in the first instance, Route Selection (VV3) must be tested.

11.2.3 Route Selection 3 - Approved by Another Party

The purpose of Route Selection (VV3) is to ensure that technical systems and products already approved by another party can also meet the Swedish Armed Forces´ requirements for satisfactory level of safety for the intended use of the technical system and products.

Another Party refers to civil authorities, notifiable bodies, certification and verification bodies and other bodies for validation and verification.

Civil authorities may approve certain types of technical systems, such as aviation authorities (FAA in the United States and EASA in Europe) for aircraft. These agencies certify aircraft and issue certificates of airworthiness.

A classification body or classification society is an organisation that handles classification of ships, among other things. Classification bodies develop rules for the characteristics of ships and other marine installations from a system safety perspective and can then carry out inspections to ensure that the installation meets the required requirements. The inspections may relate to technical design but also maintenance procedures and the quality level of shipyard work performed. The classification bodies are members of the international trade association *International Association of Classification Societies* (IACS).

Accreditation by laboratories, certification and verification bodies means that the activities they undertake for assessing conformity to various standards, have been reviewed and approved. Accreditation involves verification that operations are performed objectively, correctly and based on internationally recognised standards.

A body may be accredited for one or more types of inspections, a certification body for certain standards or certain products, and a laboratory for a number of specific methods. It is therefore important to check hat the accreditation applies to. Each accreditation mark is unique and contains the designation of the standard to which the accreditation applies, along

with the body's accreditation number. In Sweden, only bodies accredited by Swedac are allowed to use the accreditation mark.

Figure 11.2 Accreditation mark for bodies accredited by Swedac.

In some areas, accreditation is mandatory. A company engaged in vehicle inspection must be accredited. In other fields, for example for medical laboratories, accreditation is voluntary and serves as a stamp of quality. It is therefore important to check whether accreditation in the current field is compulsory or voluntary.

In the *System Objective* (SMS 2), there should be a list of which approvals from other parties that can be accepted. In *Request for Proposal* (RFP) requirements must be set for access to the standards that the approval is based on.

For remaining accident risks not taken care of by the constitutional requirements of Route Selection (VV1), through approval of another state in Route Selection (VV2) and/or a third party in Route Selection (VV3), Route Selection (VV4) must primarily be tested.

11.2.4 Route Selection 4 - Other Standards

The purpose of Route Selection (VV4) is to ensure that technical systems and products, which comply with industry standards or standards linked to international organisations, meet the Swedish Armed Forces´ requirements for satisfactory level of safety for their intended use.

Industry standards mean established and internationally applied standards as well as *General Councils* (GC) within the scope. Standards linked to international organisations are primarily those aimed at enabling interoperability, such as NATO, by specifying common system safety requirements or areas affecting system safety.

In development, the *System Objective* (SMS 2) may contain requirements stating compliance with specific civil and/or military standards in order to meet certain basic requirements such as interoperability, technology coordination, operational reliability or compatibility with general logistics systems. These standards are not normally system safety related, but may, however, provide arguments and evidence for system safety work.

There are specific system safety-related standards that specify both administrative aspects as well as design methodology in order to achieve a certain level of system safety. The use of established system safety-related industry standards, which do not form the basis for example CE marking or wheel marking, may provide conditions for evaluating measures and assessing them from a system safety point of view as these may be considered to be proven and

generally accepted. Verification criteria in the standard used must always be met in order to later be invoked in the system safety evaluation.

In *System Objective* (SMS 2), there should be a list of which other standards that can be accepted. In *Request for Proposal* (RFP) requirements must be set for access to the standards that the approval is based on. The equivalent also applies to standards linked to international organisations aimed at interoperability.

Established System Safety Standards for System Safety Operations refer to for example, MIL-STD-882, DEF STAN 00-056, GEIA-STD-0010 and ISO 12100.
Established technical standards refer to, for example, SS-EN 61508; SS-EN ISO 13849 and DO 178C.

For remaining accident risks not taken care of by the constitutional requirements of Route Selection (VV1), through approval of another state in Route Selection (VV2) and/or a third party in Route Selection (VV3), Route Selection (VV4), primarily Route Selection (VV5) must be tested.

11.2.5 Route Selection 5 - Design Rules

The purpose of Route Selection (VV5) is to ensure that technical systems and products that comply with *Design Rules* (DR) meet the Swedish Armed Forces' requirements for satisfactory level of safety for their intended use.

Design Rules (DR) may refer to the Swedish Armed Forces´ Internal Regulations (FIB), Swedish Armed Forces´ *Design Rules* (DR) and FMV *Design Rules* (DR) and handbooks (design rule collections).

Design Rules (DRs) exist where legislation and standards are inadequate or where experience with safe designs exists with similar technical systems. *Design rules* (DRs) deal with how previously known accident risks can be avoided or reduced by a certain design or requirements for principles for such design. The purpose is to specify, for proven technology, an appropriate way to prevent or reduce the effects of known accident hazards by design or requirements for the design characteristics.

In *System Objective* (SMS 2), there may be a selected list, for the technical system or product, of the Swedish Armed Forces´ FIB/DR and/or FMV *Design Rules* (DRs) and handbooks (design rule collections). In the *Request for Proposal (RFP),* requirements can be made based on the Swedish Armed Forces´ FIB/DR and/or FMV *Design Rules* (DRs) and handbooks (design rule collections).

For ammunition, Route Selection (VV5) must always be applied. This means that the requirements stated in the Weapons and Ammunition Safety Handbook must be applied and advice must be collected from FMV's Advisory Groups. If necessary, Route Selection (VV7) is also applied.

For remaining accident risks not taken care of by the constitutional requirements of Route Selection (VV1), through approval of another state in Route Selection (VV2) and/or a third party in Route Selection (VV3), Route Selection (VV4) and/or *Design Regulations* (DR) in Route Selection (VV5), Route Selection (VV6) must primarily be tested.

11.2.6 Route Selection 6 - Proven System

The purpose of Route Selection (VV6) is to describe criteria for invoking credible and traceable operating experience for a proven system.

Operating experience from a proven system refers to use and maintenance in the Swedish Armed Forces. Previous use must be relevant for the future intended use in the corresponding user environments. This means multi-year regular use that has generated many hours of operation so that credible and traceable operating experience (Proven-In-Use) exists.

It also includes analysis of accident and incident reports, as well as operational and failure follow-up. Suggestion activities and user experiences regarding safety during use and maintenance can also provide valuable information about possible safety deficiencies in the technical system or product. Aspects such as changed manner of use (slippage of norms), changing maintenance intervals or that preventive and corrective maintenance has not been carried out as directed, need to be taken into account.

In order to be able to invoke the operating experience of a proven system, the original documentation, which once as used to approve the materiel for usage may be required. With this documentation as a basis and operating experience, the technical system, a certain subsystem or the product can be handled as a proven system.

In *the Request for Proposal* (RFP), there may be criteria for credible and traceable operating experience as well as demands for access to the documentation used in the analysis work.

For remaining accident risks not taken care of by the constitutional requirements of Route Selection (VV1), through approval of another state in Route Selection (VV2) and/or a third party in Route Selection (VV3), Route Selection (VV4) and/or *Design Rules* (DRs) in Route Selection (VV5) and on the basis of operating experience in Route Selection (VV6), a new design solution is primarily to be tested. If the new system safety design solution cannot also be shown to achieve a satisfactory level of safety through the application of Route Selection (VV1 – VV6), Route Selection (VV7) must be applied.

11.2.6.1 Experiential Assessments

Criteria for the Risk Assessment for Route Selection (VV6) *Proven System,* are on operating experience (Proven-In-Use) originating, for example, in accidents and incidents involving the same technical systems and products. This experience data is required to be credible and traceable over an extended period of time. Experience data can be used from the same technical systems in use or from decommissioned systems. Other States' experience data can also be used if corresponding usage environments and operating conditions can be demonstrated. Experiential estimates are therefore regarded as a qualitative method.

A simple approach to identifying accident risks for new technical systems is to draw on lessons learned from similar technical systems and products; however, it is often difficult to

claim similar operating conditions. Transforming and adapting such data for risk assessments is basically impossible to make true and credible.

> Anyone wishing to make a risk assessment based on operating experience (Proven-In-Use) must carefully justify why the comparison can be made.

11.2.7 Route Selection 7 - Risk Matrices

The purpose of Route Selection (VV7) is to describe criteria for using system safety analysis assess whether the remaining individual accident risks are contained within the *Tolerable Risk Level* (TR) expressed in a risk matrix. Risk matrices can be both qualitative and quantitative.

The use of risk matrices is the final step in the *Route Selection Model* (VVM). Where other Route Selections (VV1 – VV6), or combinations thereof, are not deemed sufficient or applicable to demonstrate a satisfactory level of safety, Route Selection (VV7) may be applied.

A quantitative risk matrix can be used for accident risks with foreseeable causation and reliable numerical data (collected or estimated). In other cases, a qualitative risk matrix is applied.

The risk assessment methods below may be used individually or in combination. Regardless of the methodology, facts and estimates made must be justified and documented in order to be relied upon in risk assessment.

> All risk evaluations are predictions of the future. They do not constitute truths and assessments expressed by numbers are still just predictions. A model is always an attempt at imaging the real technical system from selected aspects.

11.2.7.1 Expert Assessments

Expert assessments are used in the context of qualitative risk matrix to prove that accident risks are considered tolerable. Risk assessments for Route Selection (VV7), based on expert assessments, is a method that means that one or preferably more persons with in-depth knowledge of the characteristics of the technical system and its use make a qualitative risk assessment. Expert assessments can be used as arguments to evaluate accident risks that have simple correlations and courses of events in order for an accident to occur. Examples of techniques and methods suitable for qualitative assessments include the behaviour of the technical system in case of single failure.

Expert assessments tend to become relatively person-dependent and may be considered valid in a certain period of time and in a certain context. Therefore, if there are shortcomings in the documentation, expert assessments are judged to be difficult to obtain traceable in order to repeat the risk assessment in the future. Another negative aspect may be that the risk

assessment is copied from other similar technical systems, without first critically examining whether these assessments are relevant to the new technical system.

To support expert assessments, qualitative fault tree models and/or event tree models can be used.

11.2.7.2 Modelling

Expert assessments are used in the context of qualitative risk matrix to prove that accident risks are considered tolerable. Risk assessments for Route Selection (VV7) based on probability calculations may, for example, imply that the current technical system is illustrated in a fault tree model where the base events are given numeric values. These numeric values can be derived from the manufacturer's product information, from experience values and they can be estimated values. Calculations are therefore regarded as a quantitative method.

Modelling can become complex and obscure for larger systems and requires knowledge of the internal relationships and interactions of constituent components and subsystems. In addition, uncertainty may increase in combination with an uncertain operating profile. Despite this, sometimes the values are nevertheless given too much trust.

All models are by definition incomplete because they focus only on the identified dependencies. Models can only be used as support for the evidence to make arguments stronger in the assessment of risk.

11.3 Stance, Argument and Evidence

During the design or integration work, the possibilities of fulfilling the acceptance criteria for the permitted Route Selections (VV1 – VV6) for the intended technical system, or for its constituent components are examined. Possible arguments and evidence are identified in order to demonstrate successively during the design or integration work that all or part of the technical system meets the system safety requirements set. If, for certain individual accident risks, compliance with the Route Selections (VV1 – VV6) cannot be shown, the Route Selection (VV7) applies.

In the System Safety Decision, the position must demonstrate that a satisfactory level of safety of the technical system has been achieved. In the work on the system safety evaluation, arguments should be presented detailing why the technical design is safe based on given conditions.

Arguments are one, but often several, assertions made in order for the technical system to be considered to comply with laws as well as system safety requirements. The arguments must be substantiated as far as possible with evidence.

Evidence on the one hand be empirical and on the other hand consist of other data of a stronger or weaker nature that fully or partly substantiates different arguments. Several different pieces of evidence can be brought together to substantiate a particular argument.

The arguments are assessed on the one hand on whether the evidence on which the arguments are based are sustainable and on the other hand whether the evidence is relevant. If the

evidence is durable and relevant, the argument is valid. Review of arguments is to find invalid or weak arguments and remove these so only valid arguments remain in the system safety evaluation.

In English-language contexts, a reasoning with a position, argument and evidence is often referred to as the *Safety Case*.

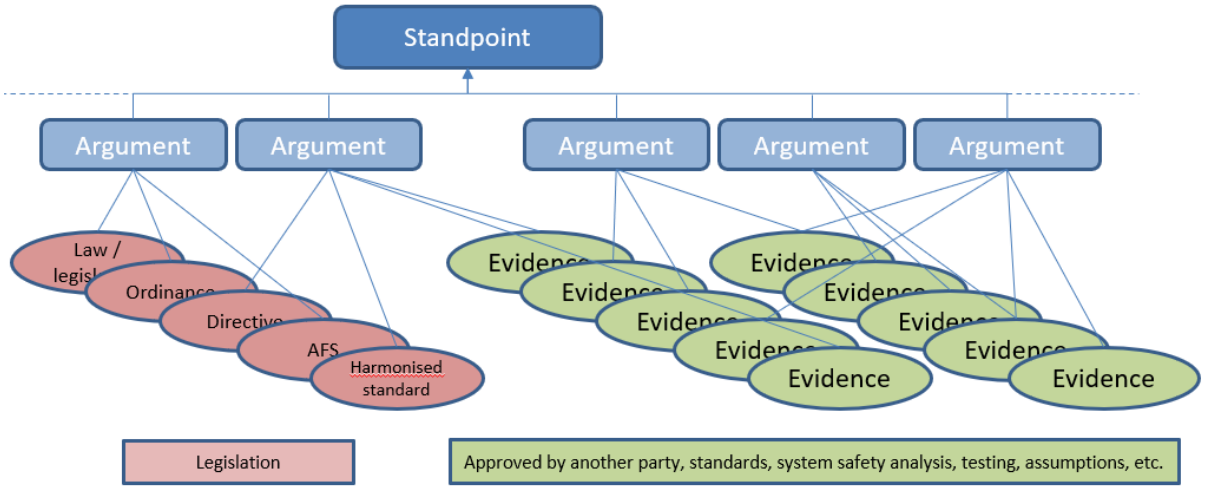


Figure 11.3 The position in the system safety decision is built up by arguments and evidence.

12 Selection of System Safety Activities

The purpose of this chapter is to describe how the choice of system safety activities can be made based on current technical systems, legislation, other regulations, experiences and taking into account the different actors and their roles.

12.1 Basics for Adapting System Safety Activities

System safety activities are carried out during all the life cycle periods of a technical system. For some technical systems and products, there is detailed legislation to protect against ill health and accidents. For other technical systems, there may be a need for specific system safety work if legislation and other regulations lack detailed and verifiable requirements.

For products that are audited and verified/approved via another procedure, such as CE marking or wheel marking, this can take care of parts of the system safety work.

System safety work consists partly of mandatory activities and partly of activities for selective parts based on the technical system at hand. The need for activities beyond the mandatory ones can be difficult to predict before the contractual *System Safety Program Plan* (SSPP) is agreed and the design work begins. Selective activities can be added or removed during design work. All activities may, if necessary, be adapted based on the current technical system or on the basis of the magnitude of the change (modification).

The mandatory activities are always carried out for all technical systems and products. Selective activities may, for example, be required to demonstrate how a satisfactory level of safety has been achieved. Selective activities may be replaced by other equivalent activities or, upon conscious decision, be opted out.

12.2 Motives for Adapting System Safety Work

In order to adapt the system safety work required by an actor in a certain role, the technical system in question needs to be delimited and risk content identified. The adaptation of system safety work through the choice of activities takes place after a combination of several different factors as shown below.

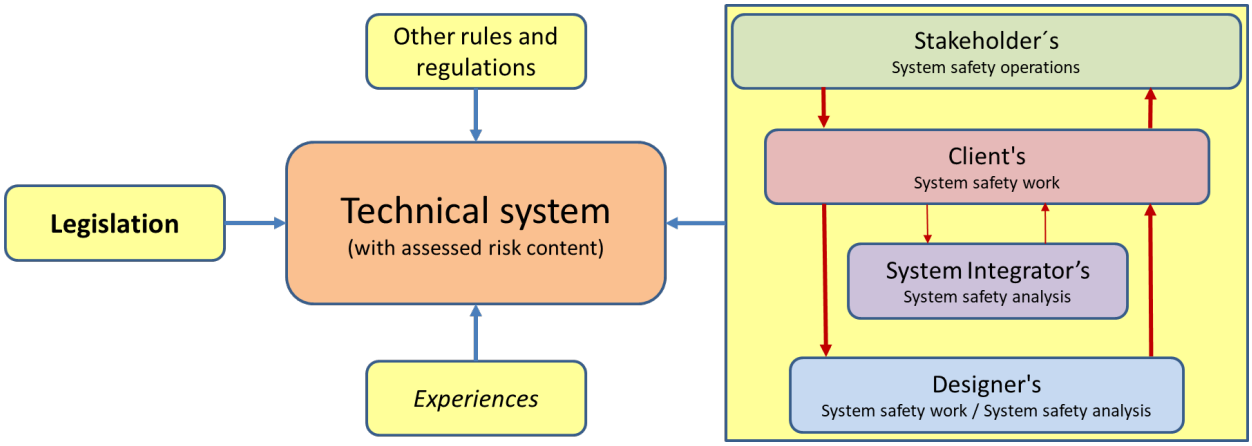


Figure 12.1 The scope of the system safety work needs to be adapted based on various factors and the role of the actor.

12.2.1 The Framework of, and Determining the Category, of the Technical System

In order to adapt the system safety work, the current technical system needs to be framed in and its interfaces defined. A focus is also required in *the System Objective* (SMS 2) if the technical system should be without or allowed to be with the exemption of military equipment. After that, to which category or categories the technical system and its included products belongs is determined. See *Chapter 10 Procurement of technical systems*.

12.2.2 Legislation, Other Regulations and Experience

Compliance with EU law, Swedish legislation, application of other regulations and approach to experience in order to achieve a satisfactory level of safety is stated in Chapter 11 *The Route Selection Model*.

12.2.3 Actors and Roles

The scope and depth of system safety work varies for the different roles. Note that an activity that is mandatory for one role may be subject to optional selection for another role.

The stakeholder leads the system safety activities for the technical system during all its life cycle periods. *The stakeholder* sets requirements for and focuses the system safety work that the *client* is to carry out. *The client* in turn, sets requirements for and focuses *the designer's* and *system integrator's* system safety work and system safety analyses, as well as requirements for the system safety documentation. *The designer and system integrator* may add more activities than those set by the client.

The system integrator has a design responsibility similar to that of the *designer*, but the responsibility is limited as long as it involves creating new capabilities and functionalities through co-operation without the constituent systems being combined or redesigns being carried out. *The system integrator* ensures that the physical interfaces fit together, that software can exchange information and that the technical systems do not affect each other, for example regarding electromagnetic compatibility (EMC). If the included systems are integrated, this actor may be considered a manufacturer under the following EU Directives. Any reconstructions are therefore always carried out by a *designer*.

12.3 Map of System Safety Activities

The system safety activities that are mostly based on the standard MIL-STD-882E, are divided into five different sections. For each section there are both mandatory activities to be carried out and activities for optional selection. Optional selection activities can sometimes be replaced by activities in other standards or by equivalent intra-stakeholder activities.

Activities are divided into the following sections:

- SECTION 100 Planning/Control
- SECTION 200 Analyses
- SECTION 300 Evaluation
- SECTION 400 Verification
- SECTION 500 Decisions

Below is shown how the activities in the different sections in general interact. Several of the activities interact with additional activities, as shown under the respective activity description in Appendix 3. Only the most essential couplings have been included in the figure below.

For example, the *System Safety Management Plan* (SSMP) can regulate more activities in sections 100, 300 and 500. *The System Safety Program Plan* (SSPP) can regulate most of the activities in sections 200, 300, 400 as well as some of the activities in sections 100 and 500.

The figure below also illustrates to some extent the time aspect. The first *System Safety Program* (SSP) activity is at the top left, and the last *System Safety Approval* (SSG) activity is at the *bottom right.* See *Appendix 3*.

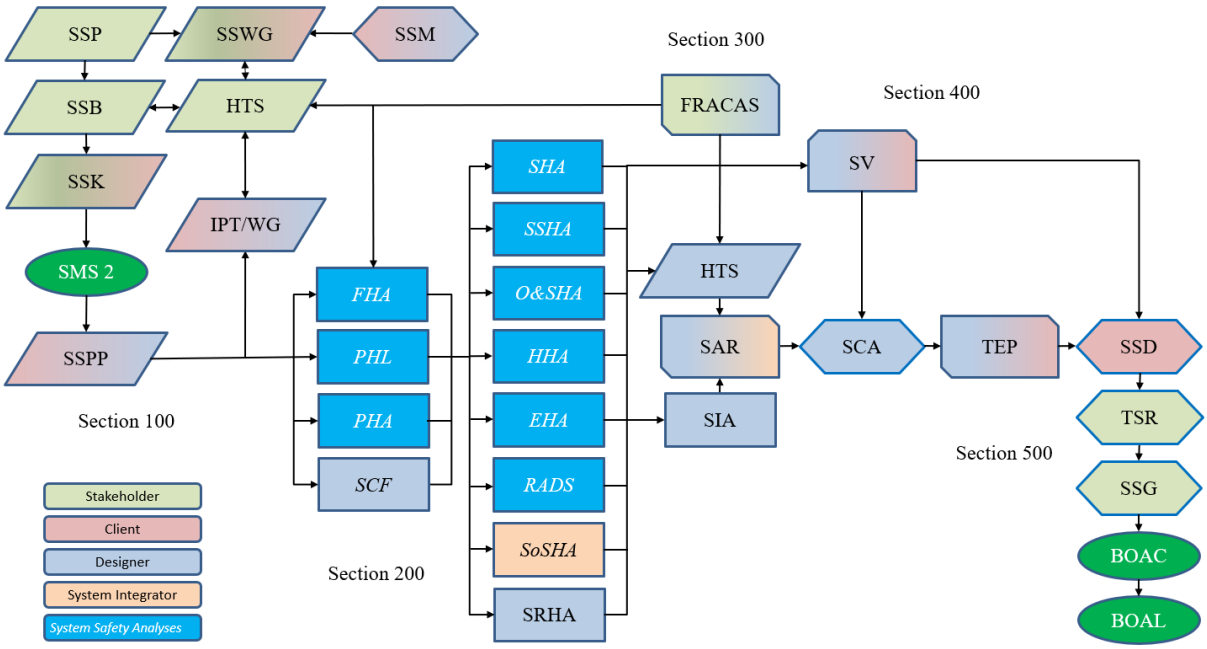


Figure 12.2 The most important links between different system safety activities from the perspective of the stakeholder.

12.4 Adaptation of System Safety Work

Several of the system safety activities can be carried out by different actors in their roles as *stakeholder*, *client*, *system integrator* and *designer*. The activities can therefore recur several times during the life cycle and be carried out with different scope and depth. Common to the actors is that the adaptation of the system safety work needs to be carried out based on the current technical system or the scope of the change (modification). Furthermore, the different activities may need to be adapted based on possible choices in the *Route Selection Model* (VVM).

For certain categories of technical systems and products, many different activities are required. For other technical systems, the selectively chosen activities can be merged or, upon conscious decision, opted out from. For example, when adapting activities, other methods can be applied or a different format for reporting can be used than those specified in the activity descriptions. Some reports can be merged or the information can be inserted into other reports.

System safety analysis activities can sometimes be merged into a fewer number of activities. However, the results of the system safety analyses must reflect all aspects that the various separate activities intend to take care of. For example, the health-related activity (HHA) and the environmental- related (EHA) can be coordinated. The activities selected must be documented in the *System Safety Program Plan* (SSPP). If the activities are adapted (simplified) compared to the activity descriptions, these also need to be described in the *System Safety Program Plan* (SSPP).

12.4.1 The Actor's Mandatory System Safety Activities

The Swedish Armed Forces in their role as *stakeholder* carry out a number of mandatory system safety activities, which in turn control or focus the *client's*, *designer's*, and/or *system integrator's* system safety work and system safety analyses.

The client, *designer* and/or *system integrator* carry out a number of mandatory system safety activities. In addition to the mandatory ones, selectively chosen activities can be carried out as a basis for the system safety evaluation.

Below are presented the system safety activities that are normally mandatory when procuring technical systems or during change (modification).

12.4.2 The Stakeholder's Mandatory System Safety Activities

The Swedish Armed Forces in their role as *stakeholder* carry out the following mandatory system safety activities during the different life cycle stages of a technical system.

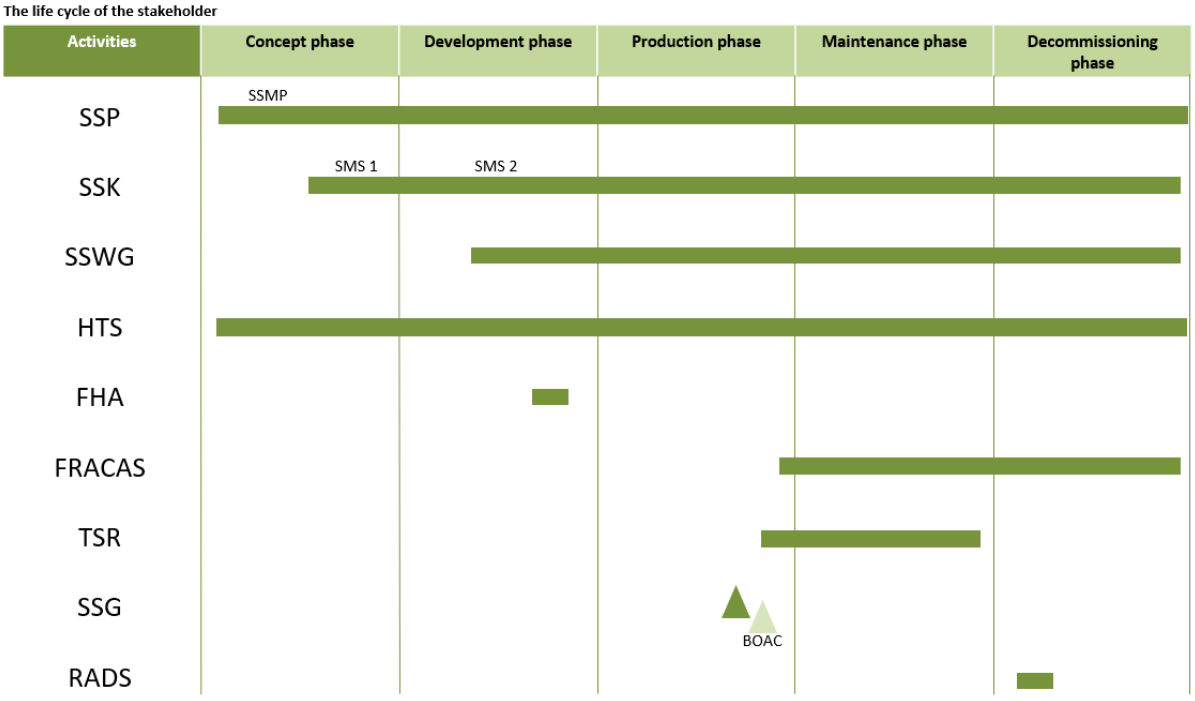


Figure 12.3 The stakeholder's mandatory system safety activities of the stakeholder.

12.4.3 The Client's Mandatory System Safety Activities

The client carries out the following mandatory system safety activities during the Swedish Armed Forces' production phase. The *client* can assist the *stakeholder* in the work already during the Swedish Armed Forces' development phase. In addition to the system safety activities in the figure below, some selectively chosen system safety activities may be added.

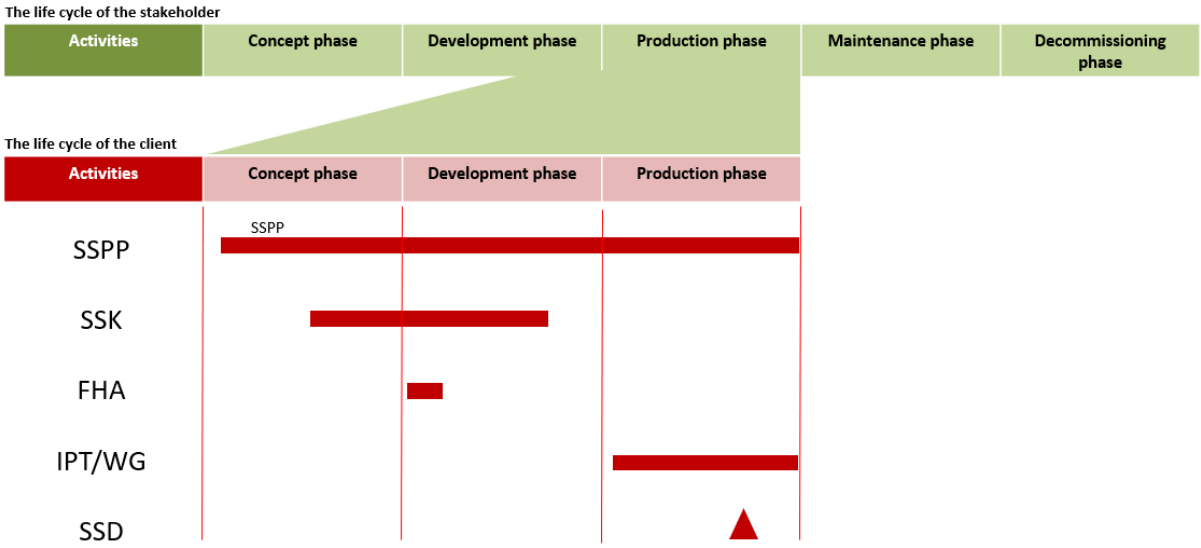


Figure 12.4 The client's mandatory system safety activities.

12.4.4 The Designer's Mandatory System Safety Activities

The *designer* most often applies an established development model for new technical systems. The audits to be conducted are normally regulated in a *System Engineering Management Plan* (SEMP).

Presentation of results from the various system safety activities is preferably linked to different design/technical reviews *(Technical Reviews)*. The advantage of linking system safety work to design/technical reviews is that these are integrated with *System Engineering* operations. That way, one obtains a strict connection with the development of the technical system.

At, or before, these design/technical reviews, technical reviews of the technical system are preferably also carried out to ensure that EU law, Swedish legislation, client requirements and related standards/handbooks are met. This is preferably done in a *Preliminary Design Review* (PDR) and a *Critical Design Review* (CDR).

Preliminary Design Review (PDR) - A formal review confirming that the preliminary design meets the requirements. It normally results in an approval to begin a detailed construction.

Critical Design Review (CDR) - A formal review to evaluate the completeness of the design and its interface.

Depending on the complexity of the technical system, the risk content and possible choices in the *Route Selection Model* (VVM), the *designer* can carry out the following system safety activities during *the client's production phase*. For the designer, the client's production phase consists of *the concept development* and *production stages*. In addition to the system safety activities in the figure below, additional selectively chosen system safety activities may be added.

Figure 12.5 The designer's mandatory system safety activities

For *Analyses* in the figure above, a number of system safety activities from SECTION 200 can be arranged.

12.4.5 The System Integrator's Mandatory System Safety Activities

Depending on the complexity, risk content and possible choices of the Technical System/System-of-Systems in *the Route Selection Model* (VVM), the *system integrator* can carry out the following system safety activities during *the Client's Production phase*. In addition to the system safety activities in the figure below, additional selectively chosen system safety activities may be added.

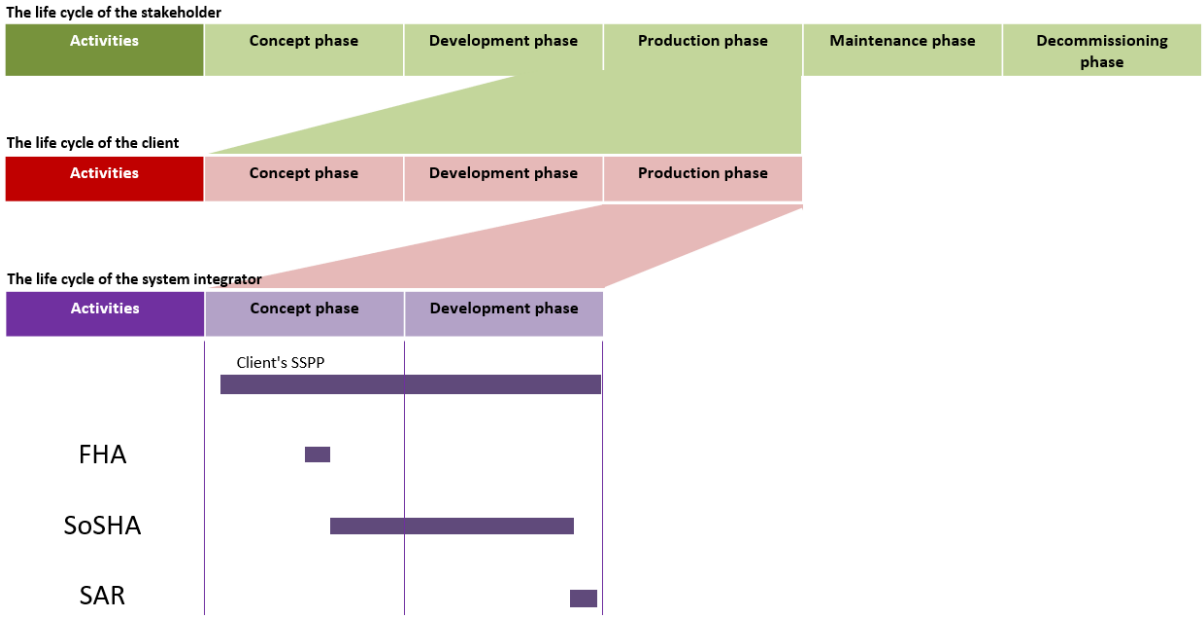


Figure 12.6 The system integrator's mandatory system safety activities.

12.5 Methodology for Selective Choice of System Safety Activities

In general, the system safety activities can be divided into mandatory activities and activities that can be selectively chosen from. Certain system safety activities are normally always applicable, such as the system safety decisions (SECTION 500) issued by different actors. Normally, one or more activities from the respective section are selected. See *Appendix 3 Description of system safety activities*.

When selectively choosing system safety activities, an initial system safety analysis needs to be carried out to clarify whether there are accident risks associated with the technical system, its use and/or operation. This can be done through a *Functional Hazard Analysis* (FHA) and/or through *the Preliminary Hazard List* (PHL). However, this initial system safety analysis does not have to be formal or follow any particular standard.

For some products, only the mandatory system safety activities need to be applied. For other technical systems, it is necessary to add selectively chosen system safety activities.

In order to assess the need for additional system safety activities beyond the mandatory ones, the following considerations need to be taken into account:

- Does the technical system cover many identified accident risks whose consequences can be considered serious?
- Can it be assumed that the technical system contains accident risks whose causal relationships are difficult to predict and therefore require a systematic approach in order to be sorted out?
- Does the technical system have complex interfaces and interactions with other systems where the interaction between these requires a systematic approach in order to be sorted out?
- Are there technical novelties about which limited experience exists or is lacking?
- Is previously known technology used in a different context or in a new way than has been done before?
- Can it be assumed that the technical system contains or can generate hazardous substances of various kinds? Then *health* (HHA) and *environmental* (EHA) system safety analyses can be applied.
- Can it be assumed that the technical system will require special handling? Then *Operating and Support Hazard Analysis* (O&SHA) can be applied.
- Is it assumed that producer responsibility for the technical system will be lacking? Then *Risk Assessment Prior to Disposal of Systems* (RADS) can be applied. Note that the RADS activity can also be used as a design aid during the development work.
- Can it be assumed that legislation and standards are new or have been significantly changed in connection with change (modification) since the technical system was put into use? Then the *System Requirements Hazard Analysis* (SRHA) activity can be applied.

12.6 The Operator's Selection of System Safety Activities

The table below indicates which role *(stakeholder, client, system integrator, designer)* normally carries out the various system safety activities when developing a new technical system or when changing (modifying). This does not apply to products that will be reviewed and verified/approved via another procedure, for example through CE marking or wheel marking.

The table below uses the following encoding:

- **Red** activities are always carried out (mandatory)
- Yellow activities are normally carried out, but can be opted out (selective choice)

Activity		Requirement definition	Client	System integrator	Designer
SECTION 100	*SSP*	SSMP			
	SSB	SSB			
	SSK	SMS	RFP		
	SSPP		SSPP		SSPP
	SSWG	SSWG	SSWG		
	IPT/WG		IPT/WG	IPT/WG	IPT/WG
	HTS	HTS	HTS		HTS
SECTION 200	*FHA*	FHA	FHA	FHA	FHA
	PHL	PHL	PHL	PHL	PHL
	PHA				PHA
	SCF				SCF
	SRHA			SRHA	SRHA
	SSHA				SSHA
	SHA				SHA
	O&SHA				O&SHA
	SoSHA			SoSHA	SoSHA
	HHA				HHA
	EHA				EHA
	SIA			SIA	SIA
	RADS	RADS			RADS
SECTION 300	*SAR*	SAR	SAR	SAR	SAR
	TEP		TEP	TEP	TEP
	FRACAS	FRACAS	FRACAS		FRACAS
	SR				SR
SECTION 400	*SV*		SV	SV	SV
SECTION 500	*SCA*				SCA
	SSD		SSD		
	TSR	TSR			
	SSG	SSG			
	SSM		SSM		SSM

Figure 12.7 Roles that typically carry out certain system safety activities.

13 Accident Risk Model (ORM)

The purpose of this chapter is to describe the relationship between a hazardous event, accident, incident, accident risk and injury outcome, and to describe the Swedish Armed Forces' Accident Risk Model (ORM), which provides the opportunity to systematically work with risk reducing measures.

13.1 Relationship Between Hazardous Event, Accident, Incident and Accident Risk

The Swedish Armed Forces demand that technical systems and products offer a satisfactory level of safety. For individual accident risks, which need to be managed through system safety analysis and risk assessment in Route Selection (VV7), risk assessment is required against a *Tolerable Risk Level* (TR) expressed in a risk matrix. Prior to the delivery or handover of technical systems or products to the Swedish Armed Forces, an account is made of how the satisfactory level of safety has been achieved and how individual accident risks can be considered to be below *the Tolerable Risk Level* (TR). The system safety evaluation provides the overall picture of the safety of the technical system or product and presents the position with arguments and evidence.

The magnitude and extent of the accident risk is expressed in the probability of accident with certain injury outcomes. The more serious the outcome of the injury and the higher the probability of this injury, the greater the risk of accidents is considered to be. Consequently, the level of *Tolerable Risk Level* (TR) needs to be set in relation to the severity of the injury outcome and the probability of the related accident occurring.

An accident occurs if a hazardous event occurs and something worthy of protection is damaged. An incident means that a hazardous event occurs that does not lead to any damage outcome.

13.2 Description of the Accident Risk Model (ORM)

Each accident or incident is unique based on the fact that different prerequisites and conditions apply at the time the event occurs. Accidents often have complex events in terms of the causes and indirect conditions that have led to them. An *Accident Risk Model* (ORM) can therefore never fully describe all the different prerequisites and conditions that may exist, but only show a simplified picture of factors that need to be taken into account in system safety work.

The Accident Risk Model (ORM) is primarily described for use in the dialogue between client and designer in connection with design review and applies mainly to accident risks that are managed through Route Selection (VV7).

The Accident Risk Model (ORM) can be applied to both physical sources of risk or sources of risk through errors in the various functions in which they operate/are active in. *The Accident Risk Model* (ORM) can thus provide support for arguments and evidence when conducting the system safety evaluation.

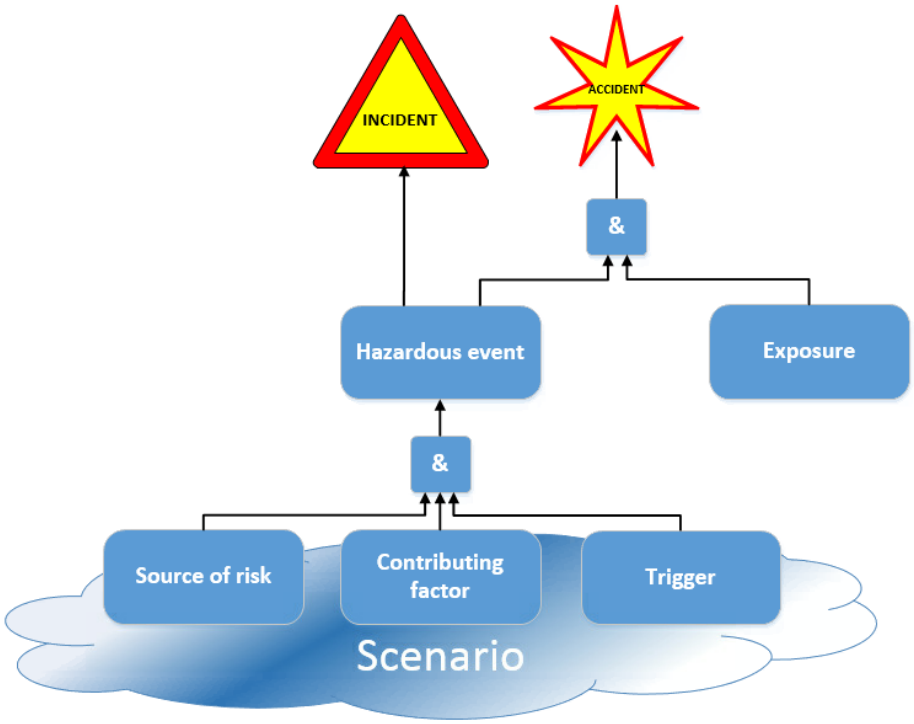


Figure 13.1 Accident Risk Model (ORM).

Below are descriptions of concepts adapted for *the Accident Risk Model* (ORM). Thus, there are no strict definitions of terms.

13.2.1 Source of Risk

The *Accident Risk Model* (ORM) assumes that each accident originates from a source of risk. A source of risk can be a functional or physical property. It can be a dangerous function, component, substance or other circumstance that can cause damage to person, property or external environment. The sources of risk are usually, but not necessarily, some kind of information, energy or emission.

A component or substance may have one or more different types of hazardous physical properties (sources of risk). The source of risk of a road vehicle in motion is kinetic energy that can injure people inside and outside the road vehicle in the event of a collision. An explosive substance is a source of risk whose dangerous property lies in the energy that can develop in the event of a detonation. The source of risk can be something that has potential (stored) energy as a dangerous property, such as a tensioned steel spring, free-hanging load or if a person is at a high altitude. The source of risk may also consist of electricity or radiation. A component is always accounted for together with its hazardous properties (sources of risk).

A component can generate one or more sources of risk through errors in the various functions in which it operates/is active in, such as misinformation. For example, a functional source of

risk may indicate the wrong target data, grouping data or time, where such errors can lead to a hazardous event of the technical system. Incorrect target data from a command and control system can result in weapon action not occurring against the intended target.

Sources of risk can also be natural phenomena such as lightning strikes, static electricity and icing. The hazardous properties that are not associated with an energy or emission form, can be a hazardous substance or an oxygen-deficient atmosphere in an enclosed space.

Different standards may have different definitions of the concept of source of risk. *The Accident Risk Model* (ORM) breakdown of component/substance, source of risk, contributing cause and hazardous condition can all be referred to as sources of risk in other standards.

> A source of risk is a dangerous property that can lead to injury to a person, property or external environment. A source of risk can also be a natural phenomenon.

In order to compile a list of components/substances with their sources of risk, the *Preliminary Hazard List* (PHL) activity *can be applied.*

Component	Source of risk
Hatch	Stored energy that turns into kinetic energy

Table 13.1 Example of component with its source of risk.

The fact that a source of risk is present does not imply that there needs to be any immediate or direct danger of an accident or incident. In some cases, there may be added value in documenting in which situations the source of risk is active and latent, respectively.

Component	Source of risk	Dangerous condition	"Harmless" condition
Hatch	Stored energy that turns into kinetic energy	Hatch open	Hatch closed

Table 13.2 Examples of situations with an active or latent source of risk.

13.2.2 Scenario

One scenario describes the different prerequisites and conditions that apply before a chain of events begins that can lead to an accident or incident. A description of a scenario can include:

- The activities that are carried out/are ongoing, either by:
    - Define specific situations
    - Use standard scenarios such as use, relocation, combat, care, maintenance, and storage (transportation)
    - Consider emergencies such as emergency evacuation and rescue operations
- Number of people present, their responsibilities, duties and possible level of tension
- Usage environment
- Light conditions
- Soundstage
- Weather effects/conditions
- Other aspects that may be of interest
    - Presence of Personal Protective Equipment (PPE)
    - Interfaces with the basic resources of facilities
    - Third person or that person's property involved

One scenario describes the usage environment.

13.2.3 Hazardous Event

A hazardous event is an undesirable event that occurs unintentionally. On the one hand, it can be a technical error, on the other hand, it can be a human error that occurs by accident or by mistake (lack of concentration). A hazardous event can result in an accident if something worthy of protection is exposed, otherwise an incident occurs.

A source of risk does not cause hazardous events solely by its presence, but it is required that the component/substance for some reason ends up in an undesirable state so that its hazardous properties are free or activated.

A hazardous event occurs unintentionally and without intent and can result in an accident or incident.

Component	Source of risk	Dangerous condition	Hazardous event
Hatch	Stored energy that turns into kinetic energy	Hatch open	The hatch re-closes

Table 13.3 Example of hazardous event.

13.2.4 Contributing Causes

Contributing causes are conditions that, together with a source of risk, provide the conditions for a hazardous event. If an ongoing contributing cause can be detected in time and prevented before a hazardous event occurs, the technical system or product returns to a safe (safer) state.

The contributing causes can be divided into permissible causes, direct causes and safety-cultural causes.

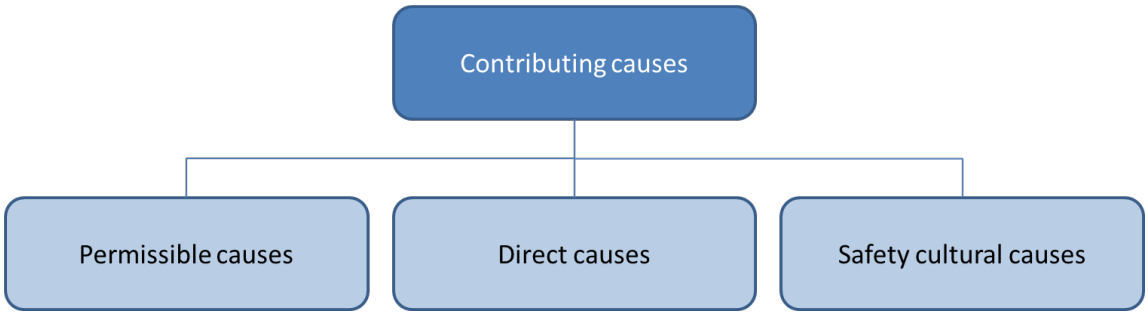


Figure 13.2 Contributing causes may be permissible, direct or safety-cultural causes.

Permissible causes mean that the technical system or product is in a certain permitted system state such as a weapon when the safety catch is off, certain data being received by a computer system, a switch being on or off, or a lid or hatch being open or closed. The causes are thus both intended and reasonable in the case of their intended use. The responsibility for these rests primarily with *the designer*.

Direct causes are those conditions that exist for some time before and until the occurrence of the hazardous event. These can be divided into *deficient conditions* and *incorrect actions or practices*.

Deficient conditions may include, for example, inadequate warning systems, inadequate or faulty protection/safety equipment, or hazardous environments. The responsibility for these rests primarily with *the designer*.

Incorrect actions or practices may include, for example, safety equipment, improper use of machinery and become inoperative, or the failure to use Personal Protective Equipment (PPE). The responsibility for rectifying these rests primarily with the person who has an employer and delegated work environment task.

The safety cultural causes are the same as the actual causes that contribute the *emergence or perpetuation of incorrect actions or practices*. The safety cultural causes can be divided into *organisational* and *personal factors*.

Organisational factors can be deficiencies in the design of the workplace, substandard maintenance, deficiencies in equipment, materiel and tools, substandard instructions for the performance of the task or inadequate leadership. The responsibility for rectifying these rests primarily with the person who has an employer and delegated work environment task.

Personnel factors can be insufficient knowledge, insufficient capacity, fatigue, stress or lack of motivation. The responsibility rests primarily with the person who has an employer and delegated work environment task.

Contributing causes are conditions that, together with a source of risk, create prerequisites for a hazardous event.

Component	Source of risk	Contributing causes	Hazardous event
Hatch	Stored energy that turns into kinetic energy	The hatch is not locked in the raised position	The hatch re-closes

Table 13.4 Examples of contributing causes.

13.2.5 Trigger

A trigger means that a certain circumstance occurs that triggers a hazardous event, provided that both the source of the risk and the contributing causes exist simultaneously.

A source of risk and a trigger can sometimes be difficult to distinguish in a particular scenario. A trigger in one scenario can be a source of risk in another scenario or vice versa. Triggers can thus be deficiencies in the technical system or product, or components that are used correctly and where the system state is deliberately changed, for example via a switch.

Triggers can also be external influences such as fire, rain, lightning, static electricity, heat, cold, moisture or pests. Even a hostile attack can be a trigger but this is handled outside the system safety area.

A trigger is a mechanism that, together with a source of risk and contributing causes produce a hazardous event.

Component	Contributing causes	Trigger	Hazardous event
Hatch	The hatch is not locked in the raised position	Wind or storm gust	The hatch re-closes

Table 13.5 Examples of triggers.

13.2.6 Accident

An accident means that a hazardous event occurs at the same time as something worthy of protection such as person, property and/or external environment is damaged. An accident is always unplanned and accidental. The accident is not the result of, for example, a hostile act.

An accident can cause both immediate injuries such as death, loss of vision or broken bones or initiate injuries that can cause ill health for a long time to come such as hearing loss or a whiplash injury. Mental illness in the form of crisis response due to the accident is handled outside the system safety area.

> An accident occurs when a person, property and/or external environment is damaged by the source of risk as a result of a hazardous event occurring.

In order to more easily identify accident risks, and not quality deficiencies, these should always be formulated as below. Also, do not grade the severity of the wording.

- Personal injury at... caused by/due to/caused by...
- Property damage at... caused by/due to/caused by...
- Environmental damage in... caused by/due to/caused by...

Component	Hazardous event	Worthy of protection	Accident risks
Hatch	Hatch re-closes	Person	Personal injury (pinching injury) caused by falling hatch

Table 13.6 Examples of accident risk.

13.2.7 Incident

An incident means that a hazardous event occurs but where nothing worthy of protection such as person, property or external environment is damaged.

There are many more incidents than there are accidents. From both event types, accidents and incidents, valuable information can be obtained to improve system safety by identifying the contributing causes and triggers. Through this, it is possible to identify risk reducing measures to reduce the probability of the hazardous event occurring or to limit the consequences if it nevertheless occurs.

> An incident means that a hazardous event occurs but it does not cause any harm.

13.3 Application of the Accident Risk Model (ORM)

The Accident Risk Model (ORM) provides opportunities for a systematic system safety work to identify one or more different risk reducing measures. During the development work, the model can complement *the Preliminary Hazard List* (PHL) and/or a *Preliminary Hazard Analysis* (PHA). During design review, the model can provide arguments and evidence for the system safety evaluation.

By methodically going through all parts of the *Accident Risk Model* (ORM), a number of different risk-eliminating/risk-reducing measures can be identified for each identified accident risk. Some measures may affect the outcome of the event, other measures may affect the probability/frequency of the occurrence.

By applying the table below, proposals for reducing measures can be identified for each column. Some actions can affect several different factors in the table.

Compo-nent	**Source of risk**	**Scenario**	**Contributing causes**	**Triggers**	**Hazardous event**	**Exposure**	**Accident**
Hatch	Kinetic energy	Frequently used materiel is stored under the hatch	The hatch does not have a latch in the raised position	The hatch is involuntaril y bumped, subjected to wind or storm surge	Hatch re-closes	Person	Personal injury (pinching injury) caused by falling hatch
Suggestion	***Suggestion***	***Suggestion***	***Suggestion***	***Suggestion***		***Suggestion***	
Hatch in lighter material	Adding soft-closing brake	Moving materiel, resulting in fewer openings/cl osings of the hatch	Supply mechanical latch that prevents the hatch from falling	The hatch is closed from the raised position to minimise the surface exposed to the wind		Instruction that a person should hold the hatch in the raised position	

Table 13.7 Example of table when applying the Accident Risk Model (ORM).

14 Risk Matrix and Tolerable Risk Level

The purpose of this chapter is to describe how risk assessment for accident risks can be made against a Tolerable Risk Level (TR) expressed in risk matrices based on basic matrices for person, property and external environment, as well as the production of evidence for the risk reduction after action.

14.1 Basic Matrix

Risk matrices are used to report accident risks that have not been handled in the previous route selections (VV1 – VV6) in *the Route Selection Model* (VVM).

The Swedish Armed Forces require that accident risks managed through Route Selection (VV7) must be assessed against a *Tolerable Risk Level* (TR) expressed in a risk matrix. This can be defined for a product area or certain technical system and inserted into *the System Safety Management Plan* (SSMP). The Swedish Armed Forces' general risk matrices according to sections 14.3 - 14.5 are normally applied, unless there are special reasons.

*System objective (*SMS 2) must refer to the product area's *System Safety Management Plan* (SSMP) and therefore does not need to contain risk matrices unless adaptation has been necessary for the current technical system.

The following describes the construction of a qualitative basic matrix.

Probability		**Severity class**			
		I	**II**	**III**	**IV**
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	ET	T	T
D	Not likely	ET	BT	T	T
E	Unlikely	BT	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 14.1 Qualitative basic matrix with Tolerable Risk Level (TR).

In the risk matrix, the colours have the following meaning:

- Red Not tolerable (ET)
- Yellow Limited tolerable (BT)
- Green Tolerable (T)
- Blue Eliminated

The risk matrices use four defined severity classes (I - IV) for consistency, where I represents the most serious severity class. For the definition of the respective severity class for person, property and environment see *sections 14.3 - 14.5*.

For probability, six different classes (A - F) are used, where A is the highest probability. Level F (blue area) *Eliminated* is only used to report accident risks where the severity class is not relevant.

Probability class	Designation	Qualitative definition of probability of accident during the service life
A	Frequent	The accident may occur frequently
B	Likely	The accident may occur several times
C	Possible	The accident may occur a few times
D	Not likely	The accident may occur occasionally
E	Unlikely	The accident cannot be assumed to occur at any time
F	Eliminated	The accident cannot occur

Figure 14.2 Qualitative probability classes of one item of the technical system during its service time.

The marked line between *Not tolerable* (ET) (red area) and *Limited tolerable* (BT) (yellow area) is defined as *Tolerable Risk Level* (TR). This line specifies the upper limit for the level of risk that the Swedish Armed Forces can accept, without the need to grant exemptions from the requirements in *System Objective* (SMS 2). However, the aim is that all managed accident risks after risk reducing measures have been introduced should be located in *Tolerable* (T) (green area) or in *Eliminated* (blue area).

The Swedish Armed Forces apply an adapted design of risk matrices that is close to that described in the MIL-STD-882E standard. The risk matrices must be applied to one (1) item of the technical system or product.

14.2 Probability and Frequency Ranges

In the quantitative assessment of accident risk against *Tolerable Risk level* (TR) for Route Selection (VV7), the following probability intervals can be applied unless otherwise specified in the product area's *System Safety Management Plan* (SSMP) or in *the System Objective* (SMS 2) for the technical system in question.

Probability interval	Designation	Quantitative definition of probability (p) of accident
A	Frequent	$p \geq 10^{-1}$
B	Likely	$10^{-2} \leq p < 10^{-1}$
C	Possible	$10^{-3} \leq p < 10^{-2}$
D	Not likely	$10^{-6} \leq p < 10^{-3}$
E	Unlikely	$p < 10^{-6}$
F	Eliminated	The accident cannot occur

Figure 14.3 Quantitative probability intervals of one item of the technical system.

The probability ranges A - F comply with the MIL-STD-882E standard. Note that the interval D ($10^{-6} \leq p < 10^{-3}$) covers three figures to the power of ten. To reclassify an accident risk past

this range, a risk reduction factor of more than 10^{-3} is required to fall below *the Tolerable Risk Level* (TR) according to the Personal Injury Risk Matrix.

The quantitative probability ranges refer to the probability of accident per defined activity, such as probability of accident/shot or accident/loading. Activity must be selected on the basis of what can most clearly link the source of risk to a possibly hazardous event and accident for the technical system in question.

This means that the probability of a hazardous event is equal to the probability of accident when exposed = 1, see *Figure 13.1* If a modelling of probability of a hazardous event can be done, this must be done with credible and traceable experience data. If computer systems and software are included in the modelling, these must comply with requirements according to the established level of criticality. See the methodology in the Swedish Armed Forces on Software in Safety-Critical Applications (H ProgSäk E).

If the probability intervals are to be recalculated against a frequency range, the quantitative probability intervals according to *Figure 14.3* need to be defined against the maximum expected/accepted number of accidents during a specified exposure, where the exposure can be based on, for example, the number of firings, hours of operation, the number of kilometres driven depending on what is most relevant for the identified accident risks based on the operational profile.

If a different probability interval is to be used, or converted into a frequency range, this must also be stated in the System Objective (SMS 2) of the Technical System in question.

14.3 Risk Matrix and Personal Severity Classes

The Swedish Armed Forces' personnel injury risk matrix must be applied to all technical systems and products unless otherwise agreed in the product area or for a particular technical system.

Probability		**Severity class**			
		I	**II**	**III**	**IV**
		Death	Serious personal injury	Less serious personal injury	Negligible personal injury
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	ET	T	T
D	Not likely	ET	BT	T	T
E	Unlikely	BT	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 14.4 Personal injury risk matrix.

Consequences/outcomes for persons refer to accidental injuries to:

- The Swedish Armed Forces' own personnel
- Third party

Severity class	Personal injury	Consequence
I	Death	An accident resulting in single or multiple deaths
II	Serious personal injury	An accident resulting in one or more serious personal injuries, where loss of bodily function is feared
III	Less serious personal injury	An accident resulting in one or more less serious personal injuries, in which those who are exposed are expected to recover after care and rehabilitation
IV	Negligible personal injury	An accident that results in one or more minor personal injuries, where those who are exposed will be fully recovered without care or rehabilitation.

Figure 14.5 Risk matrix and personal severity classes.

14.4 Risk Matrix and Property Damage Classes

The Swedish Armed Forces' personnel injury risk matrix must be applied to all technical systems and products unless otherwise agreed in the product area or for a particular technical system.

Probability		Damage class			
		I	II	III	IV
		Catastrophic property damage	Critical property damage	Serious property damage	Negligible property damage
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	BT	T	T
D	Not likely	BT	T	T	T
E	Unlikely	T	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 14.6 Property damage risk matrix.

Consequences/outcomes for property refers to accidental damages to:

- Technical systems, products or other property of the Swedish Armed Forces, such as facilities
- Property of third person (not external environment)

The range of amounts for property damage must be adjusted against the cost of replenishment of the relevant technical system or other damage to an amount corresponding to the respective damage class (including system-of-systems). If the replacement cost exceeds

100 MSEK, this is the amount for damage class I. Other amount ranges can be set at 1/10 for each damage class.

Severity class	Critical property damage	Consistency amount range (example)	Consequence
I	Catastrophic property damage	≥ 100 MSEK	An accident that results in damage in parity with total system loss (scrapping) or damage that renders the current system unusable for an extended period of time. Extensive repair or replacement is required.
II	Critical property damage	< 100 MSEK	An accident that results in damage that renders essential parts of the system unusable, but some functionality can be maintained. Minor repair efforts are required.
III	Serious property damage	< 10 MSEK	An accident that results in damage that degrades some functions, but the main functionality of the system is maintained. Major repair efforts are required.
IV	Negligible property damage	< 1 MSEK	An accident that results in minor damage affecting some functions, but the system at large can still be used while awaiting repair.

Figure 14.7 Definition of property damage classes including third-party property.

14.5 Risk Matrix and Damage Classes for Environmental Damage

The Swedish Armed Forces' environmental damage risk matrix must be applied to all technical systems and products unless otherwise agreed in the product area or for a particular technical system.

Probability		Damage class			
		I	II	III	IV
		Catastrophic environmental damage	Critical environmental damage	Serious environmental damage	Negligible environmental damage
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	ET	T	T
D	Not likely	ET	BT	T	T
E	Unlikely	BT	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 14.8 Risk matrix for environmental damage.

Consequences/outcomes for property refers to accidental damage to:

- The external environment that can be rectified and repaired through, for example, decontamination.

Irreversible (devastating) environmental damage is avoided through regulation of activities subject to a permit and is handled within the framework of the Swedish Armed Forces' sustainability work. Permissible work environment and environmental impacts such as noise, emissions of pollutants (emissions) and energy consumption are handled outside the system safety work.

The amount ranges for environmental damage are adjusted against the estimated cost for damage class I. If the assessed cost of carrying out rectification of the environment is 100 MSEK, this is the amount for damage class I. Other amount ranges can be set at 1/10 for each damage class.

Damage class	Environmental damage	Consistency amount range (example)	Consequence
I	Catastrophic environmental damage	≥ 10 MSEK	An accident that results in reversible damage to the environment but with significant environmental impact. Very extensive decontamination is required
II	Critical environmental damage	< 10 MSEK	An accident that results in reversible damage to the environment and with great environmental impact. Extensive decontamination is required
III	Serious environmental damage	< 1 MSEK	An accident that results in reversible damage to the environment and with minor environmental impact. Minor decontamination is required
IV	Negligible environmental damage	< 0.1 MSEK	An accident that results in reversible damage to the environment and with insignificant environmental impact. Decontamination is usually not necessary

Figure 14.9 Definition of damage classes for environmental damage.

14.6 Risk Matrix, Criteria for Evidence of Risk Reduction

For an accident risk, which before action is deemed to be in *the Not tolerable* (ET) red area or in *the Limited tolerable* (BT) yellow area of the risk matrix, the risk reducing measures must be presented as evidence to be able to move these in the risk matrix after action. Measures may consist of design measures that reduce the probability of a hazardous event and thus correspondingly the risk of accidents.

If design measures can eliminate or encapsulate the source of risk, the risk of accidents is completely eliminated. Design measures may also have an impact on the contributing causes or impede the triggers.

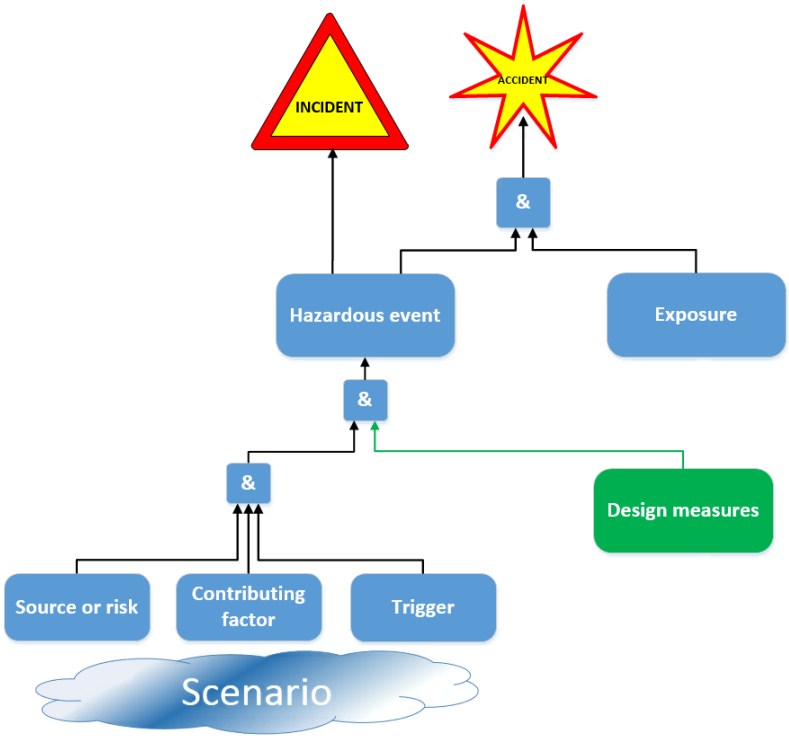


Figure 14.10 Risk reduction by design measure.

If the design measures are not deemed sufficient, warning devices, Personal Protective Equipment (PPE) or restrictions in use may also be introduced, which will reduce exposure and can thus be seen as an additional condition that reduces the risk of accidents.

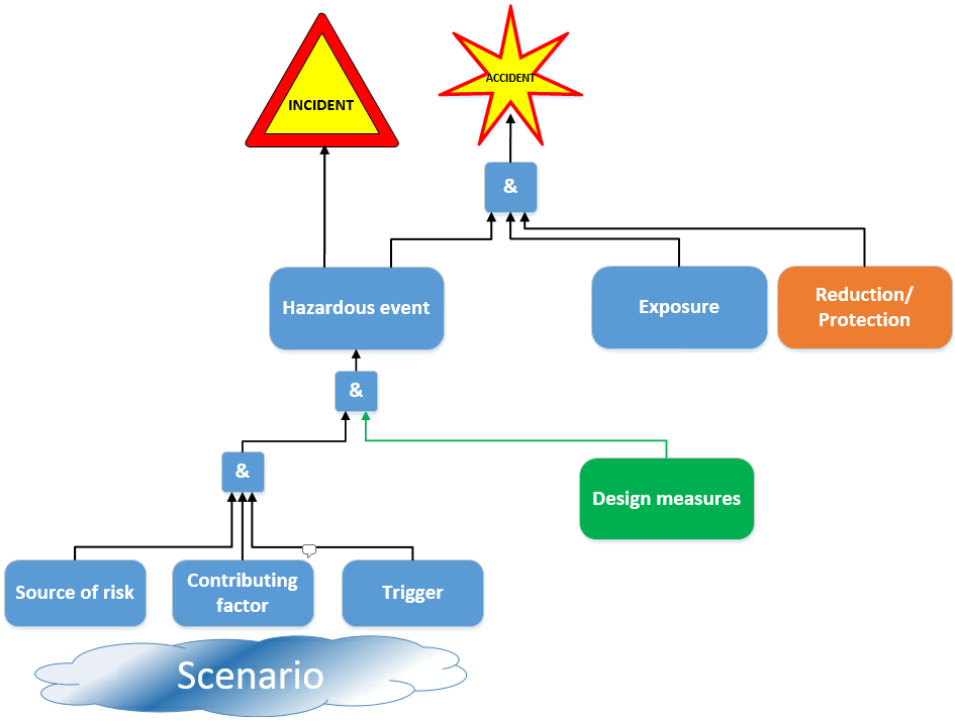


Figure 14.11 Risk reduction by design measures and reduction/protection.

14.6.1 Accounting for Design Measures

For each managed accident risk in the red (not tolerable) or yellow (limited tolerable) area of the risk matrix, design measures must be reported that can demonstrate that at least one additional &-condition is required for a hazardous event to occur for example IIC to IIE. These measures entail a vertical movement in the risk matrix. Design measures that provide an increased margin of safety can also be considered as an &-condition.

Probability		Severity class			
		I	II	III	IV
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	ET	T	T
D	Not likely	ET	BT	T	T
E	Unlikely	BT	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 14.12 Risk reduction in risk matrix.

In *Figure 14.13* below, design measures have been described that are independent &-conditions in case of simultaneous failures for a hazardous event to occur. Design measures may have an impact on the source of risk, contributing causes or triggers, but are presented in the image below simplified as additional &-conditions for the hazardous event to occur.

In a quantitative system safety analysis, accounting must also include a statement demonstrating that implemented design measures also entail risk reduction corresponding to the probability range in the post-action risk matrix. That is, for the change from IIC to IIE entails the requirement to be able to report a risk reducing factor of less than 10^{-3} compared to the change from IIIA to IIIC which entails a requirement for a risk reducing factor of more than 10^{-2}.

Thus, in order to obtain the required risk reduction, several design measures may be required. It must be possible to show that each design measure is independent in order for the model below to be valid. If there is credible experience data, these can be used to calculate a probability of error, otherwise an estimate may be made (conservative approach) on what the design measure can be judged to add. If an assumption is made for a risk reduction for a design change, it should not be applied to a value that entails a risk reduction factor of more than 10^{-1}. If a greater risk reduction is required, it must be substantiated.

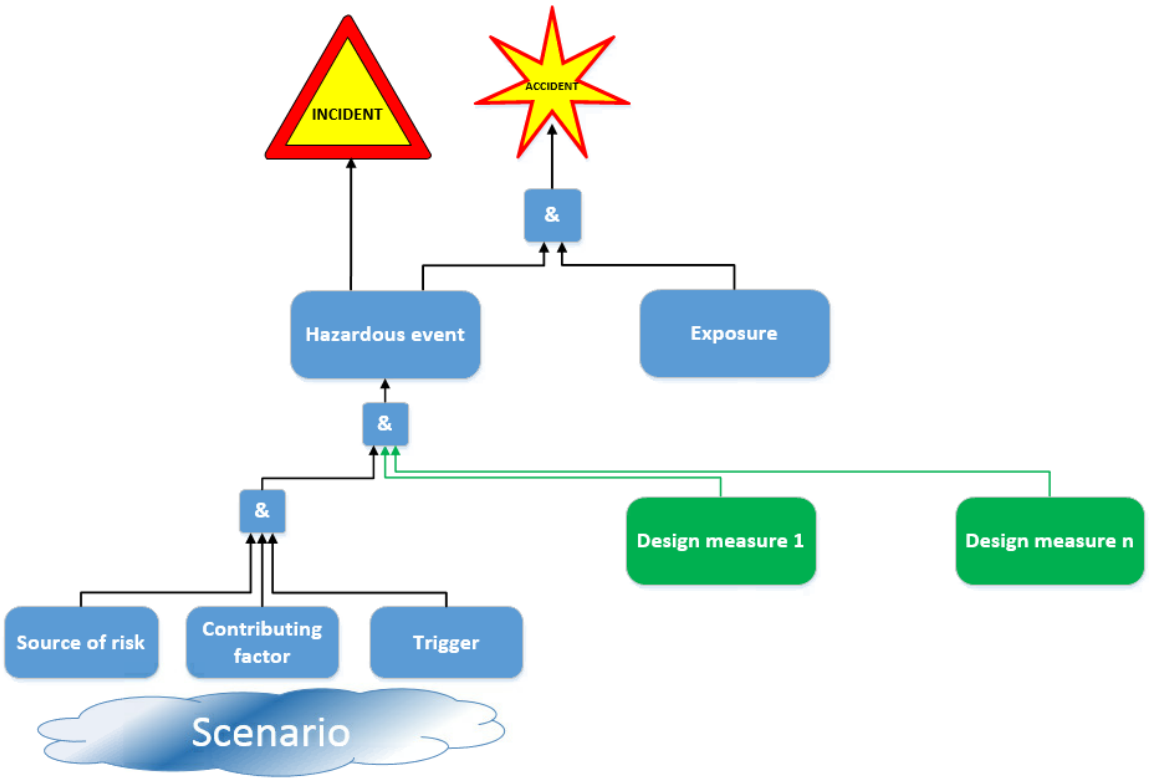


Figure 14.13 Risk reduction with design measures.

14.6.2 Accounting of Reduced Exposure

If applied design measures are not deemed to result in sufficient risk reduction, factors affecting exposure in the event of a hazardous event may be introduced.

This type of action can be, for example, protection, changes in working methods or restrictions in use. These measures mainly reduce the class of injury (the consequence), that is, they entail a horizontal movement after action in the risk matrix.

Probability		Severity class			
		I	II	III	IV
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	ET	T	T
D	Not likely	ET	BT	T	T
E	Unlikely	BT	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 14.14 Risk reduction after design measures and reduced exposure.

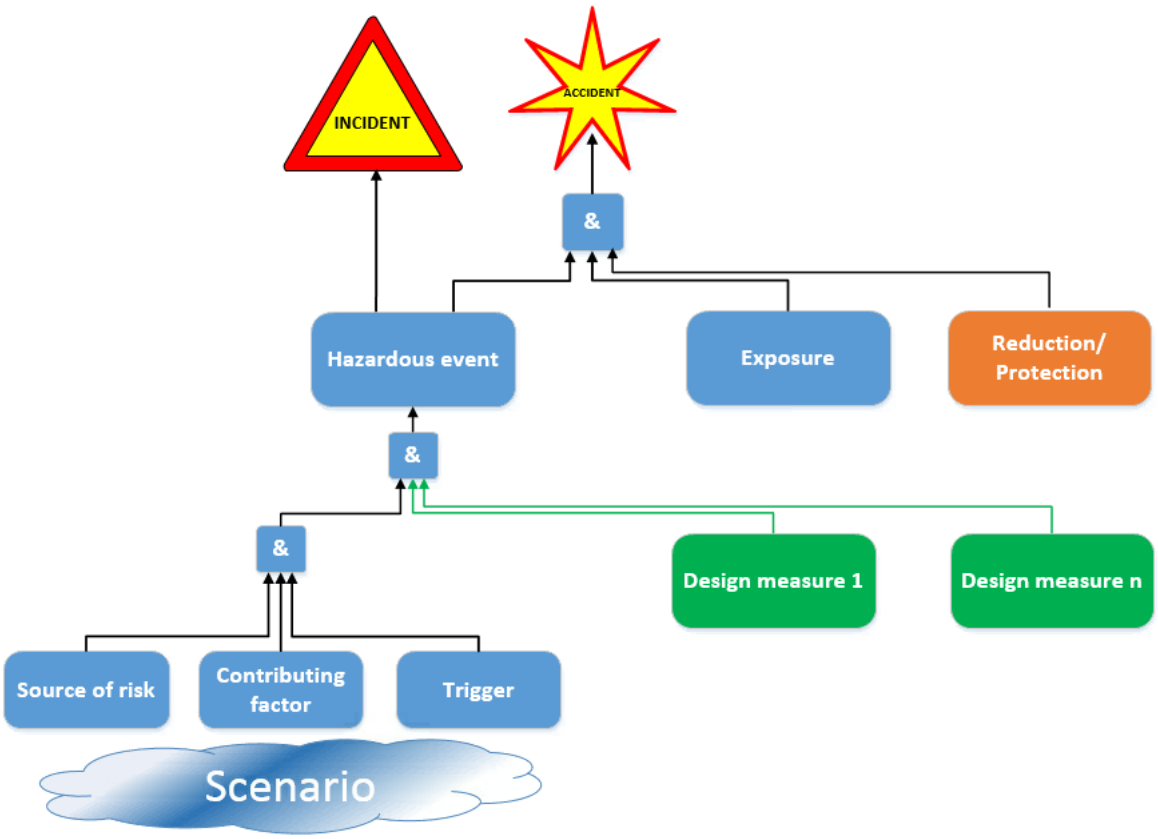


Figure 14.15 Risk reduction with design measures and reduced exposure.

15 Accident Risk Assessment and Classification

The purpose of this chapter is to describe how risk assessment and classification of accident risks can be carried out and how the closure of system safety work for individual accident risks can be carried out.

15.1 Basic Principles of ALARP Concerning Remaining Accident Risks

Before the Swedish Armed Forces are to put new or changed (modified) technical systems into use, careful consideration needs to be given to the remaining accident risks. This means that all identified accident risks by their nature must be known and documented, if necessary reduced, and that acceptance decisions for each of them must be made.

The Swedish Armed Forces require that risk assessments be carried out for remaining accident risks that have not been handled in Route Selections (VV1 – VV6) against a *Tolerable Risk Level* (TR) expressed in the risk matrix. At the same time, the aim is that all risk reducing measures that are deemed to be effective for risk reduction are taken, regardless of where the accident risk is classified in the risk matrix.

The principle that any remaining accident risks should be *as low as practicable* is commonly referred to as ALARP (*As Low as Reasonably Practicable*). The concept of *reasonably practicable* means weighing an accident risk against the problems, time and money needed to reduce it. However, there are different ways to define *as low as practicable* and the concept therefore usually needs to be put in relation to something else. With *as low as practicable,* an accident risk can be considered reduced to a sufficiently low risk level if good practice has been followed. This means, among other things, that established standards and *Design Rules* (DR) have been followed based on today's level of technology.

In order to assess whether additional reducing measures are reasonably and practically feasible, the following may be considered and determined:

- Demonstrably risk reducing if implemented
- Performance degradation is balanced and acceptable in relation to the safety increase
- Economically justifiable in comparison with the statistically calculated accident cost
- Easily realizable and that delivery delays can be avoided

Most often, it is a combination of the above points that determines whether it is a sufficient argumentation for ALARP. Normally, ALARP is applied for accident risks classified within *Limited Tolerable* (RT) (yellow area).

15.2 Classification of Accident Risk before Risk Reduction

During the design work of a technical system or product, the *designer* identifies a number of accident risks. Accident risks are initially evaluated based on the consequences that may occur. Through an iterative process, the *designer's* work begins with the aim of eliminating the *accident risks*.

Some accident risks can be eliminated by redesign and others can be reduced. Certain accident risks can be considered to be taken care of by having been managed in whole or in part by means of Route Selections (VV1 – VV6). Other accident risks and those partially managed by Route Selections (VV1 – VV6) must be risk assessed on the basis of consequence/injury outcome and probability/frequency. They must then be classified into the required risk matrices for the person, property and external environment by Route Selection (VV7) and reported to *the client*.

When *the designer* considers that the technical system or product is ready for *the client's* first design review, all remaining accident risks before risk reduction are also presented in the agreed manner. During the design review, *the client* may comment on both the design and the classification of accident risks.

Different system safety standards set out different principles for what can be presented regarding remaining accident risk. It can be *the worst possible* consequence, *the worst likely* consequence, or *usually feared* consequence. Regardless of the accounting method above, this only indicates a subset of the likely consequences if an accident occurs. The Swedish Armed Forces recommend a method where all severity classes in the risk matrix are presented for each individual accident risk. Suggested methods can be found in section 15.8.1.

15.3 Choice of Risk Reducing Measures

Following classification of the remaining accident risks, some accident risks may be necessary to remedy, while other accident risks may be further reduced in accordance with the basic principles of ALARP. For each of the remaining accident risks of personal injury, property and environmental damage, proposals for risk reducing measures, including estimated impact, must be developed and documented.

If an accident risk is classified as *Not tolerable* (NT) (red area), risk elimination/reduction must be done to fall below the *Tolerable Risk Level* (TR) requirement. For accident risks classified as *Limited tolerable* (BT) (yellow area) or *Tolerable* (T) (green area), measures should be taken if these are deemed to be proportionate to the estimated risk reduction effect in accordance with the basic principles of ALARP.

In some cases, operating rules can manage accident risks when it is not desirable to limit functionality that counteracts the safety of the technical system.

Each proposal for a risk reducing measure for an individual accident risk needs to be evaluated taking into account whether it is the consequence/injury outcome and/or probability/frequency that is affected. It is desirable to find risk reducing measures so that the risk of accidents is completely eliminated.

However, there are few risk reducing measures that have a positive impact on both consequence/injury outcome and probability/frequency. If the assessed number of accidents that are likely to occur is constant, the severity classes are affected individually. If one severity class is eliminated, the remaining severity classes must be re-evaluated. This applies even if the probability of one severity class decreases, the probability/frequency of one or more of the remaining severity classes may increase.

When a risk reducing measure is introduced in the technical system, the risk of accident must be re-evaluated from a system safety point of view. The risk reduction must be substantiated and the system safety analysis must also ensure that the chosen risk reduction measure does not entail any increase in the level of risk of another previously identified accident risk or that its sources of risk pose new accident risks.

Different system safety standards have varying priorities for risk reducing measures. Common to these, however, is the order of preference; design (accident risks must be eliminated or reduced as far as possible), protect (necessary protective measures must be taken for those accident risks which cannot be eliminated) and warn (information must be given to users on remaining accident risks).

The following order of priority may be appropriate when selecting one or more measures:

- Eliminate or switch to less dangerous sources of risk
- Carry out reconstruction
- Introduce protective devices
- Introduce warning devices
- Supply Personal Protective Equipment (PPE)
- Produce instructions, signs, stickers
- Conduct training

> The introduction of one or more risk reducing measures does not automatically mean that the risk of accidents receives a lower classification. All movements in the risk matrix after the introduction of risk reducing measures must be deducible by arguments and evidence.

In the event of a change (modification) to technical systems and products that have previously been used in the Swedish Armed Forces, new accident risks identified in connection with the change must be below the *Tolerable Risk Level* (TR) and that the modification is not deemed to result in any significant increase in the risk level of other previously managed accident risk.

If new accident risks are classified as *Limited tolerable* (BT) (yellow area) or *Tolerable* (T) (green area), measures should be taken if these are deemed to be proportionate to the estimated risk reduction effect in accordance with the basic principles of ALARP.

A rule of thumb is that new accident risks classified as *Limited tolerable* (BT) or as *Tolerable* (T) are remedied if these accident risks are assessed as more serious than for other equivalent remaining accident risks in the original technical system.

15.3.1 Design-oriented Measures

- Eliminate or switch to less dangerous sources of risk
- Carry out reconstruction

Design-oriented measures can reduce both consequence and probability.

A source of risk is something that can cause harm to a person, property or external environment through its hazardous properties. A component may have one or more different sources of risk, such as energy or emissions. Closely connected to the source of risk are the *concepts of functional source of risk* and *hazardous condition*, which can usually be seen as contributing causes of an accident occurring. In some cases, deviations in the design work can be considered a *dangerous condition*, for example, a software failure.

Firstly, a design solution containing a particularly dangerous source of risk must be eliminated and replaced by another design with a less dangerous source of risk. Secondly, the chosen source of risk may be reduced or divided, for example by reducing volume or quantity, reducing height or size, without making unacceptable restrictions on the functions and performance of the technical system.

The source of risk often constitutes the primary function of the technical system, such as radiation from an antenna, the explosive substance in ammunition or the kinetic energy of a function, and can therefore be difficult to reduce or replace without the technical system losing its performance.

If the source of risk cannot be eliminated, identified hazards remain, but other measures may be introduced to reduce them. These measures can be technical, administrative or organisational and these measures can in turn reduce the risk of accidents by being preventive, i.e. reducing the probability of an accident or limiting the consequence/outcome of the accident, should the accident nevertheless occur.

Redesign means a design-oriented measure to reduce exposure by permanently (in whole or in part) separating or encasing the source of risk in a way that reduces the probability that its hazardous properties will not be inadvertently exposed to persons, property or external environment.

Redesign may also include design measures that reduce the probability of the hazardous event occurring. Furthermore, the technical system may need to be protected from the influence of natural forces such as lightning strikes and static electricity. The concept of

redesign also includes automation with the aim of removing hazardous operations and introducing various types of safety functions.

15.3.2 Protection-oriented Measures

- Introduce protective devices
- Supply Personal Protective Equipment (PPE)

Design-oriented measures can reduce both consequence and probability.

A protective device means a structural feature whose sole function is to protect the user directly or indirectly from the source of risk.

Personal Protective Equipment (PPE) means protective measures which do not belong to the technical system or product and which the individual users provide to protect themselves. Examples of personal protective equipment are hearing protection, protective mask, helmet, goggles, clothing, gloves and shoes. While these protections may be effective in avoiding accidents or ill health, protective equipment can have a negative impact on other areas such as function and performance. Protective measures are taken only after the possibilities of design-oriented measures are no longer possible or sufficient.

15.3.3 Warning and Information-oriented Measures

- Introduce warning devices
- Produce instructions, signs, stickers
- Conduct training

Warning and information-oriented measures mainly reduce the consequence.

A warning device means a monitoring system that actively alerts if a dangerous situation is about to occur or has just occurred. Warning devices may be optical, acoustic or which, by means of vibrations in control units, are intended to attract the user's attention.

Instructions, signs and stickers mean information that passively informs the user that there are sources of risk and that dangerous conditions can occur. This category also includes instructions or other restrictions in use such as defined danger zones for ammunition or radar radiation that affect exposure.

Training refers to providing prior knowledge and training for the safe use and maintenance of the technical system or product.

Warning and information-oriented measures can be effective in avoiding accidents or ill health, but only after design and safety-oriented measures are no longer possible or sufficient.

For severity class I (catastrophic) and severity class II (critical) where the design does not follow good practice is risk reduction using only Personal Protective Equipment (PPE), instructions, signs, stickers, training, or a combination thereof, is not sufficient.

Testing is not in itself a risk reducing measure, but can partially verify a function or sequence for safe operation if a hazard event occurs.

15.4 Classification of Accident Risk before Risk Reduction

When *the client* has expressed views on both the design and the classification of accident risks during an initial design review, *the designer* takes risk reducing measures. *The designer* makes a new classification of remaining accident risks after risk reduction in the agreed manner. During future design reviews*, the client* may submit new comments. Suggested methods can be found in section 15.8.2.

15.5 Exposure and Controllability Factors

When *the client* and *the designer* jointly consider that the possible design and protection measures have been taken, exposure and controllability factors can be applied as arguments and evidence to show that the probability of accident is reasonably lower.

Exposure and controllability factors are used only for personal injury and not for property and environmental damage. Exposure factor means that the user is not always present when a hazard event occurs. Controllability factors mean that the user can influence a dangerous state by stopping the chain of events or taking cover before the hazardous event occurs.

If the user is fully or partially protected when a hazardous event occurs, the probability/frequency of an accident can be reduced. This applies even if the user can detect or be alerted in time that an accident is imminent and thus has time to stop the chain of events or take cover. The user can then obtain a lower exposure factor than = 1 when the hazardous event occurs. When using the exposure factor in risk assessment, this must be specifically stated.

Exposure factors may only be used as a component to credit a reduced probability/frequency of injury to persons in an accident.

> For pre-action risk assessment, the exposure factor must be = 1, which means that this factor can only be credited as a second step after the introduction of risk reducing measures.

15.6 New Classification of Accident Risk by Exposure Factors

As a further step, if selected risk reducing measures are still not considered sufficient, estimated exposure and controllability data for persons can be taken into account in calculations or assessments of accident risks.

If the source of risk is chosen, other conditions may be affected in the design work and later also in the intended use:

- Reduction of contributing causes and triggers to the hazardous event
- Reduction of the probability of exposure of persons
- Increase in the ability to detect and control progress before the hazardous event occurs. In standards referred to as governability or controllability
- Reduction of consequences if the accident should nevertheless occur

By applying *the Accident Risk Model* (ORM), various given circumstances can be affected in the design of the technical system or product.

15.7 Closure of System Safety Work for an Accident Risk

The system safety work for an individual accident risk that has been classified in a risk matrix is called *open* until the introduced risk reducing measures are deemed sufficient. The accident risks are reported both by severity class and by highest severity class. The highest severity class of the accident risk thus becomes the guiding principle for further management.

- For an accident risk that has at least one of the relevant severity classes within *the Not Tolerable* (NT) (red area), the entire accident risk is assessed as *Not Tolerable* (NT).
- For an accident risk that is not in the red area *Not Tolerable* (NT), but which has at least one of the current severity classes within *Limited Tolerable* (LT) (yellow area), the entire accident risk is assessed as *Limited Tolerable* (LT).
- For an accident risk that has all the current severity classes within *Tolerable* (T) (green area), the entire accident risk is assessed as *Tolerable* (T).

Since the highest severity class in the example below is red, this means that the entire accident risk is *Not Tolerable* (NT) and that additional risk reducing measures need to be taken.

Classification (severity class/probability)	**Severity class by class**	**Highest severity class**
ID		
IID		
IIIC		
IVB		

Figure 15.1 Examples of accounting by severity class for a particular accident risk.

If the highest class of injury after introduced risk reducing measures is:

- Red, the client must *send a request requesting a deviation from the Tolerable Risk Level* (TR) to *the stakeholder*. *The stakeholder* can approve or reject the request
- Yellow, the *client* must ensure that the highest severity class of the accident risk is deemed to fit within the *Tolerable Risk Level* (TR) by reviewing that arguments and evidence and that the specific requirements for ALARP regarding the yellow cells are met. *The client* may approve, or request clarification from the *designer*
- Green, *the client* must ensure that the highest severity class of the accident risk is deemed to fit within *the Tolerable Risk Level* (TR) by reviewing arguments and evidence. *The client* may approve, or request clarification from the *designer*

The system safety work for an individual accident risk can be closed when it is made sure that all damage classes of the accident risk are deemed to fit within the *Tolerable Risk Level* (TR*)* or that *the stakeholder* has approved deviations from the requirements. This is done in agreement between *the client* and *the designer* when arguments and evidence for the individual accident risk are documented in *the Safety Assessment Report* (SAR) and *the Risk Log* (RL).

Accident risks that are deemed to fit within the Tolerable Risk Level (TR) or that the stakeholder has approved deviations from the requirements definitions are referred to as managed.

Accident risks where the risk reducing measures are not yet in place and which are thus followed by restrictions are referred to as remaining.

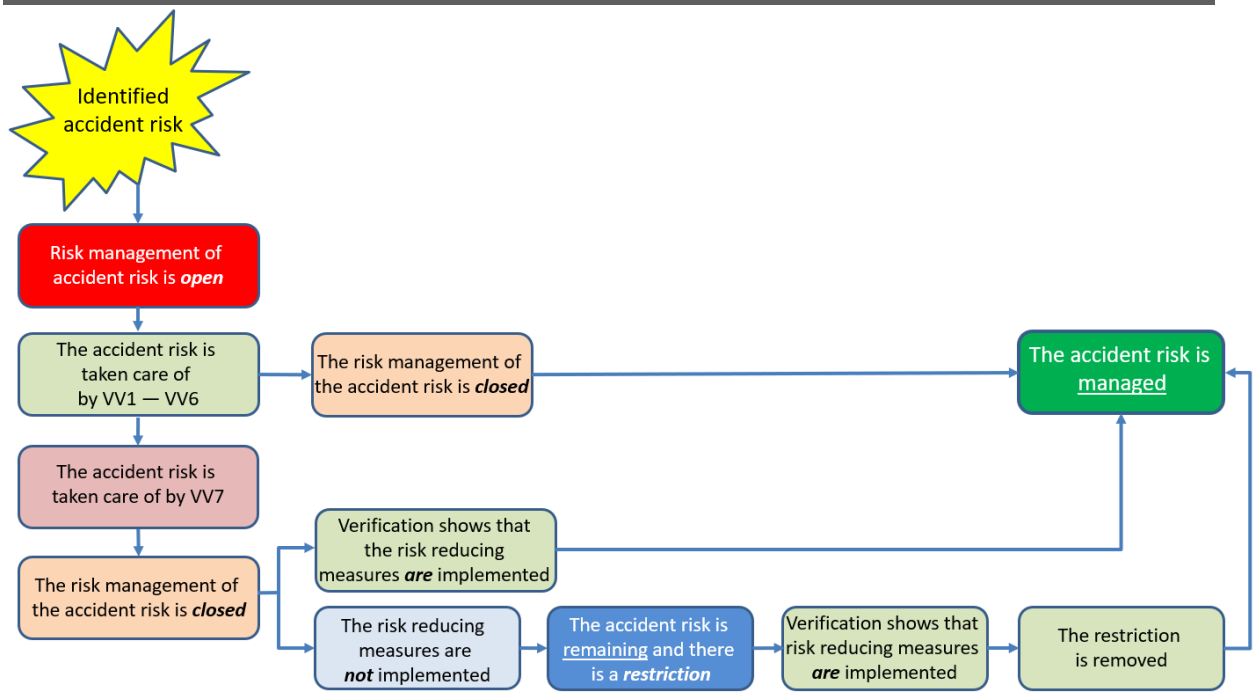


Figure 15.2 Managed and remaining accident risks.

15.8 Method for Classifying Accident Risk

Below is a methodology and workflow for classifying and presenting the assessed outcome of the entire accident risk.

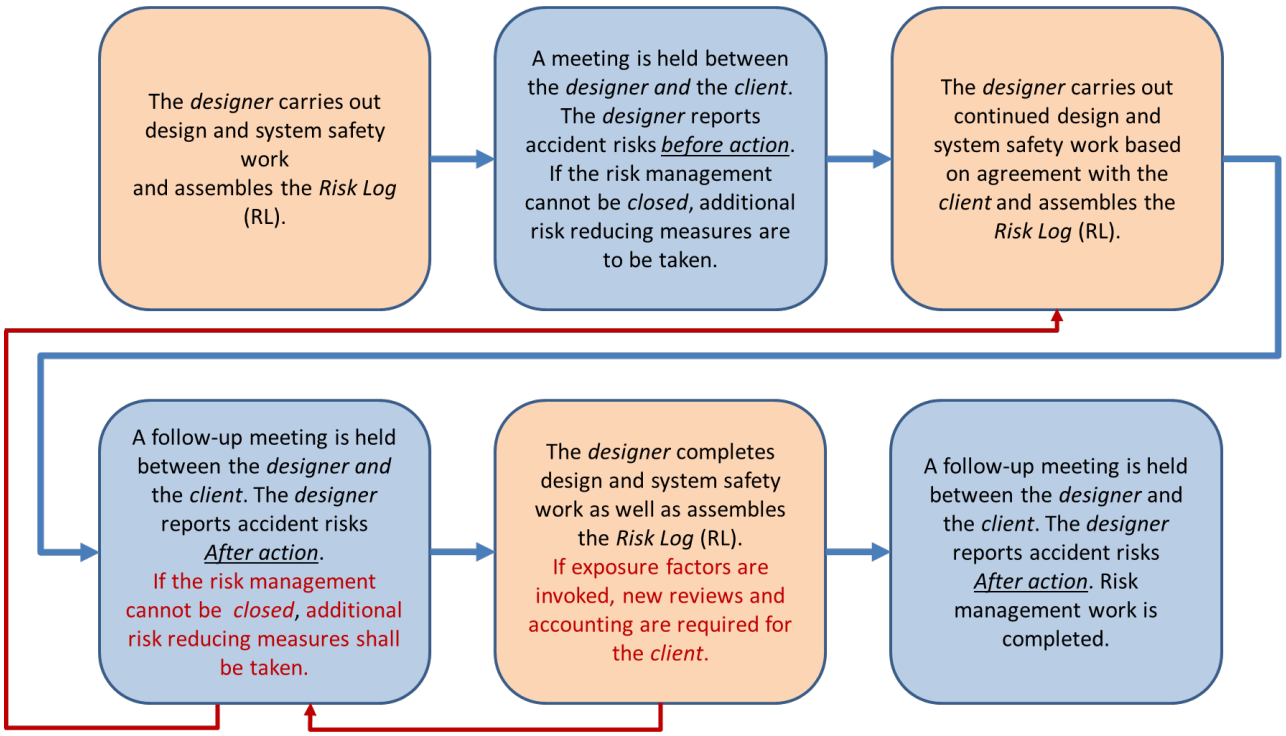


Figure 15.3 Work procedure for risk reduction of accident risk.

15.8.1 Classification of Accident Before Risk Reduction

When the technical system or product is ready for an initial design review, all remaining accident risks before risk reduction must be reported. This refers to accident risks that are managed with Route Selection (VV7) and can be carried out according to the method indicated below.

Classifying an accident risk, a number of steps are carried out in which used data, made assumptions and assessed results are documented.

1. Formulate the accident risk for persons, property and external environment, respectively.
   Apply the advice in the section Accident under the Accident Risk Model (ORM).
   - *Personal injury at... caused by/due to/caused by...*
   - *Property damage at... caused by/due to/caused by...*
   - *Environmental damage in... caused by/due to/caused by...*

2. Describe the intended scenario and sequence of events of the accident risk.
   Apply the advice in the section Scenario under Accident Risk Model (ORM).

3. Estimate how often/many times the accident may occur based on operating profile and service life.
   For this, Expert Assessments or Modelling can be used.

4. Write down all possible consequences (damage to persons, property and external environment, respectively) that may occur.

5. Imagine that the accident occurs 100 times (or 1000) and estimate how often the different consequences may occur and make a percentage distribution between the severity classes.

This is done for persons, property and external environment, but is exemplified only by the figure of personal injury below. For severity classes that are not considered to be able to occur, the value is set to "0%" and reported as "Eliminated" in the risk matrix.

Severity class	**Personal injury**	**Distribution in %**
I	Death	*a*
II	Serious personal injury	*b*
III	Less serious personal injury	*c*
IV	Negligible personal injury	*d*
Sum:		*= 100 %*

Figure 15.4 A percentage distribution of consequence/injury outcome is reported for a specific individual accident risk for personal injury before risk reduction

6. Enter the result in the risk matrices for person, property and external environment, respectively.
   This is done for persons, property and external environment, but is exemplified only by the risk matrix for personal injury below.

Probability		**Severity Class**			
		I	**II**	**III**	**IV**
		Death	Serious personal injury	Less serious personal injury	Negligible personal injury
A	Frequent	ET	ET	ET	BT
B	Likely	ET	ET	BT	T
C	Possible	ET	ET	T	T
D	Not likely	ET	BT	T	T
E	Unlikely	BT	T	T	T
F	Eliminated	*Eliminated*	*Eliminated*	*Eliminated*	*Eliminated*

Figure 15.5 Probability and consequence/injury outcome is reported for all severity classes for a particular individual accident risk for personal injury before risk reduction.

7. Document the data used, assumptions made and assessed results in *the Safety Assessment Report* (SAR) and in *the Risk Log* (RL).

15.8.2 Classification of Accident Risk After Risk Reduction

Risk assessment and classification after risk reducing measures, takes place in the same way as risk assessment and classification before action. Risk assessment after measures is carried out once more after the risk reducing measures are put in place and verified. This is to prove that the intended effect of the risk reduction has been fulfilled and to ensure that no other accident risks have been adversely affected, that no new accident risks have been added and that a balance is obtained between function and system safety.

Even for accident risks that did not require a risk reducing measure, a reassessment is carried out to confirm the classification.

In order to make a new classification of an accident risk after the introduction of risk reducing measures, steps 8 - 12 are carried out where used data, assumptions and assessed results are documented.

8. Identify different proposals for risk reducing measures. Note whether the proposals affect probability/frequency, consequence, or both probability/frequency and consequence.

9. Investigate whether new accident risks arise if certain risk reducing measures are introduced.

10. Consider whether previously identified accident risks are affected if certain risk reducing measures are introduced.

11. Select the risk reducing measure(s) and repeat steps 3 - 10 in section 15.8.1 until the desired estimated risk reduction is achieved.

12. If the chosen risk reducing measure(s) are still not sufficient, personal injury exposure and controllability factors may be applied. Repeat steps 5 - 7 in section 15.8.1 until the desired estimated risk reduction is achieved.

16 System Safety Evaluation

The purpose of this chapter is to show how different actors through system safety evaluation can build up and justify how a satisfactory level of safety of technical systems and products has been achieved. The system safety evaluation is then used as a basis for a sustainable position in the current system safety decisions.

16.1 Execution of System Safety Evaluation

After completed design and/or integration work, verification and validation against the set requirements for components, products, subsystems and technical systems upstream of the various actors takes place. The aim is to find arguments and evidence strong enough to be able to show that a satisfactory level of safety has been achieved against the requirements of the current requirements document.

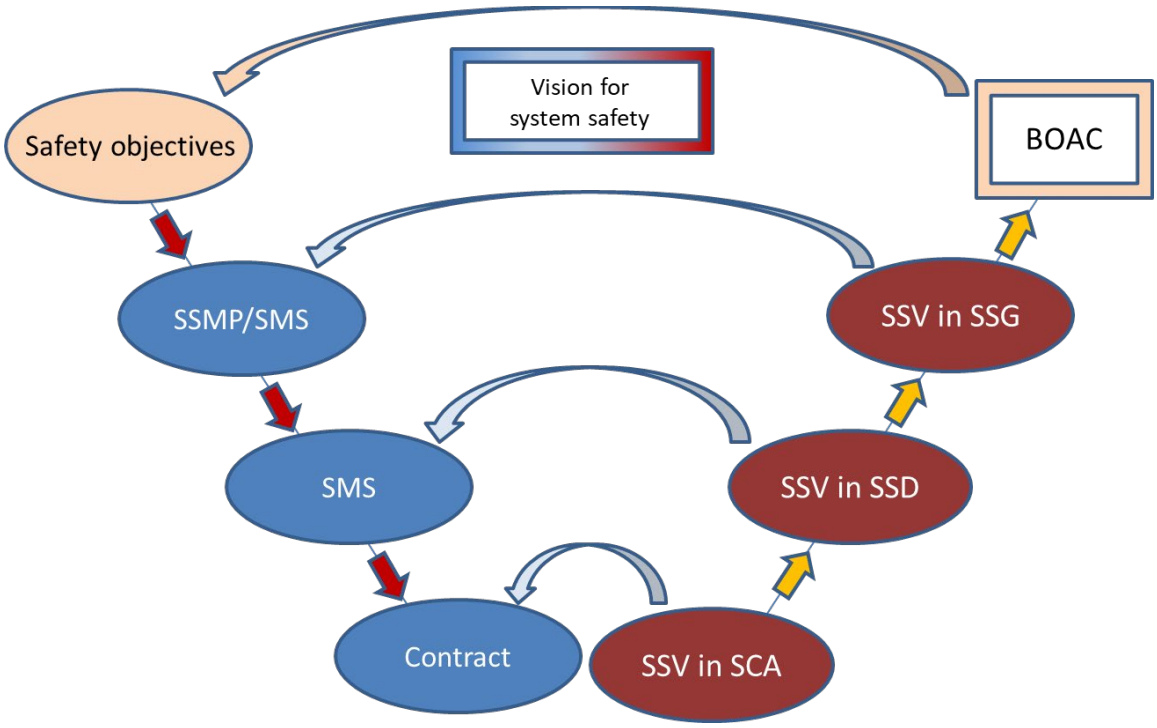


Figure 16.1 The system safety evaluation must demonstrate that the system safety requirements are met in the corresponding requirements documentation.

The permitted Route Selections may need to be reconsidered if it turns out that arguments and evidence are deemed too weak to demonstrate that the decided system safety requirements are met. For example, an approval against a particular standard by an independent certification body may be considered stronger (objective evidence), than a statement based on self-verification against the same standard. Furthermore, a system safety analysis using a fault tree showing that single failures cannot occur can be considered stronger than invoking operational experience from similar technical systems.

Arguments based on assumptions based on the activities of the Swedish Armed Forces must be presented. For example, established ways of working such as soldiers always wearing a

helmet in a combat vehicle, may be a true assumption that can be invoked. However, arguments such as that the user will not make certain errors are false and must not occur.

The system safety evaluation is based on arguments and evidence taken from the applied Route Selections (VV1 – VV7) and should be formulated by the respective actor in their system safety decisions and be structured as follows:

"The technical system (product) is safe because:"
- …
- …
- …

Overall, the system safety evaluation must show how and which EU law and Swedish legislation are met and that the set requirements for system safety are met.

The system safety evaluation can be reported in the Safety Assessment Report (SAR) with Risk Log (RL) or directly in the current system safety decision.

The Swedish Armed Forces' definitive standpoint that the technical system or product for its intended use is sufficiently safe to be put into service is made through system safety decisions, usually in *Decision on Use, Central Level* (BOAC).

16.2 Designer's System Safety Evaluation

A *designer* is a person who develops/manufactures technical systems and products based on legislation and contracts and who thus has a product safety responsibility according to EU Directive/equivalent. In the EU Directives, this is the legal manufacturer.

Prior to delivery, the *designer* reports the standpoint in the *Safety Compliance Assessment* (SCA) based on the contract and the clarifications and/or adjustments that may have occurred during the contract review. The standpoint is based on arguments and evidence taken from the applied Route Selections (VV1 – VV7), which are reported in the system safety evaluation.

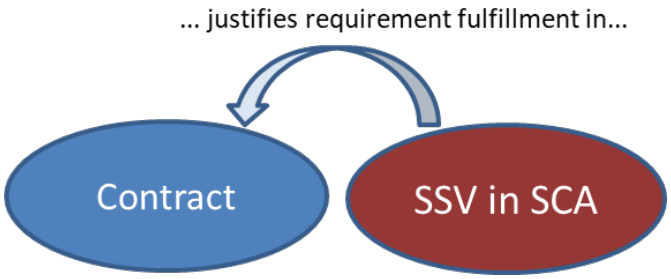


Figure 16.2 The designer's system safety evaluation must demonstrate that the system safety requirements of the contract are met.

16.2.1 SSV Route Selection 1 - Constitutional Requirements

Constitutional requirements refer to EU law and Swedish legislation with their ordinances and regulations. This also includes the Harmonised Standards which, when its more detailed requirements are met, are presumed to meet the corresponding requirements of the Constitutions. Route Selection (VV1) is a mandatory route selection.

The designer's system safety evaluation may include the following:

- That the technical system complies with the legislation at the time of delivery and is thus legal to be put into service
- That the *Declaration of Conformity* (DoC), certificate or another equivalent document is available for, for example, CE or wheel marking
    - Where a Notified body or laboratory has been used for verification/certification, this must be indicated and that it must also be demonstrated that those bodies are competent to verify the requirements of the harmonised and normative standards in question
- The existence of decisions or certificates of other authorities and what these include
- That the technical documentation *(Technical file)* is referenced and that the verification is carried out in accordance with the constitutional requirements including the applied standards. If means other than those required by the standards have been used to verify compliance with the regulatory requirements, the verification criteria and the result of the verification must be disclosed
- If a *CE-like process* has been applied, it is reported how this has been carried out as well as what has been fulfilled through this route selection and what has been handled in other route selections
- That instructions for maintenance intervals are in place and, if possible, are adapted to the Swedish Armed Forces' maintenance cycles
- That the Swedish Armed Forces' intended use fits within the above

16.2.2 SSV Route Selection 2 - Approved by Another State

Another state refers primarily to a foreign defence authority. Route Selection (VV2) is therefore not applicable in *the designer's* (industry's) system safety evaluation because that person cannot enter into an agreement with a foreign defence authority.

16.2.3 SSV Route Selection 3 - Approved by Another Party

"Other Party" refers to a civil authority, classification society, accredited laboratories, certification and inspection bodies, as well as other validation and verification bodies.

The designer's system safety evaluation may include the following:

- That the used accredited laboratories, certification and verification bodies, or bodies for validation and certification are recognised by a relevant accreditation body
- The existence of authorisations covers the current version of the technical system or product, for example:
    - Aircraft approved by civil authority
    - Ships approved by classification society

    - Road vehicles approved by inspection body
    - Pressure vessels or radios approved by third-party body (Notified body)
- CE-marked materiel, such as an electrical product, where the CE marking is based on verification by the manufacturer himself, but where *the client* has required that an independent third-party body is needed, such as an accredited body that certifies the product
- That the applied standards are relevant to the technical system or product and that the verification of the requirements of the standards has been carried out according to practice
- That the Swedish Armed Forces' intended use fits within the above

16.2.4 SSV Route Selection 4 - Other Standards

Other standards refer to industry standards that are established and internationally applied, as well as G*eneral Advice* (GA) within the scope of application.

The designer's system safety evaluation may include the following:

- That standards have been applied to enable interoperability, for example within NATO
- That motives for selected standards exist, for example:
    - MIL-STD-882, DEF STAN 00-056, GEIA-STD-0010, ISO 12100, SS-EN 61508, SS-EN ISO 13849, DO 178C and others
- That applied requirements in standards are reported, for example, on the chosen level of criticality
- That criteria for verification exist and that the results of the verification carried out show that the requirements are met

16.2.5 SSV Route Selection 5 - Design Rules

Design rules (DR) may refer to the Swedish Armed Forces' Internal Regulations (FIB), Swedish Armed Forces' *Design Rules* (DR) and FMV *Design Rules* (DR) and handbooks (design rule collections).

The designer's system safety evaluation may include the following:

- That motives for the selected *Design Rules* (DR) and handbooks (Design Rule Collections) exist
- That motives for the selected requirements from *Design Rules* (DR) and handbooks (Design Rule Collections) exist
- That criteria for verification exist and that the results of the verification carried out show that the requirements are met
- That the agreed procedure for independent review has been completed and that the result is documented

16.2.6 SSV Route Selection 6 - Proven System

Proven system means being able to rely on credible and traceable operating experience for the technical system in question or for certain subsystems.

The designer's system safety evaluation may include the following:

- That initial approval exists and that this is deemed relevant to the future intended use
- That the operating experiences are credible and traceable and is judged to be from regular and multi-year use and maintenance
- That previously identified safety deficiencies during use and maintenance have been addressed and that measures taken such as redesigns, changes in use or maintenance are documented
- That up-to-date materiel documentation and technical data are available for the current version of the technical system or subsystems

16.2.7 SSV Route Selection 7 - Risk Matrices

Risk matrices refer to that accident risks that could not be handled in the previous route selections must be evaluated against requirements for tolerable risk levels expressed in risk matrices.

The designer's system safety evaluation may include the following:

- That all remaining accident risks that could not be handled in previous route selections are classified in the required risk matrices
- That there is evidence to justify the classification of all accident risks in the risk matrix
- That the principle of ALARP has been applied to accident risks in yellow area *Limited Tolerable* (LT) and that the motives for ALARP are reported
- That special data is reported for the accident risks that have been classified in red area *Not Tolerable* (NT)

16.3 Client's System Safety Evaluation

The *client* refers to the person who procures technical systems and products based on EU law and Swedish legislation as well as *System Objective* (SMS 2).

Prior to handover, the *client* reports the position statement in the *System Safety Declaration* (SSD) based on requirements in *System Objective* (SMS 2) and the clarifications and/or adjustments that may have occurred with the *stakeholder*. The position is based on arguments and evidence taken from the applied Route Selections (VV1 – VV7), which are reported in the system safety evaluation.

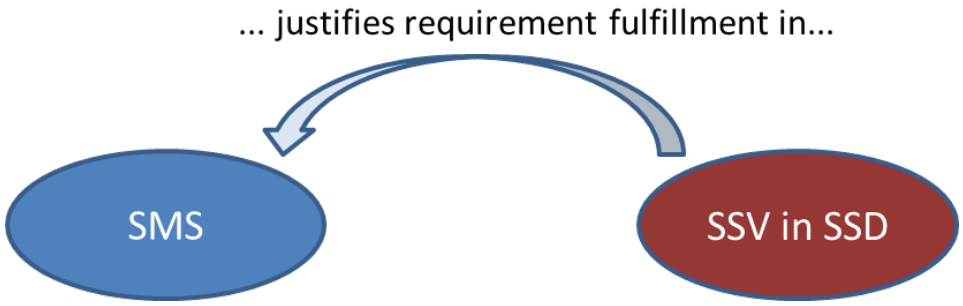


Figure 16.3 The client's system safety evaluation must show that the system safety requirements in the System Objective (SMS 2) are met.

The *Client's* system safety evaluation must show that:

- The system safety requirements in the contract have followed the focus in *System Objective* (SMS 2)
- The system safety work of the *designer* or *system integrator* has been continuously followed up to ensure that the system safety work has complied with the agreed *System Safety Program Plan* (SSPP)
- Materiel documentation and technical data are established
- *The designer's* system safety work includes use, maintenance, storage (transport) and disposal
- *The designer's* instructions for maintenance intervals comply with or are adapted to the Swedish Armed Forces' maintenance cycles
- *The designer's* arguments and evidence for the technical system are durable and thus show that a satisfactory level of safety has been achieved
- *The designer's* application of the route selections and the fulfilment of acceptance criteria are in accordance with the *System Safety Program Plan* (SSPP)
- Completed verification and validation shows that the set system safety requirements have been met

16.3.1 SSV Route Selection 1 - Constitutional Requirements

Constitutional requirements refer to EU law and Swedish legislation with its ordinances and regulations. This also includes the Harmonised Standards which, when their more detailed requirements are met, are presumed to meet the corresponding requirements of the Constitutions. Route Selection (VV1) is a mandatory route selection.

The client's system safety evaluation may include the following:

- That the technical system complies with legislation and is thus legal to be put into service
- That CE, wheel or other equivalent marking is correctly performed
- Where a Notified body or laboratory has been used, that verification has been carried out that those bodies are competent to verify the requirements of the relevant harmonised and normative standards

- That other authorities' decisions or certificates exist, for example:
    - Swedish Civil Contingencies Agency (MSB) for classification of explosives
    - Swedish Radiation Safety Authority (SSM) for permission to handle strong radiation sources
    - Food Agency (LMV) for veterinary certificates for handling foodstuffs
    - Swedish Environmental Protection Agency (NV) for the use of depleted uranium
- If a *CE-like process* has been accepted, that it is properly accounted for the materiel handled under any exemption from the CE marking and if otherwise than by the standards required to verify compliance with the regulatory requirements, the verification criteria and the result of the verification must be present
- That the Swedish Armed Forces' intended use fits within the above

16.3.2 SSV Route Selection 2- Approved by Another State

Another state refers primarily to a foreign defence authority.

The client's system safety evaluation may include the following:

- That the authorisation from another state covers the current version of the technical system or product
- That system safety work has followed an established system safety standard
- That the system safety documentation has been reviewed and deemed credible
- That the Swedish Armed Forces' intended use fits within the above

16.3.3 SSV Route Selection 3 - Approved by Another Party

"Other Party" means a civil authority, classification society, accredited laboratories, certification and inspection bodies, and other validation and verification bodies.

The client's system safety evaluation may include the following:

- That the used accredited laboratories, certification and verification bodies, or bodies for validation and certification are recognised by a relevant accreditation body
- That authorisations cover the current version of the technical system or product, for example:
    - Aircraft approved by civil authority
    - Ships approved by classification society
    - Road vehicles approved by inspection body
    - Pressure vessels or radios approved by third-party body (Notified body)
- That CE-marked materiel, such as an electrical product, where the CE marking is based on verification by the manufacturer itself, but where *the client* has required that an independent third-party body is needed, such as an accredited body that certifies the product
- That the standards applied are relevant to the technical system or product and that the verification of the requirements of the standards has been carried out according to practice
- That the Swedish Armed Forces' intended use fits within the above

16.3.4 SSV Route Selection 4 - Other Standards

Other standards refer to industry standards that are established and internationally applied, as well as G*eneral Advice* (GA) within the scope of application.

The client's system safety evaluation may include the following:

- That standards have been applied to enable interoperability, for example within NATO
- That motives for selected standards exist, for example:
  - SS-EN 61508, SS-EN ISO 13849, DO 178C and others
- That applied requirements in standards are reported, for example, the chosen level of criticality for included computer systems and software
- That criteria for verification exist and that the results of the verification carried out show that the requirements are met

16.3.5 SSV Route Selection 5 - Design Rules

Design rules (DR) refer to the Swedish Armed Forces' Internal Regulations (FIB), Armed Forces' *Design Rules* (DR) and FMV *Design Rules* (DR) and handbooks (design rule collections).

The client's system safety evaluation may include the following:

- That motives for the selected FIBs, *Design Rules* (DR) and handbooks (Design Rule Collections) exist
- That motives for the selected requirements from *Design Rules* (DR) and handbooks (Design Rule Collections) exist
- That criteria for verification exist and that the results of the verification carried out show that the requirements are met
- That the agreed procedure for independent review has been completed and that the result is documented
- That the design complies with the advice of FMV's Advisory Groups in the field of weapons and ammunition safety in accordance with the Handbook weapons and ammunition safety (H VAS) and that the formal advice of FMV's Advisory Groups is taken care of

16.3.6 SSV Route Selection 6 - Proven System

Proven systems mean being able to rely on credible and traceable operating experiences for the technical system in question or for certain subsystems.

The client's system safety evaluation may include the following:

- That initial authorisation exists and that this is deemed relevant to the future intended use
- That the operating experiences are credible and traceable and are deemed to be from regular and multi-year use and maintenance

- That previously identified safety deficiencies during use and maintenance have been addressed and that measures taken such as redesigns, changes in use or maintenance are documented
- That up-to-date materiel documentation and technical data are available for the current version of the technical system or subsystems

16.3.7 SSV Route Selection 7 - Risk Matrices

Risk matrices refer to that accident risks that could not be handled in the previous route selections must be evaluated against requirements for tolerable risk levels expressed in risk matrices.

The client's system safety evaluation may include the following:

- That all remaining accident risks that could not be handled of in the previous route selections are classified in the required risk matrices
- That there is evidence that justifies the classification of all accident risks in a risk matrix
- That the principle of ALARP has been applied to accident risks in yellow area *Limited Tolerable* (LT) and that the motives for ALARP are reported
- That the report for accident risks that have been classified in red area *Not Tolerable* (NT) is complete and that the Swedish Armed Forces' response to the request for deviation from the set system safety requirements exists.

16.4 Stakeholder's System Safety Evaluation

The Swedish Armed Forces in their role as stakeholder carry out their system safety evaluation with the support of *the Route Selection Model* (VVM). The system safety evaluation is carried out from a number of perspectives and the final standpoint is documented in a *System Safety Approval* (SSG).

16.4.1 Evaluation from the Perspective of Technical Design Responsibility

During the system handover (SÖL), the Swedish Armed Forces check that the received *System Safety Declaration* (SSD) and its attachments meet the system safety requirements set out in *System Objective* (SMS 2) and *System Safety Management Plan* (SSMP).

The current standpoint is reviewed to ensure that it demonstrates that a satisfactory level of safety of the technical system has been achieved, is comprehensive and that it does not contain any undue disclaimers. The arguments and evidence in the system safety evaluation are examined in order to find invalid or excessively weak arguments. Furthermore, any restrictions on remaining accident risks are managed by developing proposals for operating rules.

The documentation may need to be supplemented with the corresponding documentation for other products that are outside the current *System Safety Declaration* (SSD). For example,

documentation for existing equipment or from other suppliers may together constitute the technical system that the *System Safety Approval* (SSG) must cover.

16.4.2 Evaluation from the Perspective of Operational Responsibility

An evaluation from the perspective of operational responsibility is a check and quality review that the operational activities are ready to handle the technical system or product in a safe manner. Delivered technology always has limitations, which means that training, methodology and organisation as well as management are crucial components for the safe use and fulfilment of the current legislation.

Once evaluation from the perspective of technical design responsibility has been carried out, the documentation is reviewed to ensure that a satisfactory level of safety for the technical system has been achieved, is comprehensive and that proposals for operating rules are in place for any restrictions on remaining accident risks.

Furthermore, it is checked that the documentation and its annexes meet the set system safety objectives in the *System Safety Management Plan* (SSMP) and thus fits within the established system safety objectives.

The documentation may need to be supplemented with a corresponding documentation for facilities, which may be outside the relevant technical system deliveries. For example, documentation from the Swedish Fortification Agency together with the technical system may constitute the total technical system that the *System Safety Approval* (SSG) must cover.

16.4.3 System Safety Approval

After completed evaluations, the documentation is compiled together with the relevant appendices to a *System Safety Approval* (SSG). Before approval, a review is ensure by standing and any consultations are signed. After that, a decision is made on *System Safety Approval* (SSG).

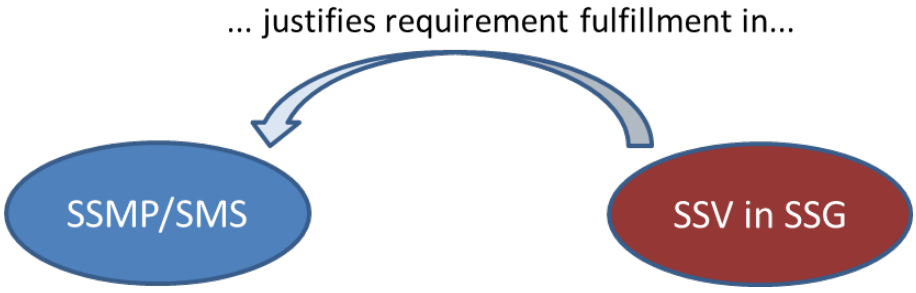


Figure 16.4 The stakeholder's system safety evaluation in the System Safety Approval (SSG) must demonstrate that the system safety requirements in the System Safety Management Plan (SSMP) and System Objective (SMS 2) are met.

17 System Safety Decisions

The purpose of this chapter is to describe the decision-making system for all actors in their different roles such as stakeholder, client and designer. Furthermore, some special cases are described that fall outside the formal system safety decisions.

17.1 Different System Safety Decisions

System Safety Decision is a collective term for *Safety Compliance Assessment* (SCA), *System Safety Declaration* (SSD), and *System Safety Approval* (SSG), which are decisions that are passed from one role to the next. These system safety decisions form the basis for *Decision on Use, Central Level* (BOAC) and *Decision on Use, Local Level* (BOAL).

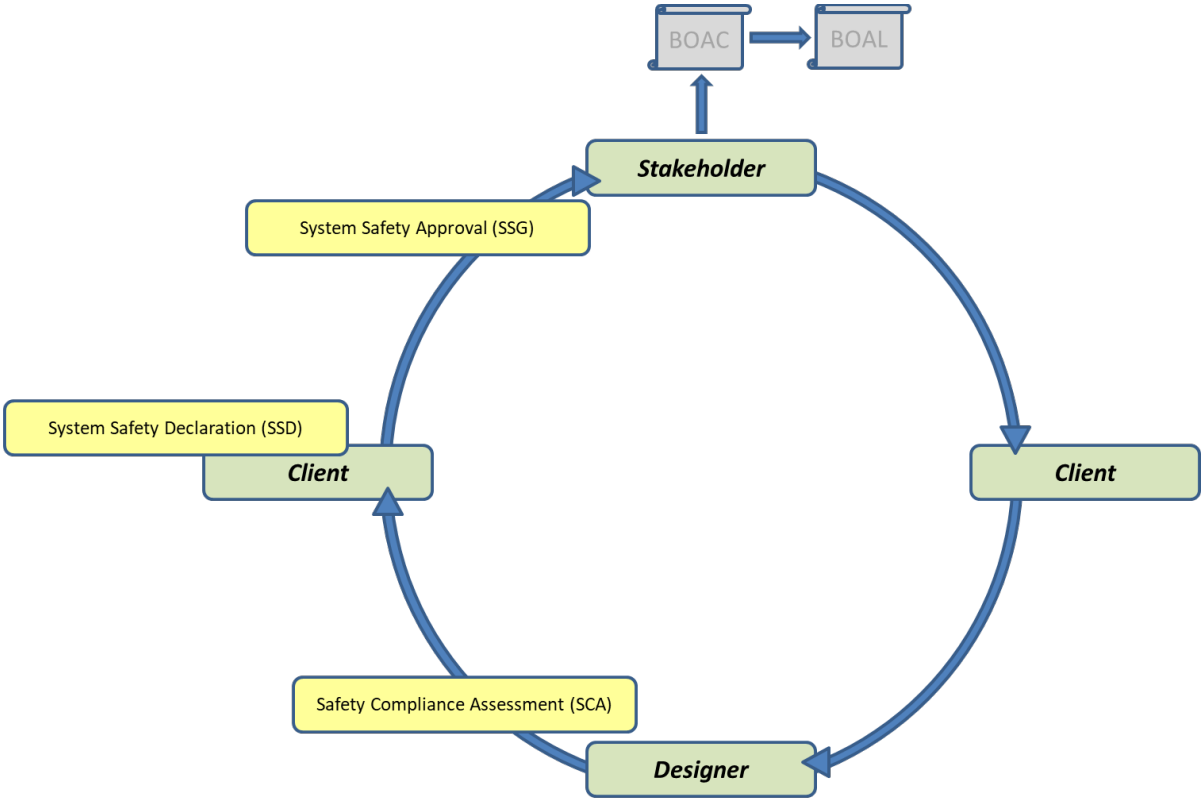


Figure 17.1 System safety decisions for handover between different roles.

The System Safety Decision must ensure that the technical system or product is ready to be put into service at the Swedish Armed Forces under the given conditions. The System Safety Decision confirms, on the one hand, that regulatory and system safety requirements are met and that the technical system, with its assembled technical documentation, offers a satisfactory level of safety.

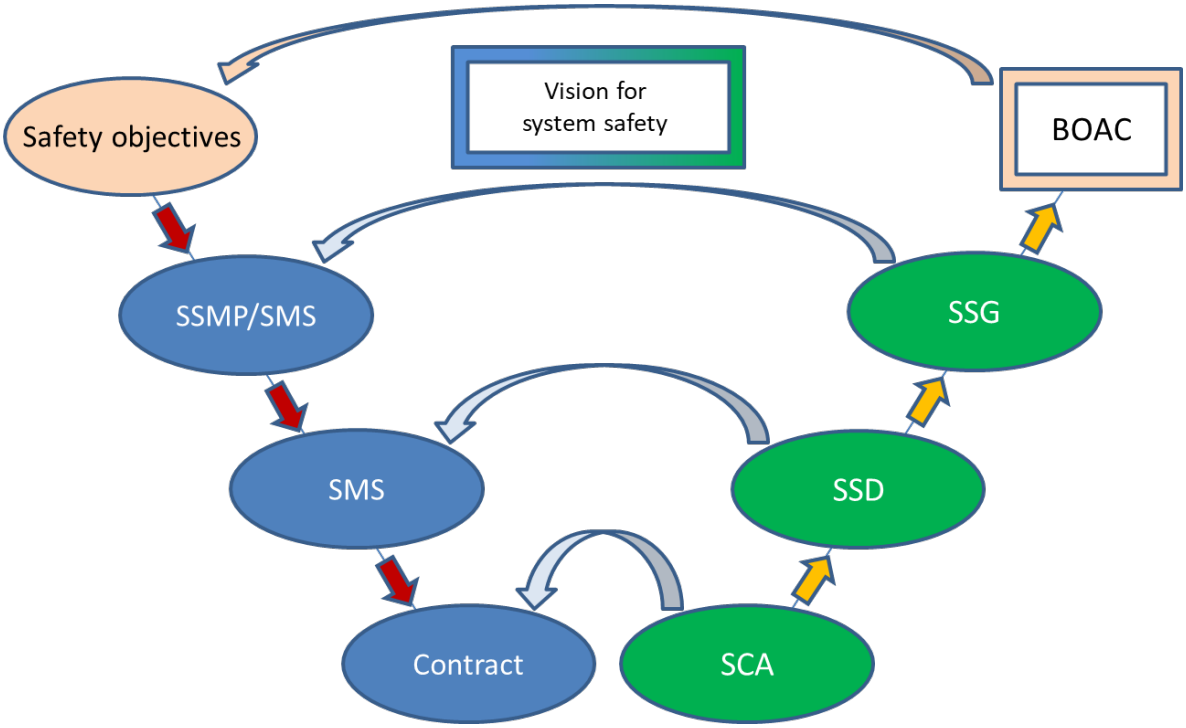


Figure 17.2 A system safety decision must demonstrate compliance with the legislation and, that system safety requirements at the corresponding level are met.

The Swedish Armed Forces' *System Safety Approval* (SSG), as the basis for *Decisions on Use, Central Level* (BOAC) and *Decision on Use, Local Level* (BOAL), must normally be applied to all technical systems and products. However, there may be motives for some disposition around decisions by pooling some of them for less risky products or when a change (modification) can be considered as part of a superordinate decision already made. For example, a change (modification) taken in a *System Safety Approval* (SSG) can be accommodated within the existing *Decision on Use, Central Level* (BOAC). The motives for this must be described in the *System Safety Approval* (SSG).

17.2 System Safety Decisions - General

The heading of the System Safety Decision must be clear and not contain epithets such as temporary, limited, time-limited, interim or for experimental use. Any need for restrictions is regulated under the current headings of the System Safety Decision.

The System Safety Decision clearly defines the permissible configurations of the technical system or product, its use environments and requirements on interfaces towards for interacting systems and facilities. Furthermore, the materiel documentation and labelling state how the system may be used, maintained, stored (transported) and decommissioned.

For remaining accident risks where agreed risk reducing measures have not yet been introduced into the technical system, restrictions must be reported as well as the criteria for lifting the restrictions.

The aggregate amount of information that has a bearing on system safety can be divided between the System Safety Decision, the *Safety Assessment Report* (SAR), the *Risk Log* (RL) and other risk documentation. For products that are, for example, CE-marked/wheel-marked, approved by another party or belong to the category COTS, all information may be contained in the System Safety Decision.

The System Safety Decision must state that legislation and requirements for system safety at the time of delivery are met. The system safety decision must be clear and transparent and not contain disclaimers.

A system safety decision is made by a competent person who, moreover, has not personally participated in the system safety work that has resulted in the decision-making basis.

17.3 Safety Compliance Assessment

The Swedish Armed Forces or Industry, in the role of *designer,* must issue a *Safety Compliance Assessment* (SCA) with the associated risk documentation. *The Safety Compliance Assessment* (SCA) must comply with the requirements of the contract (or equivalent).

The Swedish Armed Forces or FMV, in the role of the *client,* reviews the *designer's Safety Compliance Assessment* (SCA) on the basis that:

- The *Safety Compliance Assessment* (SCA) is signed by a competent person
- The position based on the conditions given is clearly formulated and is free from disclaimers
- The system safety evaluation shows that the system safety requirements of the contract are met through Route Selections (VV1 – VV6) and that managed accident risks in Route Selection (VV7) are accommodated within the *Tolerable Risk Level* (TR)
- The system safety evaluation with its arguments and evidence is judged to be sustainable and true
- Permissible configurations of the technical system are defined
- Allowed configurable parameter ranges are defined
- Usage environments and interfaces are described
- Instructions for use, maintenance instructions and warning labels are available
- Training and/or educational materiel are available
- Applicable legislation is met at the time of delivery and that any exemptions for military materiel are documented
- Required authority/agency decisions exist to bring the system into service
- Markings such as CE, CIP or wheel markings are available and that certificates such as DoC, CoC or CA are attached, alternatively referenced
- Safety Data Sheets for Chemical Products are available
- Applied civil and military safety-related standards are documented

- Risk reducing measures have been implemented and documented in the *Risk Log* (RL)
- Restrictions exist on remaining accident risks where risk reducing measures have not yet been implemented

17.4 System Safety Declaration

The Swedish Armed Forces or FMV, in the role of the *client,* must issue a *System Safety Declaration* (SSD). The *System Safety Declaration* (SSD) must meet the requirements of *System Objective* (SMS 2).

The Swedish Armed Forces in the role of *stakeholder* reviews the *client's System Safety Declaration* (SSD) on the basis that:

- The *System Safety Declaration* (SSD) is signed by an authorised person
- The position based on the conditions given is clearly formulated and is free from disclaimers
- The system safety evaluation shows that the system safety requirements in *System Objective* (SMS 2) are met through Route Selections (VV1 – VV6) and that managed accident risks in Route Selection (VV7) are accommodated within the *Tolerable Risk Level* (TR)
- The system safety evaluation with its arguments and evidence is judged to be sustainable and true
- Permissible configurations of the technical system are defined
- Allowed configurable parameter ranges are defined
- Usage environments and interfaces are described
- Materiel documentation and warning markings for use and maintenance are established
- Training and/or educational materiel are available
- Applicable legislation is met at the time of delivery and that any exemptions for military materiel are documented
- Required authority/agency decisions exist to bring the system into service
- Markings such as CE, CIP or wheel markings are available and that certificates such as DoC, CoC or CA are attached, alternatively referenced
- Safety Data Sheets for chemical products are available
- Applied civil and military safety-related standards are documented
- Risk reducing measures have been implemented and documented in the *Risk Log* (RL)
- Restrictions exist on remaining accident risks where risk reducing measures have not yet been implemented
- Any records from reviews of the *Safety Compliance Assessment* (SCA) are available
- If the technical system includes weapons, ammunition or explosives:
    - Minutes from FMV Advisory Groups exist and that advice is commented and justified
    - Lists of approved ammunition that may be used in the weapon system exist, alternatively that the ammunition is approved for certain weapon systems

17.5 System Safety Approval

The Swedish Armed Forces in the role of *the stakeholder* must issue a *System Safety Approval* (SSG). This decision confirms the fulfilment of the *client's System Safety Declaration* (SSD) and that any proposed restrictions on remaining accident risks are reasonable and are taken care of by temporary operating rules.

The *stakeholder* prepares the *System Safety Approval* (SSG) by ensuring that:

- Compliance with legislation and that any exemptions for military materiel and/or military use are documented
- A safety management system is available, if required
- Required authorisations/permits from authorities are available
- Operating rules are available, such as the basis for SäkR
- Restrictions on remaining accident risks exist
- Materiel documentation for use and maintenance is available
- The technical system is registered in various management systems
- Training documentation for training instructors and users is available
- Requirements for interfaces with other technical systems and products exist and comply with the requirements imposed.
- Requirements for basic resources, premises and/or equipment are specified and that requirements are met
- Safety Data Sheets for chemical products are registered in management systems
- A *System Safety Working Group* (SSWG) is available
- Operational experiences can be reported
- Ammunition monitoring is established

The stakeholder formulates a position that both the system safety requirements of the *System Safety Management Plan* (SSMP) for the product area and *System Objective* (SMS 2) for the technical systems are met.

In cases where the Swedish Armed Forces integrate materiel into facilities built by the Swedish Fortification Agency, additional system safety work is required for the integration. The Swedish Armed Forces have to demand construction documents for basic resources such as electricity, power, heating, cooling, ventilation, water and sewage from the Swedish Fortification Agency. In addition to the physical outer and interior dimensions of the facility, different weights and placement on floors or other surfaces may also limit its use. When existing or new materiel is integrated into these basic resources and/or within the framework of physical constraints, integration risks may arise. Furthermore, the total fire load needs to be analysed and evacuation routes be tested. This system safety work is documented in a *Safety Assessment Report* (SAR) with *Risk Log* (RL), and appended to the *System Safety Approval* (SSG).

17.6 Decision Regarding Use, Central Level

The Swedish Armed Forces in the role of *stakeholder* must also include system safety in the decision gate *Decision on Use, Central Level* (BOAC), including system safety.

The system safety basis must show that:

- A possible approval from the *Delegation for the International Law Review of Weapons Projects* is available
- System Safety Objectives in the *System Safety Management Plan* (SSMP) are met
- System Safety Requirements in *System Objective* (SMS 2) are met
- *System Safety Approval* (SSG) is established

If the *System Safety Approval* (SSG) is not approved, the corresponding documentation and positions must be presented in the *Decision on Use, Central Level* (BOAC).

The *Decision on Use, Central Level* (BOAC) governs what is to be managed in the *Decision on Use, Local Level* (BOAL). This may include, for example, requirements for training personnel or access to basic facilities, premises or equipment. If the *Decision on Use, Local Level* (BOAL) is not necessary, this must be stated in the *Decision on Use, Central Level* (BOAC).

17.7 Decision Regarding Use, Central Level

The Head of the Organisational Unit of the Swedish Armed Forces (C OrgE) in the role of employer with delegated occupational health and safety responsibilities must issue a *Decision on Use, Local Level* (BOAL), which is a local decision that also includes system safety.

In the decision gate, requirements from the *Decision on Use, Central Level* (BOAC) may need to be managed, such as:

- Procedures for risk management when introducing new materiel and/or methods exist
- Materiel documentation and SäkR are available
- Any restrictions are known and understood by users and maintenance personnel
- Handling of hazardous substances, including explosives can take place
- Management of expected software updates can be implemented
- Implementation of training for users and maintenance personnel can take place on an ongoing basis
- Feedback of operational experiences, for example in the form of operational data, takes place

For materiel for which the Swedish Armed Forces have the technical design responsibility, modification and technical adaptation is carried out through a Technical Order (TO), decided by the Technical Design Manager. Management of this is done according to internal procedures in the organisation and may ultimately lead to a new *Decision on Use, Local Level* (BOAL).

Where the procurement of technical systems or products is carried out under OrgE's own direction, the Head of Organisational Unit (C OrgE) must make a *Decision on Use, Local*

Level (BOAL) which corresponds to the scope and content of a *Safety Compliance Assessment* (SCA).

17.8 Other Cases Outside the Formal System Safety Decisions

The purpose of this section is to describe certain special cases that fall outside the formal system safety decisions.

17.8.1 System Safety Announcement

System Safety Announcements (SSM) are used by the operator who wishes to inform the Swedish Armed Forces in the role of a *stakeholder* about a safety deficiency in a technical system or product, or of any shortcomings and inaccuracies in its use, maintenance or handling, without rescinding an issued system safety decision. A *System Safety Announcement* (SSM) applies until the safety defect has been rectified.

A *System Safety Announcement* (SSM) should include at least:

- Identification of a technical system or product
- Analysis of the incident or observation
- Risk assessment
- Proposal(s) for recommendations

If several different events or observations exist for the same technical system or product, it is recommended that one *System Safety Announcement* (SSM) be issued per observation. This simplifies the administration when deciding that the safety defect has been rectified.

If a *System Safety Announcement* (SSM) means that information to clarify, inform or remind the user of conditions related to the intended use, change of use including norm slippage or that operating rules need to be tightened, the case may be closed by the Chairman of the *System Safety Working Group* (SSWG), and new system safety decisions need not be issued.

If a *System Safety Announcement* (SSM) means that a Technical Order (TO) for modification needs to be developed, new system safety decisions are issued.

A *System Safety Announcement* (SSM) may be recalled by the issuer if the safety defect is no longer considered current. Such an action is documented by the Chairman of the *System Safety Working Group* (SSWG) in minutes or meeting notes.

17.8.2 System Safety Certificate

System Safety Certificates (SSI) are issued prior to verification and validation of technical systems and products. There are a number of different methods for both objective and subjective evaluations.

A *System Safety Certificate* (SSI) must correspond to a *System Safety Declaration* (SSD) when it comes to scope and content, but be limited to planned activities described in a particular test program or test plan.

The test or trial organisation reviews the *System Safety Certificate* (SSI) on the basis that:

- The *System Safety Declaration* (SSD) is signed by an authorised person
- Test program or test plan available

- Sample object, with its permissible configurations and configurable parameter ranges, is approved for the planned operations
- *Safety Assessment Report* (SAR) is available with identified accident risks and proposed restrictions, which can be based on the *designer's Safety Compliance Assessment* (SCA)
- Usage environments and interfaces are described
- Required materiel documentation and warning markings for use are available
- Safety Data Sheets for chemical products are available

Where the technical system contains weapons, ammunition or explosives, minutes from the FMV Advisory Group must be included and proposed advice must be managed.

System Safety Certificates (SSI) may be issued for organisational and methodology trials conducted under the direction of the Swedish Armed Forces.

Safety certificates are issued for warships carrying out test operations with a Sea Trial Command (PTK). The content and scope of the safety certificate is regulated in a special order.

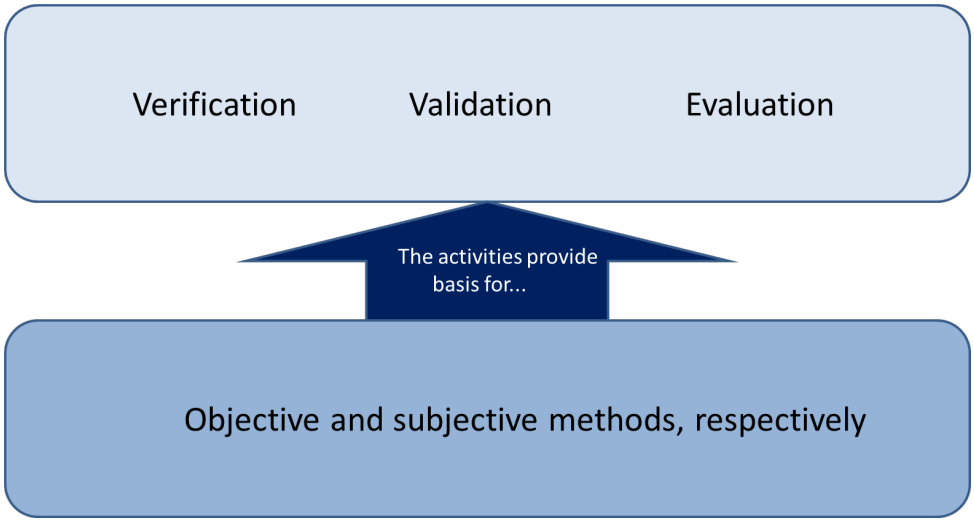


Figure 17.3 Description of verification and validation.

17.8.3 Lending of Materiel from FMV to the Swedish Armed Forces

If the Swedish Armed Forces borrow materiel from FMV before the system handover (SÖL) is implemented, an agreement between the parties should be developed. The agreement should include:

- Activity description
- Date (period) and units involved
- Technical execution (type configuration) including materiel documentation
- Individual designations, alternatively the number of products if there is no individual designation
- *Safety Compliance Assessment* (SCA)
- The client's *Safety Assessment Report* (SAR) with *Risk Log* (RL)

- Restrictions on remaining accident risks
- Need for Personal Protective Equipment (PPE)
- Training
- Division of responsibilities between the actors
- Procedures for coordination meetings (e.g. SSWG)

17.8.4 Lending of Materiel to Another Authority or Municipality

If the Swedish Armed Forces lend materiel, without accompanying personnel, to another authority or municipality for the purpose of promoting the safety of the community, this organisation needs information about any exemptions for military materiel or military use. They also need the required materiel documentation and to be informed about other matters such as risk areas, Personal Protective Equipment (PPE) needs or training requirements. The other authority or municipality is then given the opportunity to take its own measures to compensate for the Swedish Armed Forces' exemption for military materiel or military use. The Swedish Armed Forces notify any exemptions and other relevant information in loan documents.

17.8.5 Technical Design Responsibility in Export, Rental and Lending

If the Swedish Armed Forces, or other organisation such as FMV, provide materiel to another state, that organisation becomes the technical design manager. In cases where it is an export configuration, a *System Safety Management Plan* (SSMP) is required. If necessary, a *System Safety Program Plan* (SSPP) can also be developed for the expected system safety work prior to various changes (modifications) and deliveries to another state.

Using the manufacturer's basis, the Swedish Armed Forces, or other organisation such as FMV, may issue a *System Safety Approval* (SSG) for the export configuration of the technical system. System safety decisions and risk documentation are issued in the language agreed upon in contract with the relevant state (other defence authority).

17.8.6 System Integrator's System Safety Work

The *system integrator* conducts system safety work in accordance with the *client's System Safety Program Plan* (SSPP) to handle combined technical systems and products such as software or physical products. Such a system-of-systems means new functionality and new combinations of physical products. System safety work is documented in the *Safety Assessment Report* (SAR). The system safety analysis is based on the *System-of-Systems Hazard Analysis* (SoSHA) activity.

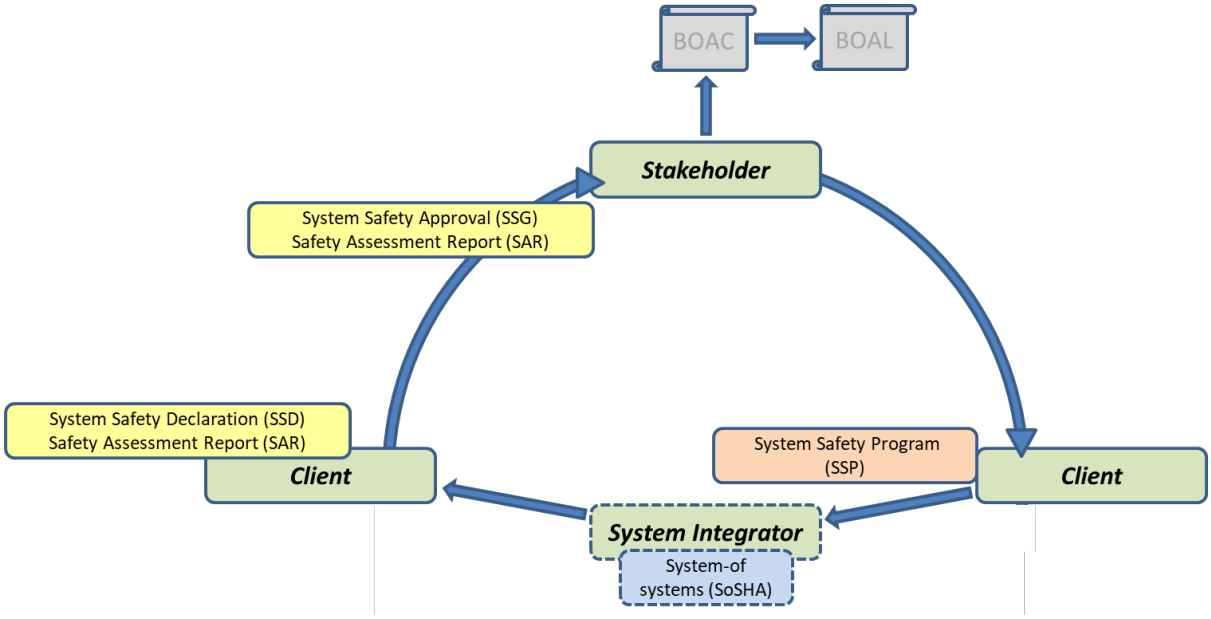


Figure 17.4 System Integrator´s System Safety Work.

18 Changes and Modifications of Technical Systems

The purpose of this chapter is to describe different variants of changes (modifications) and to focus on the scope of the system safety work that needs to be carried out.

18.1 Grounds for Changes (Modifications)

Changes refer on the one hand to modifications to technical systems and on the other hand to changes to operating rules, materiel documentation, maintenance, training, storage, modes of transport and more for the technical system.

Modifications refer specifically to the design (configuration) of the technical system with respect to mechanical parts, electronics, software or other parts. Modifications may involve performance enhancements to the existing technical system or the addition of new subsystems with new functionality.

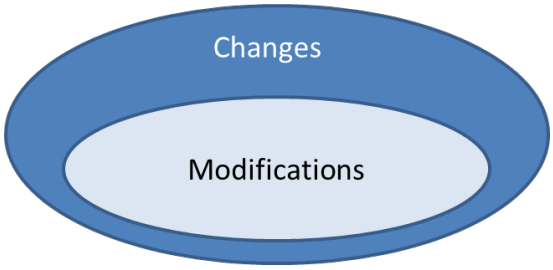


Figure 18.1 Modifications are a subset of changes.

There may also be changes (modifications) that are introduced temporarily and to a limited extent for certain activities or when managing technical systems in the battle line.

18.2 Reasons for Changes (Modifications)

The Swedish Armed Forces have technical design responsibility for all technical systems and products and are responsible for leading the system safety operations so that they can maintain a satisfactory level of safety throughout their lifetime. This can be done through necessary or predetermined changes (modifications). All technical systems and products handed over to (received by) the Swedish Armed Forces are regulatory counted as put into service, that is, considered as second-hand.

The need for changes (modifications) can arise for many different reasons such as new legislation, addressing identified safety deficiencies, dealing with changing modes of use including norm slippage, changing training, different environmental environment, changing maintenance intervals or that spare parts of the original design are no longer available. Changes (modifications) can also be introduced based on changed requirements to improve accessibility or achieve changed functionality to provide increased capability of the units.

Before changed (modified) technical systems can be put into service, they must have undergone the necessary system safety work and be determined to be sufficiently safe for the intended use.

18.3 Permanent Changes, New System Objective

With a new edition of *System Objective* (SMS 2), change requirements for the technical system are established. For such predetermined changes (modifications), corresponding system safety activities are carried out as for the procurement of new technical systems or products. New system safety decisions need to be issued.

18.4 Permanent Changes, Original System Objective

When changing (modifying) existing technical systems or products, with the intention of maintaining technical capability and performance over time, i.e. within the original *System Objective* (SMS 2), the system safety work needs to be adapted to the impact of the change (modification) on existing system safety evaluation and the Route Selections (VV) on which it is based.

If the change (modification) takes place within the framework of a previous approval according to the Route Selection (VV1), for example, regarding CE marking, VV2 or VV3), no system safety work needs to be carried out if it can be demonstrated that the change (modification) is within the scope of this approval and that the approval is still fully valid and fits within the Swedish Armed Forces' intended use. Decisions, if this is the case, are made in connection with the approval of the Technical Order (TO).

If the change does not fit within previous approvals for Route Selections (VV1 – VV3), this needs to be investigated under a separate arrangement.

Changes (modifications) are normally regulated through a Technical Order (TO). In the Technical Order (TO), the grounds for determination with regard to system safety are presented or referenced. The TO presents existing or new system safety decisions and justifications that the system safety work is satisfactory. The system safety work must take care of the new configuration of the technical system and show that the workflow during the practical work on the introduction of the change (modification) is safe. Note that new system safety decisions may be needed from the different actors in the roles of *designer, client* and *stakeholder* depending on the nature of the change.

18.5 Change (Modification) of Products Verified Under Civil Regulations

In cases where a used product that has previously been verified according to civil regulations is intended to be changed (modified), the CE marking may need to be reworked. The change may be a *minor/non-significant change* or a *significant/substantial change*. This may be decided on a case-by-case basis with the support of EU guides and possibly with the support of the manufacturer who carried out the verification, for example the CE marking or the wheel marking.

Experience has shown that most changes (modifications) of machines have been deemed to be *non-significant changes*, and therefore the existing CE marking is considered to be valid. When changing (modifying) a product, risk reducing measures must always be taken for the identified accident risks. Verification must take place against the requirements of the EU

Directives and the results must be documented. This is done even if it concluded that the CE marking, including compliance with the essential health and safety requirements, has not been affected by the change (modification). Such a change (modification) is then designated as a *non-significant change*.

A *significant change* implies that the manner in which the product complies with the essential health and safety requirements of the EU Directive has changed, which is why the conformity assessment and the CE marking needs to be reworked. This is normally difficult and complicated. In case of doubt, it is recommended that a contact be made with the manufacturer who carried out the CE marking for a discussion of the planned change (modification) before its introduction.

18.6 Temporary Changes (Modifications) Introduced by the Swedish Armed Forces

In the event of temporary changes (modifications) such as technical adaptation, temporary repair or war damage repair, basis for the decision regarding system safety needs to be produced for the current situation to the extent necessary.

18.6.1 Technical Adaptation

'Technical adaptation' means a temporary change (modification) of a technical system which, immediately after the end of its operation, is to be restored to the original and established configuration. Technical adaptation is carried out via a technical order (TO) decided by the person with the design responsibility.

From a system safety point of view, technical adaptation should include:

- Requirements for decision-making (description of the purpose of technical adaptation, alternative possible measures, advantages and disadvantages of the respective alternatives)
- Minimum system safety analysis requirements
- Minimum documentation requirements of the action carried out
- Minimum materiel documentation requirements for the user
- How to report the implemented action for the technical system (certain items)
- When and how decisions are made on the restoration of the technical system
- How to report the restoration of the technical system (certain items) after the technical adaptation

18.6.2 Temporary Repair or War Damage Repair

Temporary repair or war damage repair means an alternative repair by a non-standard method and/or by repair components (replacement of original spare parts) pending regular repair.

Temporary repair or war damage repair may be relevant in the case of, for example, the handling of the technical system that needs to be moved pending salvage or towing to the workshop.

The Swedish Armed Forces continuously decide on alternative repair methods. Decisions on repair methods outside of established maintenance instructions should include, from a system safety point of view, the following:

- Decision-making power
- Requirements for decision-making (description of the purpose of technical adaptation, alternative possible measures, advantages and disadvantages of the respective alternatives)
- Minimum system safety analysis requirements
- Minimum documentation requirements of the action carried out
- Minimum materiel documentation requirements for the user
- How to report the implemented action for the technical system (certain items)
- When and how decisions are made on the restoration of the technical system
- How to report that the technical system (certain items) was restored after temporary repair/war damage repair

18.7 Older Materiel that Lacks System Safety Decisions

In 1996, the Swedish Armed Forces decided that all new or modified technical systems and products should have system safety decisions. System safety decisions are required both for the Swedish Armed Forces to receive the materiel and for the equipment to be put into active service in units. Technical systems and products put into service before 1996 are *considered de facto* approved (proven system) and do not normally require any system safety decisions as long as they are used and maintained in accordance with the operational experiences available.

If there is materiel in use that lacks system safety decisions prior to changes (modification), this needs to be handled by the Swedish Armed Forces before the configuration handover (KÖL).

The Swedish Armed Forces may choose to retroactively carry out a complete system safety audit for the entire technical system, or to only impose requirements to carry out system safety work on the parts covered by the change (modification). The system safety decisions will then have the scope chosen as above.

If the Swedish Armed Forces choose to carry out retroactive system safety work for the complete technical system, the original documentation that once approved the equipment for use needs to be produced if possible. With this documentation as a basis, a complete system safety work can be carried out.

Alternatively, the technical system can be managed as a proven system, where credible and traceable operational experiences are relied upon. This may include analysing previous accident, incident and fault reports. The results of the system safety analysis are documented in a *Safety Assessment Report* (SAR) and are the basis for the current system safety decisions.

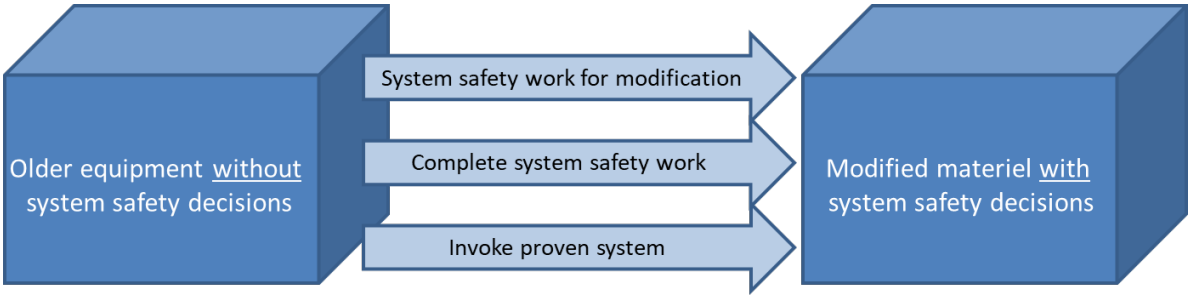


Figure 18.2 Three alternative ways to manage system safety work when modifying older materiel

19 Decommissioning of Technical Systems

The purpose of this chapter is to describe the scope of the system safety work that needs to be carried out depending on the way in which technical systems and products are to be decommissioned.

19.1 Background to the Disposal Work

The Swedish Armed Forces are the owner representatives of the state's defence materiel. Technical systems with the exemption of military materiel often contain components with large energies or with multiple hidden/embedded sources of risk. The Swedish Armed Forces therefore need to identify the accident risks that may occur during the physical disposal of the current technical system.

It is the responsibility of the Swedish Armed Forces to provide information to the person who acquires materiel for continued use or receives materiel for destruction/scrapping, the nature of these accident risks and the characteristics of current sources of risk. It primarily applies to such characteristics that are not normally found in materiel without exception for military materiel. Thus, the Swedish Armed Forces should ensure that the materiel offers a satisfactory level of safety.

All materiel being decommissioned is to be seen as in service, that is, it is considered second-hand. The Swedish Armed Forces decide on total disposal, partial culling or discarding of materiel. Decommissioning of materiel can occur in various ways such as transfer, sale or destruction. The materiel can also be transferred as museum objects or exhibits. Transfer and export restrictions may exist for certain materiel classed, for example, as munitions.

19.2 Final Use

Final use implies, before total disposal occurs, that the products, such as ammunition or batteries, are used until they expire. If operating profiles change, it may be necessary to issue an updated *System Safety Approval* (SSG).

19.3 Implementation of System Safety Analysis Prior to Disposal

The Swedish Armed Forces ensure that a *Risk Assessment prior to Disposal of Systems* (RADS) is carried out. The purpose of RADS is to identify and analyse accident risks that may occur during physical disposal. The accident risks are related to the materiel or to the disposal method (including utilities and work operations). If the technical system is relatively modern, that is, system safety analysis has been carried out during procurement, much information on the potential accident risks of the technical system associated with planned disposal has already been identified. In addition, materiel documentation in the form of repair handbooks and spare parts catalogues can be used in RADS and be used in the removal of subsystems and components.

If the Swedish Armed Forces' system safety methodology has not been followed during procurement, *RADS* will become more comprehensive. This also applies if there are

deficiencies in the type configuration documentation or if the materiel has been unduly modified during the maintenance stage and documentation is consequently missing or deficient. The Swedish Armed Forces conduct the configuration handover (KÖL) to the operator carrying out the disposal work.

The following describes the system safety work that needs to be carried out during the disposal phase depending on the complexity, nature and risk content of the technical system.

19.3.1 Transfer

Transfer means that technical systems or products are handed over (given away) by the Swedish Armed Forces to a new owner such as state or municipal activities, alternatively to humanitarian and voluntary organisations. The Swedish Armed Forces need to document the status/deficiencies of each item or product and ascertain that sufficient product information for the type configuration is available. Product information may consist of materiel documentation for use and maintenance including maintenance documentation, schedules, drawings, Safety Data Sheets, system safety analyses and training materiel. Information needs to be provided on such properties of the materiel that are not normally found in military materiel.

Certain exemptions for military materiel directly linked to the use of the Swedish Armed Forces may expire, which depends on how the exemption has been formulated in the current regulatory framework. It will be the responsibility of the new owner to examine the consequences of this, such as whether new verifications and approvals are needed or if the use has restrictions.

In addition to any end-user certificate, there may also be transfer and export restrictions.

19.3.2 Sales

Sales mean that technical systems or products are sold to legal entities (companies, organisations) or individuals. The Swedish Armed Forces need to document the status/deficiencies of each item or product and ascertain that sufficient product information for the type configuration is available. Product information must consist at least of material documentation for use and maintenance. Schedules, drawings, Safety Data Sheets, system safety analyses and training materiel should also be handed over to legal entities. Information needs to be provided about such properties of the materiel that are not normally found in military materiel.

Certain exemptions for military materiel directly linked to the use of the Swedish Armed Forces may expire, which depends on how the exemption has been formulated in the current regulatory framework. It will be the responsibility of the new owner to examine the consequences of this, such as whether new verifications and approvals are needed or if the use has restrictions.

Older products (which if they were new would be subject to CE marking/wheel marking) that are not CE-marked/wheel-marked may be sold, but it should be kept in mind that the products are less attractive on the market, especially for new owners who are employers when they, for example, must take into account regulations (AFS 2006:4). Use of work equipment, which

also imposes certain technical requirements. Products that are machines may be handled on a case-by-case basis.

This could mean that opportunities for revenue to the Swedish Armed Forces are lost and disposal costs may be taken. To subsequently try to CE-mark/wheel-mark a product can cost very large amounts, if it is even possible to obtain the required technical data.
CE marking/wheel marking should therefore be aimed at when the materiel is acquired. This also means that the person who voluntarily or not, CE-marks/wheel marks such a product is to be regarded as the legal manufacturer with all that it implies in terms of liability and obligations.

19.3.3 Destruction

Destruction means that technical systems or products are physically destroyed. Note, however, that some subsystems and components may be taken care of by the Swedish Armed Forces before destruction if subsystems/products can be reused in similar technical systems.

A technical system is prepared by emptying hazardous substances, removing radiation sources, tensioned springs/pressure vessels or other structures are released, and removing foreign objects such as ammunition that has been left behind or other foreign objects. Components subject to producer liability are sorted out and submitted to the collection systems provided by the producers. The Swedish Armed Forces can inform the above through a Declaration of Destruction and allow the operator carrying out the destruction to manage this.

Information on hazardous substances/surface treatments which are hidden or difficult to detect, such as substances referred to in Article 33 of the EU Regulation REACH and on its list of candidates, must be provided to the destruction operator through the care of the Swedish Armed Forces. Such information may be specified in the Recycling Handbook or a corresponding document.

The Swedish Armed Forces administer the Destruction Declarations.

19.3.4 Museum Objects

Museum objects mean that technical systems or products are transferred to be exhibited to the public's view in a museum or equivalent. A museum is to be seen as the new owner of the materiel unless the museum is located at a unit.

Complete product information, if available, is submitted to the museum and may consist of materiel documentation for use and maintenance including maintenance documentation, schedules, drawings, Safety Data Sheets, system safety analysis and training materiel. Information needs to be provided about any properties of the materiel that are not normally found in military materiel.

In case of a request for the transfer of museum objects to another country, in addition to any end-user certificate, there may also be transfer and export restrictions, for example for some hazardous substances or for military designs.

19.3.5 Display Objects

A display object remains in the possession of the Swedish Armed Forces and can, for example, be placed at a unit. The display object must normally be emptied of all contents, such as engine, hazardous substances and fittings. Moving parts such as doors and hatches should be welded closed and protruding parts be removed.

Concepts

This handbook uses a large number of concepts that, from a system safety perspective, are used to explain different contexts. In cases where the handbook has its own glossary (own wording or adjusted from other literature) is stated "H SystSäk 2022".

Concept	Reference	Glossary
Ability	H GOALS FORB 2011	The fact that someone (a unit) is able or able to do/accomplish something.
Accident	H SystSäk 2022	An accident occurs when a person, property and/or external environment is damaged by the source of the risk as a result of the occurrence of the hazardous event.
Activity	FOI-R-3546-SE ISSN 1650-1942	A defined amount of work to be done, including any input and output requirements.
Activity rules	H SystSäk 2022	Restrictions or limitations on the use of technical systems or products for the purpose of managing remaining accident risks.
ALARP	H SystSäk 2022	The concept of ALARP (*As Low as Reasonably Practicable)* means weighing an accident risk against the problems, time and money needed to reduce the accident risk to as low a *level* as is practically possible based on good practice, i.e. that established standards and *Design Rules* (DR) have been followed based on today's level of technology.
Basic resources of civil engineering	H SystSäk 2022	For example, resources such as electricity, power, heating, cooling, ventilation, water and sewage.
CE marking	EU Blue Book 2016	The marking, made by the manufacturer, indicates that the product is in conformity with the EU legislation (transposed into national law) applicable to the product and that it can thus be placed on the internal market.
Changes	H SystSäk 2022	Includes modifications (permanent or temporary), changed operating rules, changed materiel documentation for use and maintenance, changed environmental environment, and changed training.
Client	H SystSäk 2022	Actor who carries out procurement and who hands over materiel to the *stakeholder*.
Component	FOI-R-3546-SE ISSN 1650-1942	A unit, with discrete structure within a system, that interacts with other components of the system and thus contributes at the lowest level to the system and characteristics of the system.
Concept	FOI-R-3546-SE ISSN 1650-1942	A fundamental idea or basic concept of how different parts should be combined or coordinated.

Concept	Reference	Glossary
Configurable Parameter Ranges	H SystSäk 2022	Approved intervals for software settings as well as allowed updates to individual data or databases.
Contract	H SystSäk 2022	Documents that refer, among other things, to specified system safety requirements (Technical specification and/or Operative Commitment Specification) between *the client* and *the designer*.
Contributing causes	H SystSäk 2022	Contributing causes are conditions that, together with a source of risk, provide the conditions for a hazardous event.
Controllability factor	H SystSäk 2022	Controllability factors mean that the user can influence a dangerous state himself by stopping the chain of events or taking some protection before the hazardous event occurs.
COTS products	H SystSäk 2022	COTS (*Commercial Off the Shelf*) products include products that are already on the market and may be approved by an accredited body against international standards.
Dangerous condition	H SystSäk 2022	A physical situation that can lead to an accident.
Decision gate	FOI-R-3546-SE ISSN 1650-1942	Checkpoint between different life cycle stages. The principle, comprehensive decisions based on predefined decision criteria, which are taken at the respective decisions.
Declaration of Conformity	EU Blue Book 2016	The document in which the manufacturer indicates and certifies that the product individual complies with all the relevant requirements of the applicable legislation. Also known as EU assurance regarding conformity.
Design rules	H SystSäk 2022	Design impacting requirements.
Designer	Boverket Wikipedia	Supplier who meets the set contract requirements by designing or inventing something and also the person who performs design drawings and performs calculations.
Disposal	H SystSäk 2022	Disposal of materiel through final consumption, sale, transfer or destruction/landfill.
Distributor	Tradepartners-Sweden	A distributor is an economic actor who purchases goods and then resells the goods to the client himself. The distributor has its own warehouse, sends to and invoices his client himself.
Environment	H SystSäk 2022	Consists of other technical systems and products (including hazardous substances), installations and nature and climate. The interfaces of the technical system with the environmental environment can be mechanical, electrical or information technology.

Concept	Reference	Glossary
Ergonomics	IEA, International Ergonomics Association	Scientific discipline that deals with understanding interactions between people and other parts of a system as well as the profession in which one applies theory, principles, data and methods to optimise in design human well-being and overall system performance.
Evaluation	H SystSäk 2022	Investigation of the properties a technical system has and how it can be used and put to use in other contexts.
Evidence	H SystSäk 2022	Evidence or other information that fully or partially substantiates various arguments.
Exposure factor	H SystSäk 2022	The probability that a user is present and will be exposed to a hazardous event when it occurs.
Final use	H SystSäk 2022	The products, such as ammunition in storage, are used until they run out.
General advice	H SDH 2021	Format of non-binding rules in the form of general recommendations on the application of a statute specifying how someone can or should act in a particular respect.
Handbook	H SDH 2021	Type of document that contains instructions with explanations and descriptions regarding a particular activity or administration and management. A handbook may reproduce laws, ordinances, rules, regulations and handbooks. A handbook may also contain guidelines, advice and recommendations with images for the application of rules and regulations. A handbook can also describe procedures and processes, which can be published separately on the Swedish Armed Forces' intranet. The procedures, processes, advice, guidelines and recommendations etc. that are stated should always be followed unless there are special reasons to carry out the activities in another way.
Harmonised Standard	EU Blue Book 2016	A European standard adopted on the basis of a mandate from the European Commission for the application of a legal act of Union harmonisation legislation, such as a specific EU Directive, and set out in EU's Official Journal. Harmonised Standards are voluntary to apply, unless otherwise agreed.
Hazardous event	H SystSäk 2022	A hazardous event occurs unintentionally and without intent and can result in an accident or incident.
Hazardous substances	Wikipedia	According to European legislation, these are chemicals that are difficult to degrade, are concentrated in the food chain (bio accumulative) and have one or more toxic properties.
Human factors	Wikipedia	The application of physiological and physiological principles to the design of products, processes and systems.

Concept	Reference	Glossary
Incident	H SystSäk 2022	An incident means that a hazardous fire event occurs but it does not cause any harm. (An incident is, for example, when a foreign power violates Swedish airspace and has nothing to do with system safety)
Integrated/built-in safety	Machinery Directive, Appendix I.	(Accident) risks must be eliminated, reduced in a certain order of priority where design measures are the first step. The procedure is called *Integration of Safety*.
Internal regulations (FIB)	H SDH 2021	This is a form of binding legal rules characterised by the fact that they do not relate to an individual case but have general application where there is no authorisation in a regulation. Internal regulations apply only within the Swedish Armed Forces.
Interoperability	FOI-R-3546-SE ISSN 1650-1942	Ability for external communication and resource management aimed at being able to function efficiently together with others.
Life cycle	FOI-R-3546-SE ISSN 1650-1942	Evolution of a system, product, service, project, or any other human-made entity from creation to disposal.
Limitation	H SystSäk 2022	Permanent limitation of the intended use.
Limited tolerable (BT)	H SystSäk 2022	For accident risks in the Yellow area, the *client* must ensure that the highest severity class of the accident risk is deemed to fit within the *Tolerable Risk Level* (TR) by reviewing that arguments and evidence and that the specific requirements for ALARP regarding yellow cells are met.
Maintenance Instructions	H SystSäk 2022	Swedish translation of the English *Service Handbook* and is intended for technical personnel who are going to maintain, repair or calibrate the product. Technical personnel may be present within the manufacturer's own organisation or at another operator.
Management	H SystSäk 2022	Use (training, exercises and operation), maintenance, storage (transport) and disposal.
Manufacturer	H SystSäk 2022	Physical or legal entity who designs and/or manufactures, or who has a product designed and/or manufactured and who is responsible for ensuring that the product complies with the applicable product legislation with a view to placing that product on the market, under their name or trademark. Manufacturing also includes anyone who assembles, packages, processes, labels or substantially modifies a product or its use so that compliance with the essential safety requirements is affected.
Materiel supplied	H SystSäk 2022	Products that are already in the Swedish Armed Forces' management system and that are made available for integration. *(Government Furnished Equipment, GFE)*

Concept	Reference	Glossary
Military materiel	H SystSäk 2022	Military materiel from a system safety perspective has been designed and manufactured (also through integration into a system-of-system) for military purposes, where regulatory frameworks may allow exemptions or where civil standards are lacking
Military materiel specially designed and manufactured for certain military purposes	H SystSäk 2022	Is from a system safety perspective is when a technical system has been designed and manufactured (also through integration into a system-of-systems) in order to have in its military function (organised armed combat) a direct destruction-giving effect
Military purpose	H SystSäk 2022	Refers to military activities that are only permitted to be carried out by the Swedish Armed Forces during exercise and operations.
MOTS products	H SystSäk 2022	Military Off the Shelf (MOTS) products *i*nclude commercially available finished products such as hardware or software
Not tolerable (NT)	H SystSäk 2022	For accident risks in red (NT) area of the risk matrix risk elimination/reduction must be conducted to reduce the *Tolerable Risk Level* (TR) requirement.
Notified body	EU Blue Book 2016	Certification bodies that carry out conformity assessment tasks under EU Regulations /EU Directives/EC Directives when the participation of a third party is necessary. Sometimes voluntary use of a Notified body is allowed.
Objective	FOI-R-3546-SE ISSN 1650-1942	A measurable result (mode) to be achieved at a specified time.
Operational safety	H SystSäk 2022	From a system safety perspective refers to the ability of the Swedish Armed Forces to manage accident risks in all activities so that the constitutional requirements for occupational health and safety of Swedish Armed Forces' personnel, as well as the safety of third persons, property and external environment is fulfilled.
People	H SystSäk 2022	Individuals are needed to manage a technical system and consist of, for example, users, maintenance, storage and transport personnel, who may hold a military or civil employment, be affiliated with the Home Guard, belong to a voluntary defence organisation or be conscripts.
Phase	SAMO 2020	A division of the life cycle of a technical system specified in the Government's investment planning directive.
Placing on the market	EU Blue Book 2016	A product is placed on the market when it is made available on the EEA/internal market, e.g. in the Member State of Sweden, for the first time, in order to be put into service. Refers to each individual product. The term refers to a point in time. Provision includes sale, loan, rent, gift, etc.

Concept	Reference	Glossary
Procurement	H SystSäk 2022	Collective terms for procurement, purchasing, loans, rent, leasing, Foreign Military Sales (FMS), gift, takeover and spoils of war.
Product liability	The Product Liability Act, SFS 1992:18	The liability of an economic operator for damage that a product may cause due to a safety deficiency. Refers only to financial compensation (damages) when a product has caused damage. The product should be in circulation, i.e. released on the market.
Product Safety Responsibilities	EU Directive for different products, about 25 pcs. EU Blue Book 2016	The responsibility of a Manufacturer (Importer) for a product so that it is sufficiently safe when it is placed on the market. The responsibility includes correctly carrying out a number of activities, including any certification, before the product is marked with e.g. CE marking. The EU Directives also state a responsibility for the post-market when the product is distributed, used. In this handbook, the product user is to be considered professional.
Put into service	EU Blue Book 2016	Occurs when the product is used in the EEA, e.g. in Sweden, by the end user for the first time and for the purposes for which the product is intended. Refers to each individual product. The term refers to a point in time. When the product is put into use by an employer and is to be used by employees, the employer is considered to be the end user.
Regulation (FFS)	H SDH 2021	A form of binding legal rules characterised by the fact that they do not relate to an individual case but have general applicability. The Swedish Armed Forces' regulations are published in the Swedish Armed Forces´ Statute book (FFS). A regulation always requires an authorisation in an ordinance and can apply both within and outside the Swedish Armed Forces.
Regulations	H SDH 2021	Type of action for binding provisions on the management and implementation of, or approach to, activities within the Swedish Armed Forces. A regulation may contain detailed and indicative explanations as well as descriptions and images.
Reliability	Swedish standard SS 441 05 05, Reliability	The ability of a system (device) to perform a demanded function under given conditions in a given time interval.
Request for Proposal (RFP)	H SystSäk 2022	Contains a description that clearly shows what the *client* wants. May include Technical Specification (TS) and Business Commitment Specification (VÅS).
Requirements	FOI-R-3546-SE ISSN 1650-1942	Specifies what systems must accomplish. Requirements can be divided into functional and non-functional requirements where the functional requirements describe what is to be achieved while the non-functional requirements describe what properties the system must have.
Requirements, stakeholder	FOI-R-3546-SE ISSN 1650-1942	Actors that enable a coordinated, integrated and holistic description of the demanded capabilities of future technical systems. The actor checks the fulfilment of requirements and makes the necessary decisions.

Concept	Reference	Glossary
Restrictions	H SystSäk 2022	Non-permanent limitation of the intended use.
Risk Awareness	FHS, Department of Leadership Rescue Department's Action Program	Knowledge, expertise and approach to accident risks and appropriate measures.
Risk number	H SystSäk 2022	Unique sequential numbers of individual accident risks for a particular technical system.
Risk reduction	H SystSäk 2022	The risk mitigation measures presented with evidence to be able to move accident risks in the risk matrix by measure.
Safety data sheet	Swedish Chemicals Agency	A document containing information on the hazardous properties, risks and protective measures to be taken of chemical products. *(Safety Data Sheet, SDS).*
Safety objectives	H SystSäk 2022	Safety objectives are the overall focus on the tolerable risk an activity can accept. The safety objectives define the risks to which the organisation and the environment are exposed when the technology within a function chain is not working as intended. Safety goals are defined based on the most safety-critical functional chains within the respective technical arena (Army, Navy, Aviation, Command and Logistics) that the Swedish Armed Forces need to maintain in order to carry out the missions specified in the Ordinance with instruction to the Swedish Armed Forces.
Satisfactory level of safety	H SystSäk 2022	Society's accepted level of risk is achieved by adhering to legislation and established standards.
Severity class	H SystSäk 2022	**Personal injury:** Death, serious personal injury, minor serious personal injury and negligible personal injury. **Economic damage:** Catastrophic property damage, critical property damage, severe property damage, negligible property damage **Environmental damage:** Catastrophic environmental damage, critical environmental damage, serious environmental damage, negligible environmental damage.
Source of risk	H SystSäk 2022	Dangerous property that can lead to injury to persons, property or external environment. Can also be a natural phenomenon.
System Goal Plan	FOI-R-3546-SE ISSN 1650-1942	System objectives are developed to determine the Swedish Armed Forces' requirements for a technical system that is intended to be procured to meet an identified need, preferably based on one or more unit objectives. System objectives can also be relatively independent unit objectives, for example regarding Swedish Armed Forces common materiel such as uniform systems and ammunition.

Concept	Reference	Glossary
System Integrator	Based on the definition in FOI-R-3546-SE ISSN 1650-1942	Actor tasked with combining technical systems, software, or both, into one system-of-system.
System Safety	H SystSäk 2022	The property of a technical system is not to inadvertently cause injury or damage to the person or external environment.
System safety analysis	H SystSäk 2022	To systematically use available information to describe and investigate accident risks.
System Safety Assessment (SSV)	H SystSäk 2022	Presentation of arguments and evidence to confirm that the system safety requirements are met for the use of Route Selections according to the Route Selection Model. *The technical system (product) is safe because:*
System safety decisions	H SystSäk 2022	A collective term for system safety statement, system safety declaration and system safety approval.
System Safety Objectives	H SystSäk 2022	System safety goals are the objectives a product area or technical system has to meet a *Tolerable Risk Level* (TR) in order to fulfil its part in a functional chain. The system safety requirements that follow then become dependent on whether the product area is included in a safety objective defined per arena.
System safety operations	H SystSäk 2022	The total work carried out for technical systems and products during all life cycle periods in order to set requirements, carry out system safety work and make system safety decisions.
System safety work	H SystSäk 2022	The total work carried out for a particular technical system during all life cycle periods in order to identify, analyse, evaluate and classify accident risks, eliminate or reduce these against set requirements.
System-of systems	Based on the definition in FOI-R-1830-SE	Several systems that work together, but lack common owners and policies. For the included technical systems, various system safety decisions have been issued and these technical systems may be approved against different requirements.
Task	FOI-R-3546-SE ISSN 1650-1942	Delimited activities carried out with the aim of achieving strategic, operational or tactical objectives.
Technical Design Responsibilities	SAMO FM - FMV 2020	Technical design responsibility means that defined design for permissible configurations of technical systems (including maintenance solutions) meets regulatory requirements, set objectives and other requirements including performance, function, information and system safety across the entire life cycle.
Technical Order	H SDH 2021	Documentation group for written orders relating to the regulation of configuration, technical service, technical systems and materiel, including the operation, maintenance, care and modification of supplies.

Concept	Reference	Glossary
Technical systems	H SystSäk 2022	Consists of components, consumables and software, as well as material documentation and technical data organised to achieve one or more purposes in a given environmental environment.
Test/trial	19FMV1007-2:1	The activities carried out during development/integration, for example, to determine if and how a solution works until the requirements are formally verified and/or validated in a typical configuration. The concepts of test/experiment are not covered in the concept of VoV.
Third Party/person's property	H SystSäk 2022	Person and/or his property that is not involved in ongoing activities.
Third-party bodies	Inter alia EU Blue Book 2016	Competent body/laboratory independent of manufacturers, users, authorities carrying out assessment of products (persons) and/or quality systems; often in the context of regulatory compliance assessment. For example, accredited bodies working as notified bodies.
Tolerable (T)	H SystSäk 2022	Green, *the client* must ensure that the highest severity class of the accident risk is deemed to fit within *the Tolerable Risk Level* (TR) by reviewing arguments and evidence.
Tolerable risk (for aviation safety)	FM R LML	The Decision of the Chief of the Air Force (FVC) on how large any aviation safety risks can be allowed for a defined activity within the military aviation system in the Swedish Armed Forces, i.e. how large aviation safety risks can be accepted in the military aviation system during all levels of conflict, both in peacetime production and during active operations.
Tolerable Risk Level (TR)	H SystSäk 2022	*Tolerable Risk Level* (TR) is the Swedish Armed Forces' accepted risk level for accident risks that need to be assessed in a risk matrix and where the level of acceptance can be both higher or lower than the satisfactory level of safety.
Trial	H SystSäk 2022	The use of established materiel for the purpose of evaluating its suitability in a given situation of use.
Triggers	H SystSäk 2022	A trigger is a mechanism that, together with a source of risk and contributing causes, produces a hazardous event.
Unit	H SystSäk 2022	Is a personnel and materiel part of the Swedish Armed Forces' basic or operational organisation and that carries the Swedish Armed Forces' various capabilities.
Usability	Based on the definition in ISO 9241-11	The degree to which a specific user can use a product in a given context to achieve specific objectives in an effective, efficient and satisfactory manner for the user.

User	FOI-R-3546-SE ISSN 1650-1942	Someone who, with permission, intentionally interacts with the system to achieve a purpose. Primary or direct users interact directly with the system, while secondary users interact with the system through direct users
Validation	19FMV1007-2:1	Confirmation by providing evidence that requirements for a specific, intended use or application have been met.
Verification	19FMV1007-2:1	Confirmation by providing evidence that the specified requirements have been met.
Vision	FOI-R-3546-SE ISSN 1650-1942	Description of desired characteristics without the requirements for precision that *goals* and *requirements* should contain and usually intend to describe long-term wishes.
Wheel marking	EU Directive 2014/90/EU	The marking, made by the manufacturer, indicates that the product complies with the EU Directive 2014/90 on Marine Equipment (corresponding to national legislation).
Work environment	WHO	A summary term for biological, medical, physiological, psychological, social and technical factors that affect the individual in the work situation or in the workplace environment.

Acronyms/Abbreviations

Acronym/abbreviation	Explanation
AFS	The Swedish Work Environment Authority's Statute book
ALARP	As Low as Reasonably Practicable
ANSI	American National Standard Institute
AOP	Allied Ordnance Publication (NATO)
AP	Allied Publications (NATO)
ASIL	Automotive Safety Integrity Level
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (Germany)
BOAC	Decision on use, Central Level
BOAL	Decision on Use, Local Level
BRI	Fire and Rescue Instruction
BT	Limited Tolerable
C OrgE	Head of Organisational Unit
CAS	Chemical Abstract Service
CDR	Critical Design Review. A formal review to evaluate the completeness of the design and its interfaces.
CE	Conformité Européenne; European compliance. (EEA).
CEN	European Committee for Standardisation
CENELEC, CLC	Committee for Electrotechnical Standardisation (Europe)
CI	Critical Item
CIL	Critical Item List
CIP	Commission Internationale Permanente pour l'épreuve des armes à feu portatives; Permanent International Commission for Firearms Testing
CLP	Classification, Labelling and Packaging (of substances and mixtures)
COTS	Commercial Off the Shelf
DEF-STAN	Defence Standard; British defence standard
DID	Data Item Descriptions; Document Guides, U.S. Military

Acronym/abbreviation	Explanation
DoC	Declaration of Conformity
DoD	Department of Defence (USA)
DoDI	Department of Defence Instruction; (USA)
DR	Design Rule
EASA	European Aviation Safety Agency
EDA	European Defence Agency
EEA	European Economic Area
EGT	EU's /EG's Official Journal
EHA	Environmental Hazard Analysis
EHAR	Environmental Risk Analysis Report
ELSÄK-FS	Statute book of the National Electrical Safety Board
EMAR	European Military Airworthiness Requirements
EMCD	Electromagnetic Compatibility Directive
EN	European Norm; European standard
ET	Not tolerable
ETSI	European Telecommunications Standards Institute
FBD	Functional Block Diagrams
FFS	Statute book of the Swedish Armed Forces
FHA	Functional Hazard Analysis
FHS	Swedish Defence University
FIB	Internal regulations of the Swedish Armed Forces
FIHM	Defence Inspector for Health and the Environment
FLYGI	Military Aviation Inspectorate

Acronym/abbreviation	Explanation
FM	Swedish Armed Forces
FM BMTS	The Swedish Armed Forces' decision-making system for technical systems
FMECA	Failure Mode, Effects & Criticality Analysis
FMS	Foreign Military Sales
FMUK	Swedish Armed Forces' Commission of Inquiry
FMV	Swedish Defence Materiel Administration
FORTV	Swedish Fortification Agency
FoT	Research and Technology Development
FRACAS	Failure Reporting Analysis and Corrective Action System
FSD	Swedish Defence Standard (publication) and Defence Standardisation Secretariat (unit at FMV)
FSI	Flight Safety Inspector
FTA	Fault Tree Analysis
GAO	Government Accountability Office (USA)
GEIA	Government Electronics & Information Technology Association (SAE)
GFE	Government Furnished Equipment, materiel provided by the state
HFI	Human Factors Integration
HHA	Health Hazard Analysis
HHAR	Health Hazard Analysis Report
HL	Hazard Log
HMAR	Hazard Management Assessment Report
HMI	Human Machine Integration
HMMP	Hazardous Material Management Plan

Acronym/abbreviation	Explanation
HMP	Hazard Management Plan
HMPR	Hazard Management Progress Report
HTO	Human, technology and organisation
HTS	Hazard Tracking System
HUD	Head Up Display
IACS	International Association of Classification Societies
IEC	International Electrotechnical Commission
IPT/WG	Integrated Product Team/System Safety Group
ISO	International Organisation for Standardisation
ITAA	Information Technology Association of America
ITS	Swedish Information and Telecommunications Standardisation
ITU	International Telecommunication Union
IVDR	In-Vitro Devices Regulation, Regulation (EU) 2017/746 on medical devices for in-vitro diagnostics
JSP	Joint Service Publication (UK)
KBV	Swedish Coast Guard
KÖL	Configuration Handover
LC	Certificate of Delivery
LFV	Civil Aviation Authority, CAA
LOU	Public Procurement Act
LUFS	Defence and Safety Procurement Act
LVD	Low Voltage Directive. Nowadays EU Directive on electrical equipment
MCS	Minimal Cut Set
MD	Machinery Directive

Acronym/abbreviation	Explanation
MDR	Medical Devices Regulation, Regulation (EU) 2017/745 on medical devices
MED	Marine Equipment Directive
MIFOR	Military Vehicle Registry
MIL-SPEC	Military Specifications (USA)
MIL-STD	Military Standard (USA)
MOA	Materiel Area Manager
MOTS	Military Off the Shelf
MSB	Swedish Civil Contingencies Agency
MSBFS	The Swedish Civil Contingencies Agency's Statute book
MTP	Medical Device
MTRF	Military Traffic Ordinance
NATO	North Atlantic Treaty Organisation
NSPA	NATO Support and Procurement Agency
O&SHA	Operating and Support Hazard Analysis
O&SHAR	Operating and Support Hazard Analysis Report
ÖB	Commander-In-Chief, Swedish Armed Forces
OJ	Official Journal; EC
ORM	Accident Risk Model
PARP	Partnership for Peace Planning and Review Process
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List

Acronym/abbreviation	Explanation
PPE	Personal Protective Equipment;
PTK	Sea Trials Command
PTS	Swedish Post and Telecom Authority
PTSFS	Statute book of the Swedish Post and Telecom Authority
R LML	Regulations Management of Military Aviation
RADS	Risk Assessment Prior to Disposal of Systems
RADSR	Risk Assessment Prior to Disposal of Systems Report
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
RED	Radio Equipment Directive
RFP	Request for Proposal
RML	Rules of military aviation
RMS	Rules for Naval Operations
VVM	Route Selection Model
SAAMI	Sporting Arms and Ammunition Manufacturers' Institute
SAE	Society of Automotive Engineers; USA
SAE ARP	Society of Automotive Engineers Aerospace Recommended Practice
SÄKINSP	Swedish Armed Forces' Safety Inspectorate
SäkR	The Swedish Armed Forces' Operational Safety Regulations
SAMO	Collaboration Agreement
SAR	Safety Assessment Report
SCA	Safety Compliance Assessment

Acronym/abbreviation	Explanation
SCF	Safety Critical Functions
SDB	Safety Data Sheet
SDS	Safety Data Sheet, (se SDB)
SE	Country code for Sweden
SE-EMAR	European Military Airworthiness Requirements endorsed in Sweden
SEK	Swedish electricity standards. Formerly Swedish Electrical Commission
SEMP	System Engineering Management Plan
SEP	System Engineering Plan
SFS	Swedish Statute book
SGRA	Support of Government Reviews/Audits
SHA	System Hazard Analysis
SHAR	System Hazard Analysis Report
SHK	State Accident Investigation Commission
SI	Safety Instructions
SIA	Safety Instructions Analysis
SIL	Safety Integrity Level
SIS	Swedish Institute for Standards
SMS	System Objective
SÖL	System Handover
SoS	System-of-Systems
SoSHA	System-of-Systems Hazard Analysis
SoSHAR	System-of-Systems Hazard Analysis Report
SR	Safety Review

Acronym/abbreviation	Explanation
SRHA	System Requirements Hazard Analysis
SRHAR	System Safety Requirements Analysis Report
SS	Swedish standard
SSB	System Safety Evaluation
SSD	System Safety Declaration
SSG	System Safety Approval
SSHA	Subsystem Hazard Analysis
SSHAR	Risk Analysis Report for Subsystems
SSI	System Safety Certificate
SSK	System Safety Requirement
SSKB	System Safety Concept Evaluation
SSM	System Safety Announcement
SSMP	System Safety Management Plan
SSP	System Safety Program
SSPP	System Safety Program Plan
SSV	System Safety Evaluation
SSWG	System Safety Working Group
STANAG	Standardisation Agreement (NATO)
SV	Safety Verification
SVR	System Safety Verification Report
Swedac	Board of Accreditation and Technical Control. Previously: Swedish Board for Accreditation and Conformity Assessment
T	Tolerable
TC	Technical Director

Acronym/abbreviation	Explanation
TDir	Technical Director
TEP	Test and Evaluation Participation
THR	Technical Rules of Practice
ToR	Terms Of References
TR	Tolerable Risk Level
TS	Swedish Transport Agency
TSFS	Statute book of the Swedish Post and Telecom Authority
TSR	Training Safety Regulations
TVK	Technology and Maintenance Offices
UK	United Kingdom
UK MOD	UK Ministry of Defence
UKCA	UK Conformity Assessed
VoV	Verification and Validation
VTR	Road Traffic Register
VV	Route selection
WBS	Work Breakdown Structure
WG	Working Group

Appendix 1 - EU Law and Swedish Legislation

The purpose of this appendix is to describe the EU law, Swedish legislation and other civil regulations that have affected the content of this handbook.

Civil Regulations

CE Marking

For specified product categories according to EU Directives, CE marking is mandatory. Other product categories, which are not covered by the EU Directives with CE marking, must not and thus may not be CE-marked. Products specially developed for certain military or police purposes may be exempted from CE marking according to the current EU Directives. They must not be CE-marked according to these particular EU Directives. However, there may be other EU Directives that require CE marking. If the product is specially developed for military purposes and then happens to have an exemption from CE marking and at the same time is made available on the market with a civil purpose (*dual use product*), then the product must be CE-marked. The CE marking must be applied permanently to the product and in the accompanying documents etc.

Appendix 1, figure 1 *CE marking, where CE stands for European Compliance (Conformité Européenne).*

Application of the CE Marking

By CE marking, the legal manufacturer certifies that the product complies with the statutory requirements for safety, health and the environment, i.e. that all applicable EU Directives are met. The EU Directives are different in scope - some operate individually, others in parallel, while some accident risks are included in other EU Directives that make EU Directive B take over from EU Directive A for the product in question. For example, electrical accident risks are now covered by the Machinery Directive, which means that the Low Voltage Directive (LVD) no longer applies to a complete electrical machine, but only the Machinery Directive. In parallel, however, the EMC Directive applies on the electric machine in question.

> Legal manufacturer refers to the person who has full product safety responsibility, but is not necessarily the one who physically manufactures the products.

Sometimes other product characteristics such as performance are also attested. The legal manufacturer is also responsible for ensuring that the product intended to be released within the EU/EEA has been designed, manufactured and inspected in accordance with the regulations. For most products, it is sufficient for the manufacturer himself to ensure that the

product meets all the requirements, but for some products that are considered particularly risky, the manufacturer is required to allow an independent third-party body, known as a *Notified body* to inspect the product. Depending on the EU Directive, this may refer to the design of the product, the manufacturing of the product, the manufacturer's quality system or a combination of these. Once the Notified body has been used, the CE marking must be accompanied by the body's four-digit ID number.

As part of the CE marking, the manufacturer must also create technical documentation (*Technical File, Technical Construction File*) for the product, as well as issue a *Declaration of Conformity* (DoC). The technical documentation referred to is the documentation whereby the manufacturer demonstrates that the requirements of the EU Directive are met. This documentation is a subset of the total design and manufacturing base of a product. The CE-marked device must also be accompanied by instructions containing all essential information to enable the device to be used and handled for its intended purpose safely. Upon delivery to the end client, the product must be accompanied by an instruction handbook and the *Declaration of Conformity* (DoC), in the language of the country of destination. The language requirement also applies to the labelling and signs that the product must have.

The person responsible for placing on the common internal market or putting into service an equipment for the first time in the EU internal market (EEA) must comply with all obligations regardless of whether this person is an economic operator (legal manufacturer, importer, authorised representative, distributor) or user. Distributors, such as wholesalers and retailers, must also have basic knowledge of applicable legislation, such as which products must be CE-marked and what information must accompany them.

Manufacturers must keep themselves informed of updating the standards applied in order to assess whether the product type in question is still considered to comply with the requirements of the Directive or whether action is needed for new product variants to be manufactured. Similarly, manufacturers should monitor whether the Directive, or its detailed requirements, are revised and, if so, whether action needs to be taken on newly manufactured product variants of the product.

Exemption from CE Marking

Products developed for certain military or police purposes may be exempted from CE marking. For example, the EU Machinery Directive does not apply to weapons, including firearms, or to machinery specially designed and manufactured for military or police purposes. On the other hand, ordinary machines used by the military or police are covered by the Machinery Directive. Note that even if a directive happens to have an exemption for the product in question, one or more other directives may be mandatory. For example, a training system that is not intended to be used in organised armed combat should be CE-marked just like a crane/hoist put on a tank, even if the tank's use itself has a destructive effect. See also the section on Wheel marking.

UKCA Marking

In 2021, the UK introduced a *UK Conformity Assessed* (UKCA) product safety marking in conjunction wi*th the UK's exit from the EU.* In doing so, the UK also left EU law including CE marking.

The UKCA marking corresponds to CE marking by the manufacturer declaring that the essential health and safety requirements are met. Please note that special rules apply to Northern Ireland.

Appendix 1, figure 2 *UKCA mark, where UKCA stands for United Kingdom Conformity Assessed.*

A product covered by the Product Safety Directives within the EU may not be placed on the EU internal market (EEA) without CE marking. Similarly, a CE-marked product may not be placed on the UK market without a UKCA marking. Note that the product safety directives within the EU require that the instructions for use and marking are in the correct language for the country where the product is to be used.

There is UK legislation that corresponds, among other things, to the Electromagnetic Compatibility Directive (EMCD) and the Low Voltage Directive (LVD). Machines, lifts, measuring instruments and radio equipment are examples of products subject to UKCA marking. For certain product groups, there may be special rules that deviate from the EU Directives.

As long as the technical requirements are the same within the EU and the UK, the rules usually involve only an administrative task. On a product intended for both markets, there will be both CE and UKCA marking.

Please note that in cases where a Notified body within the EU has been used, the corresponding UK approved body should also be used to place the product on the UK market.

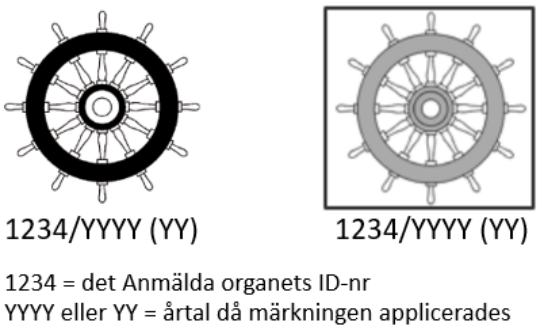
Wheel Marking

The EU law aims to improve maritime safety, health and the prevention of pollution at sea through requirements on how marine equipment must be manufactured and controlled. Wheel marking is used to show that equipment covered by the EU Marine Equipment Directive 2014/90/EU (MED) meets current requirements. For specified product categories wheel marking is mandatory according to EU law, but only products stipulated for wheel marking may be marked. Products specially designed for military purposes may be exempt from wheel marking. The Swedish Armed Forces' application of the provisions on marine equipment is regulated in the Rules for Naval Operations (RMS).

Application of Wheel Marking

The EU Directive 2014/90/EU for Marine Equipment is applied through the Marine Equipment Act (SFS 2016:768) concerning marine equipment and the Ordinance (SFS 2016:770) for marine equipment together with the Swedish Transport Agency Regulations TSFS 2016:81 for marine equipment. A product that is type-approved/equivalent by a Notified body in an EU Member State may be placed on an EU vessel, regardless of the flag it flies, thus promoting the free movement of marine equipment in the internal market.

Equipment regulated by the EU Marine Equipment Directive (mainly for the ship's maritime safety as well as for water and air purification) must be wheel-marked and not CE-marked. The wheel mark indicates that the product meets the requirements of the EU Directive by the manufacturer carrying out a certification (type approval or comparable specified procedure) carried out by the Notified body. The EU Directive lays down common rules with the aim of eliminating differences in the implementation of international conventions by having a clearly identified set of requirements and uniform certification procedures. According to rules from the Maritime Safety Inspectorate (SJÖI)/Navy's Ship Inspection (MFI), the EU Directive applies to specified marine equipment. This EU Directive with wheel marking thus replaces other EU Directives with CE marking for such equipment as listed above. Note that there are other products on board ships that are covered by EU Directives with CE marking. The use of CE-marked products on board warships is regulated in the Rules for Naval Operations (RMS).



Appendix 1, figure 3 Examples of wheel marking.

The EU Directive applies to equipment that is placed or intended to be placed on EU ships, if certain international maritime conventions require the approval of the equipment by the State whose flag the ship is flying. The legislation contains provisions on requirements for marine equipment and obligations for manufacturers and other economic operators making such equipment available on the market. Furthermore, there are provisions on market surveillance to ensure that marine equipment complies with the prescribed requirements and on fines in the event of non-compliance.

Exemption from Wheel Marking

On smaller vessels (displacements below 40 tons), the Swedish Armed Forces use different types of commercial products. For the smallest boats, so-called pleasure craft products are often used. The products can be simpler types of radar systems and chart plotters. Products

that are certified according to the EU Directive and thus wheel-marked are designed for larger vessels. Technical limitations of smaller vessels and boats may mean that wheel-marked products are not suitable for integration. Wheel-marked products are often both heavier and physically larger. For example, smaller boats may need to have a built-in antenna to avoid obstruction of operations. Smaller boats usually have open steering positions and the products must therefore be waterproof, which is not the case with most of the wheel-marked products. The Maritime Safety Inspector may therefore need, after assessment, to grant exemptions from wheel marking for individual products.

CIP Marking

The obligation to mark weapons is set out in EU Directive 2021/555/EU on control of the acquisition and possession of weapons. In addition to this, a number of states have agreed on a common labelling and control system. Swedish manufacturers and importers of weapons are advised to apply the CIP system, which meets the requirements of the EU Directive.

CIP *(Commission Internationale Permanente pour l'Epreuve des Armes à Feu Portatives/ Permanent International Commission for Firearms Testing)* is a governmental international organisation consisting of a number of countries that agree on the mutual recognition of the *proof-test* marking of firearms as well as ammunition that has passed the safety test. CIP's intention is to ensure the safety of civil firearms, commercial ammunition and all other equipment that uses explosives for purposes such as sports and hunting.

There is also a corresponding American association of ammunition and weapons manufacturers known as SAAMI *(Sporting Arms and Ammunition Manufacturers' Institute)*, which is a standardisation body for weapons and ammunition.

Application of CIP Marking

The CIP Convention has the following main provisions:

- Mutual recognition of each country's test verification mark certifying the identity of firearms and the fact that satisfactory testing has been carried out in accordance with the established rules
- Testing is standardised to ensure safety
- That at least one state-controlling (accredited) national testing facility is located in each member state (Sweden is not a member of CIP and therefore does not have an accredited testing facility)
- That each Member State enacts laws making it mandatory to carry out testing in accordance with the methods, limitations and procedures established by the Convention.

Exemption from CIP Marking

As military application differs significantly from civil application, CIP marking is generally not suitable for military small-calibre weapons and ammunition. NATO uses other procedures to control the safety and quality of military small-calibre weapons and its ammunition, NATO EPVAT, for example for 7.62mm, STANAG 2310 is used. Otherwise, the FMV Handbook Weapons and Ammunition Safety (H VAS) is applied.

Post-market Measures and Market Surveillance

Manufacturers and other economic operators also have certain responsibility (differing between different EU Directives) for the post-market, i.e. once the product is on the market. For example, they must take care of complaints, safety deficiencies, deal with possible accidents and incidents involving the products and be able to trace the products upstream and downstream to other economic actors. This is to be able to inform about, rectify or recall dangerous or defective products.

Some EU Directives also require suspected dangerous products, as well as accidents and incidents, to be reported by manufacturers and other economic operators to the responsible authority. A manufacturer or importer may also need to carry out random checks on delivered products to ensure that the products comply with the requirements of an EU Directive.

Furthermore, Member States must carry out market surveillance activities in accordance with the provisions of EU Regulation 765/2008 on accreditation and market surveillance. Market surveillance means that the responsible authority takes measures to ensure that products already on the market comply with current legislation and that they are controlled and labelled in the prescribed manner. Thus, it does not cover ex ante control of products. It is part of the chain of ensuring adequate protection of consumers and workers, public health and the environment. It must also prevent distortions of competition between undertakings. The Swedish Government has identified 17 Government agencies as responsible for market surveillance. Most of these authorities are also the regulatory authority for the products or product characteristics for which they have market surveillance responsibility.

FMV is the supervisory authority for EMC (according to the Ordinance SFS 2016:363 on electromagnetic compatibility) regarding products within the Swedish Armed Forces, the Swedish Fortification Agency (FORTV), the Swedish Defence Radio Establishment (FRA) and the Swedish Defence Research Institute (FOI). The National Electrical Safety Board is the market surveillance authority and supervises the EMC of other products.

In the case of wheel-marked products, the Swedish Transport Agency must take into account the specificities of the marine equipment sector, for example whether an equipment can be assumed to pose a risk to maritime safety.

For explosives, including ammunition, but excluding weapons, the Swedish Civil Contingencies Agency (MSB) is responsible for market surveillance.

The authority must take action against economic operators whose products do not comply with the requirements. The interventions that may be relevant are, for example, information obligations, product actions, sales bans or the recall of products from the market or end users. This can take the form of information, planned controls (supervision, inspection) on the premises of manufacturers, importers and retailers for products placed on the market. It can also take place due to reported accidents, incidents or after warnings via the EU Commission's databases or authorities in other countries.

The manufacturer, importer or distributor must assist the market surveillance authority in its supervision, for example by providing access to the necessary parts of the technical file.

The Market Surveillance Council is a national coordinating body for this market surveillance. The Board for Accreditation and Technical Control, SWEDAC, is responsible for coordinating the Swedish market surveillance authorities. The work consists primarily of legislation, interpretation and method development, as well as information exchange. The Council must also facilitate public contacts with the authorities and consult representatives of, inter alia, industry and consumers.

The Swedish Armed Forces need to have traceability of CE-marked and wheel-marked products if the manufacturer or market surveillance authorities take measures such as modifications warnings, prohibitions on use or whether the products should be recalled.

Environmental Legislation

The Environmental Code (SFS 1998:808) aims to promote sustainable development, which means that current and future generations are ensured a healthy and good external environment. The Environmental Code applies to all activities that have, or may have, environmental impact. Anyone who conducts a business is obliged to have knowledge of the environmental impact that the activity entails.

Chemical products and chemical substances in articles are primarily regulated in two EU Regulations, REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals), EU 1907/2006, and CLP (Classification, Labelling and Packaging of Substances and Mixtures), EU 1272/2008. REACH contains rules on information on hazardous substances in the supply chain, for example on Safety Data Sheets. Anyone who manufactures, imports or distributes articles or chemical products within the EEA/EU must check whether the articles or chemical products contain any substance on the Candidate List as this may entail special requirements for handling in accordance with the EU Regulation REACH. CLP governs how hazardous substances are to be classified, packaged and labelled.

The responsible party is obliged to carry out the protective measures, observe the restrictions and take the precautions necessary to prevent, prevent or counteract the fact that the activity causes harm or inconvenience to human health or the environment. The best possible technology should be used and products should be selected that have the least environmental impact. Operators must manage raw materials and energy and use the possibilities for reuse and recycling. Detailed regulations can be found in the follow-on legislation to the Environmental Code.

According to the Swedish Work Environment Authority's regulations AFS 2011:19, on chemical work environment risks, risk assessments must be made prior to work that includes handling chemical products.

A large number of central, regional and local authorities have specifically designated tasks in relation to the Environmental Code, including responsibility for guidance and supervision. Within the Ministry of Defence's area of responsibility, the Defence Inspector for Health and

the Environment (FIHM) supervises the application of the Environmental Code at the Swedish Armed Forces, the Swedish Defence Materiel Administration (FMV), the Swedish Fortification Agency (FORTV) and the Swedish Defence Radio Establishment (FRA). The Defence Inspector for Health and the Environment (FIHM) is the function that examines environmentally hazardous activities, healthcare, dental care, infection control, food safety and animal welfare.

Electrical Safety Legislation Including the Low Voltage Directive

The first Electricity Act was introduced in 1902 and was thoroughly revised to a new Electricity Act (SFS 1997:857). Given the risks of electricity (invisible, lethal/harmful effect, fire) and increased use, the Swedish Parliament also decided on Sweden's first Electrical Safety Act (SFS 2016:732).

The Electrical Safety Act regulates, among other things, the following obligations:

- For owners of electrical installations
- For those who manufacture, import, distribute or install electrical equipment
- Regarding the performance of electrical installation work
- For those who possess or use electrical equipment

Two key definitions can be found in the Electrical Safety Act:

- Electrical plants consist of individual electrical equipment that is built together to bring electricity to socket outlets/connection boxes where electrical equipment (electrical materiel/electrical equipment) is connected for the consumption of electricity. An electrical plant cannot be purchased as a ready-made device by a manufacturer, instead it must be built together in the place where it will be used.
- Electrical equipment is manufactured by one manufacturer and placed on the market (supplied) as a finished product. The manufacturer has a clear responsibility for ensuring that the equipment meets the applicable safety requirements of the EU Directives.

The term electrical plant has previously often been used as an umbrella term even for electrical equipment. As a result, procurement requirements documents have been perceived as unclear as well as the requirements for competence for the personnel who are to carry out the maintenance.

Electrical safety legislation in Sweden is goal-related and specifies how electrical installations and electrical equipment must be designed to be safe to use. Requirements for the safety of equipment and how it is met are handled via EU Directives and the Harmonised Standards established by the EU to meet the essential health and safety requirements of EU Directives.

Standards have always been important for electrical products as a means of meeting the requirements of the legislation. Standards are mainly developed within the IEC and then transferred to EN standards and Harmonised Standards.

The Swedish Armed Forces' internal Regulations (FIB) set out how to deal with the requirements of the Electrical Safety Act.

FMV has, on behalf of the Swedish Armed Forces, carried out extensive investigative work on how the requirements for safety for the Swedish Armed Forces' personnel are met when technical systems are used in the field environment and there is no access to a fixed electricity distribution network and what the regulations define as system grounding (so-called approved grounding). This resulted in the *Design Rule - Swedish Armed Forces' Electrical Facilities in Field Environment* (FMEAF).

FMEAF is an established concept within the Swedish Armed Forces. It is a summary term for plants established with equipment for the production and distribution of electricity in a field environment, i.e. transportable generator sets, switchboards and connecting cables.

By applying established standard together with documented risk assessment in the design rule, the legislation's requirements for personal and facility safety are met. The design rule also affects the design of electrical equipment (current consumers) that are connected to FMEAF because they are included as part of the grounding system.

For more information, see FMV's Handbook Safe Electrical Products and Systems (H SEPS) and the Swedish Armed Forces' Handbook for Electrical Safety (H ELSÄK).

Electrical materiel (electrical equipment) must be CE-marked according to the EU's LVD (so-called Low Voltage Directive) 2014/35/EU, if it is designed to run with, or emit, a voltage of 50-1000V AC or 75-1500V DC. The EU Directive is transposed through the National Electrical Safety Board's Regulations ELSÄK-FS 2016:1. The basic requirement is that electrical equipment must have a high level of protection regarding the health and safety of people and domestic animals and provide protection for property. The manufacturer can verify for himself that the basic requirements are met for the products. There is no requirement for certification, that is, approval by third parties (Notified body). However, an accredited body may be engaged voluntarily.

At present, there are no exemptions for military equipment. Conditional exemptions exist for equipment on ships, planes and trains.

Vehicle Legislation

A vehicle may be used in traffic only if it is reliable from the point of view of road safety and otherwise suitable for traffic. A vehicle is roadworthy if it is designed, built, verified, equipped and maintained in such a way, and has such characteristics, that safety and environmental requirements are met. Roadworthiness is achieved by passing vehicles during a registration inspection and periodic checks. Registration inspection and testing prior to an individual approval can be carried out by an accredited inspection body or by a military inspection engineer. The Swedish Armed Forces may issue special regulations to this effect.

When procuring, reference is made to current EU Regulation, such as *"Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles"*. The exemptions that can be given with regard to Swedish Regulations may be determined by the military inspection engineer in each individual case.

The above EU Regulation points to the *ECE Regulations*. These are annexes to the 1958 United Nations Global Agreement to adopt uniform technical regulations for wheeled vehicles or for equipment and components that can be fitted or used on such vehicles. Each new provision enters into force for all those Parties that have indicated to the UN General Secretariat that they approve of the Regulations. The ECE regulations are applied by some 60 countries. However, the EU and Sweden have not adopted all the regulations.

Under the Vehicle Act (SFS 2002:574), the Vehicle Ordinance (SFS 2009:211) and the Military Traffic Ordinance (MTRF, SFS 2009:212) are published. For military vehicles, these regulations are applied in parallel. The Military Traffic Ordinance contains special provisions on the nature and equipment of vehicles belonging to the state and operated by the Swedish Armed Forces, FMV and the Swedish Defence Radio Establishment (FRA). The Military Traffic Ordinance (MTRF) also gives the Swedish Armed Forces the possibility to grant certain exemptions from traffic legislation.

The Swedish Armed Forces may issue regulations on vehicles belonging to the State and manufactured for special military purposes. This is stated in the Swedish Armed Forces' regulations on military traffic (FFS 2021:2).

In the Swedish Transport Agency's Statute book, vehicles that are registered in the Military Vehicle Registry (MIFOR) and that are used by the Swedish Armed Forces, FMV and the Swedish Armed Forces Radio Establishment are given exemptions regarding certain equipment requirements for vehicles. Further exemptions for individual vehicles can be applied for from the Swedish Transport Agency by a military inspection engineer.

Other Statute books that may affect the equipment and nature of vehicles are:

- Swedish Civil Contingencies Agency Statute book, MSBFS
- The Swedish Work Environment Authority's Statute book AFS
- The Swedish Transport Agency´s Statute book, e.g. TSFS 2019:19

Some machines that fall under AFS 2008:3 on *Machinery* can also be classified as vehicles and therefore be subject to registration according to the Military Traffic Ordinance (MTRF). They may also be subject to additional regulations from the Swedish Transport Agency. This applies, for example, to trucks, motor tools and snowmobiles.

FMV’s Handbook Vehicle Safety (H FordonSäk) is a complement to vehicle legislation and describes exemptions and additions and provides suggestions for requirements for safe structures. Furthermore, there are proposals for requirements for, for example, the installation of weapons and command and control systems in vehicles.

Maritime Legislation

For ships and diving systems, there is a comprehensive regulatory framework. The Ship Safety Act (SFS 2003:364) imposes requirements on all types of vessels, but only applies to warships to the extent prescribed by the Government. Additional legislation exists that regulates the working environment on board ships. Below is a selection of the statutes that govern this regulation.

The Ordinance (SFS 2003:440) on the Safety of warships regulates which parts of the Ship Safety Act *(*SFS 2003:364) apply to warships, and authorises the Swedish Transport Agency, formerly the Swedish Maritime Administration, to both issue additional rules and exercise supervision over military shipping. Furthermore, the Swedish Armed Forces must have a system for checking seaworthiness and safety on warships that is approved by the Swedish Transport Agency.

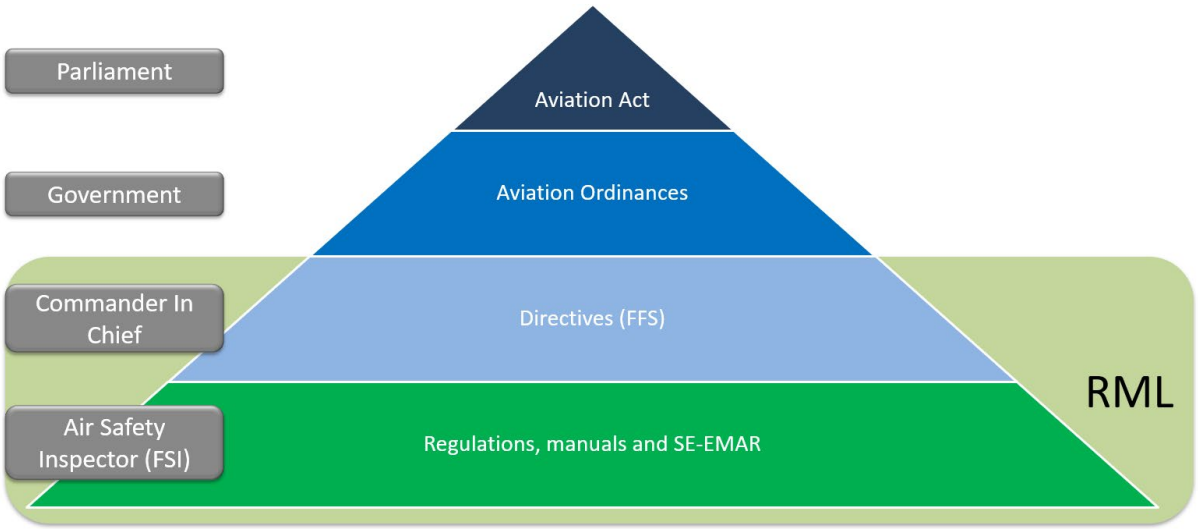
The Ordinance (SFS 2003:440) on the Safety of warships regulates that the Swedish Transport Agency may create rules for the seaworthiness of warships. The same ordinance also regulates that the Swedish Transport Agency may regulate the working environment on warships. The work environment regulations contained in the Swedish Transport Agency's Regulations TSFS 2011:91 and general advice on the work environment on warships, consist in part of ship-specific rules and part of a number of the Swedish Work Environment Authority's regulations (AFS) are put into force on warships. This regulation means that an AFS is only applicable to warships if it is included in TSFS 2011:91.

Aviation Legislation

All activities that are considered aviation activities are subject to a permit in accordance with the Aviation Act (SFS 2010:500). The Government, or the authority determined by the Government, specifies the terms and conditions that apply to the exercise of aviation activities in Sweden and to Swedish registered aircraft used abroad.

For civil aviation, as well as for air navigation services for both civil and military aviation, the Government has authorised the Swedish Transport Agency to issue regulations and to act as a supervisory authority. EASA (*European Aviation Safety Agency*) governs civil aviation in the Union area. This influence is exercised, inter alia, through EU Directives that apply directly or indirectly to civil aviation.

For the military aviation system, the Government has through the Aviation Ordinance (SFS 2010:770) authorised the Swedish Armed Forces to issue regulations and exercise supervision.



Appendix 1, figure 4 *Hierarchy between laws, rules, ordinances including the Swedish Armed Forces' regulations.*

The Commander-in-Chief (Supreme Commander) is responsible for military aviation safety within the military aviation system. Provisions for military aviation are set out in the Swedish Armed Forces' Regulations on military aviation FFS 2019:10.

The Aviation Act (SFS 2010:500) states that the military aviation system consists of systems for air operations, airports and air bases as well as for airspace. The Swedish Armed Forces' regulations and handbooks for military aviation contain more detailed provisions on the application of the Swedish Armed Forces' regulations on military aviation. The Head of the Military Aviation Inspectorate (FLYGI) may decide on the regulations, handbooks and SE-EMAR *(European Military Airworthiness Requirements)* for military aviation.

A Government agency engaged in military aviation in one or more areas of activity must have an approval issued by the Flight Safety Inspector (FSI). A Government agency engaged in military aviation must notify the Military Aviation Inspectorate (FLYGI) in which area or areas of activity the authority intends to conduct business and in what way the applicant meets the applicable requirements according to the Swedish Armed Forces' regulations on military aviation. Operators other than the State must be licensed to operate in the military aviation system. An application for a permit to operate in the military aviation system (operating permit) must be made to the Military Aviation Inspectorate (FLYGI). An operating licence and a decision on the approved area of operation are issued in a military aviation document issued by the Flight Safety Inspector (FSI).

A military aircraft may only be flown if it is airworthy. A military aircraft is considered airworthy if it is designed, manufactured, tested, equipped and maintained or modified in such a way, and has such flight characteristics that the requirements of military aviation safety are met. It is for the operator to demonstrate that a military aircraft is airworthy.

The Aviation Ordinance (SFS 2010:770) states that the Flight Safety Inspector (FSI) supervises compliance with the provisions of the Aviation Act (SFS 2010:500) and regulations issued pursuant to the Act (such as the Swedish Armed Forces' Regulations on

military aviation FFS 2019:10) in respect of military aviation. The Military Aviation Inspectorate (FLYGI) in the Swedish Armed Forces' Headquarters must support the Flight Safety Inspector (FSI) regarding these licensing and supervisory activities.

Legislation on Flammable and Explosive Goods

The Act (SFS 2010:1011) on Flammable and Explosive Goods (LBE) applies to the handling and import of flammable and explosive goods. The purpose of the Act is to prevent such goods from causing a fire or explosion that is not intended, as well as to prevent and limit damage to life, impact on health, external environment or property by fire or explosion when handling such goods.

For design and review requirements regarding ammunition for military purposes (military ammunition), there are special rules. The Ordinance (SFS 2007:936) on international law review of weapons projects states that review of projects from the point of view of international law must be carried out by *the Delegation for The International Law Review of Arms Projects*. The Ordinance requires the Swedish Armed Forces to notify the Delegation as soon as possible of any project relating to the study, development, acquisition or modification of weapons or combat methods.

FMV Weapons and Ammunition Safety Handbook (H VAS) covers ammunition intended for military purposes and sets out requirements for the safety characteristics of the functions that occur in military ammunition. Furthermore, there are also specific requirements for military ammunition that follow from international law requirements.

Legislation in Other Areas of Safety

Technical systems and products may be subject to specific legislation, regulations and/or standards, for example for, lasers, radiation sources, hazardous substances or medical devices (MTP). This also applies to technology-independent sources of risk such as ionizing and non-ionizing radiation, noise, vibration and hygienic limit values for hazardous substances. For some products, such as lasers, the Swedish Armed Forces may have certain exemptions.

For certain equipment such as connecting equipment (bridges), there may be special regulations, standards and/or design rules.

For products subject to their own rules and designed and tested/verified accordingly, this is usually considered sufficient. The overall documentation regarding design and testing becomes part of the basis included in the system safety assessment.

For certain technical systems and products, another party such as accredited laboratories, certification and inspection bodies, and validation and verification bodies is required to certify that laws, regulations and standards are met before products can be placed on the market. This, too, becomes part of the basis included in the system safety assessment.

When moving technical systems and products by road and rail, as well as for air and maritime transport, there may be restrictions on physical dimensions, weights and weight distribution, as well as on individual goods such as hazardous substances, batteries and explosives.

Human limitations on exposure to technology-independent sources of risk are often required by technical standards or industry-specific guidance. There are also accepted test methods to verify the requirements of the standards.

A related area to the safety area that has great importance and an indirect impact, is the ability of products to work together without disturbing or being disturbed, that is, electromagnetic compatibility.

Electrical material (electrical products) must be CE-marked in accordance with the EMC Directive 2004/108/EU. The EU Directive is transposed through the National Electrical Safety Board's Regulations ELSÄK-FS 2016:1. Basic requirements are that electrical equipment must meet protection requirements in terms of emission and immunity. In principle, everything electrical is covered from 0Hz to 1THz (really no upper limit) regardless of the rated voltage. Protection requirements are set out in Harmonised Standards. Electrical environment, requirements levels in the regulations/standards are limited/not so stringent, compared to what is found in military EMC standards.

The manufacturer can verify for himself that the basic requirements are met for the products. There is no requirement for certification, that is, approval by third parties (Notified body). However, an accredited body may be engaged voluntarily.

At present, there are no exemptions for military equipment. Exemptions exist for certain aeronautical products and for components which do not have a function of their own (*intrinsic function*) and thus do not interfere with or are interfered by, such as cables, transformers and induction motors. If the equipment falls under the Radio Equipment Directive (RED, 2014/53/EU), the Marine Equipment Directive (MED, 2014/90/EU) or EU Regulations for medical devices, these directives should be applied instead of the EMC directive, as the former include EMC requirements.

Product Safety and Product Liability Legislation

This description of the two product legislations is made to provide general information in this handbook. A complete system safety work according to the methodology in this handbook can constitute an important basis for individual manufacturer/supplier.

Product safety legislation requires that all goods and services offered by companies must be safe. A piece of goods or service is safe if, under normal conditions of use, it does not present a risk of accident, or a low risk of accident, for the health and safety of persons. The EU Directives in previous sections are examples of specialised product safety legislation.

Product liability legislation enters into force after an accident has occurred. The legislation aims to hold the producer liable and provide for the possibility of financial compensation to consumers and is neither not preventive nor does it affect the design of an item before it is placed on the market. The legislation requires, among other things, recalls and warning information to consumers if a serious safety deficiency has been identified.

Product Safety Act

The Product Safety Act (SFS 2004:451) itself does not apply to goods that are only intended for professional use (e.g. within the Swedish Armed Forces) but relates to goods and services for consumers. These must be safe when offered to consumers. Property damage and environmental damage also fall outside the area of this Act. Simplified, it can be said that the law is a general law and that it does not apply if there is special legislation, such as legislation that transfers a more specialised EU Directive, for a particular product or accident risk. The manufacturer or distributor must provide safety information that allows you as a consumer to assess the accident risks of the product or service. If the risk of accidents is obvious, the manufacturer or distributor does not need to provide the information.

The Swedish Consumer Agency is the supervisory authority for the Product Safety Act (SFS 2004:451) and shares responsibility with other authorities that have supervision of specific goods or accident risks. For example, the National Electrical Safety Board supervises most electrical accident risks and the Swedish Chemicals Agency supervises most chemical-related accident risks.

Product Liability Act

The Product Liability Act (SFS 1992:18) regulates the conditions for damages for damage caused by a product due to a safety deficiency. This refers to damage to an individual or individual property and is thus a consumer protection law. The law only applies when traders sell to consumers, i.e. not to professional users in, for example, the Swedish Armed Forces. Damage to the product itself is not reimbursed.

A product used by a person in their employment is primarily covered by the Work Environment Act and by the employer's responsibility for a good and safe work environment.

A product has a safety flaw if the product is not as safe as might reasonably be expected. Defects in products that depend on the design, manufacture or an unclear instruction handbook are called safety flaws. Safety must be assessed taking into account how the product was foreseeable to be used and how it has been marketed, as well as taking into account instructions for use, the time when the product was placed on the market/put into circulation and other circumstances.

Appendix 2 - Standards

The purpose of this Appendix is to describe standards that have influenced the content of this handbook.

U.S. Defence Standards, MIL-STD

U.S. defence standards are divided into military standards (MIL-STD) and defence specifications (MIL-SPEC). According to *the Government Accountability Office* (GAO), a MIL-STD describes the desirable processes and practices that a supplier should apply to develop the right technical systems and products while a MIL-SPEC describes the physical and/or operational characteristics of a technical system or a product. In addition to this, there may also be military handbooks that are primarily sources of compiled information or guidance.

MIL-STD-882E, (System Safety)

The MIL-STD-882E standard, *DEPARTMENT OF DEFENSE STANDARD PRACTICE SYSTEM SAFETY* published on May 11, 2012, is intended for use by all military agencies within the *U.S. Department of Defence* (DoD). The standard is consistent with the intentions of *Department of Defence Instruction (DoDI) 5000.02*.

The standard contains requirements for system safety activities as well as a description of a system safety process. The standard requires that the process be documented and that coordination with other risk management within *System Engineering* (SE) must take place.

The standard provides instructions for the implementation of system safety activities in *System Engineering* (SE) with the aim of eliminating or minimizing accident risks related to technical systems, products, equipment and infrastructure during all life cycle phases of the system from development through disposal. The principle of the standard is that a selection of the various activities (*tasks*) must take place for the technical system in question. The various activities of the standard are divided into governance (*management*), analysis, evaluation and verification. The standard also provides a list of applicable document guidance (DID) for the various reports that are the results of the various activities.

Hazardous events and/or accident risks must be systematically identified and documented in a hazard log and evaluated in terms of consequence and probability. There are proposed consequence and probability classifications as well as examples of risk matrices for assessment.

The standard also includes a separate section dealing with software in safety-critical applications. There are both *software control categories* and *software safety criticality matrices* as well as an assessment table regarding the level of risk of the software.

Appendix A, *Guidance on the scope of system safety work*, provides guidance on how to select activities, as well as when they are appropriately performed. Further, an example of quantitative probability definitions is given. Appendix B, *Software Safety Operations*, provides guidance to the operations of safety-related software. For a detailed description, please see:

- *Joint Software Systems Safety Engineering Handbook*
- *Allied Ordnance Publication (AOP-52), Guidance on Software Safety Design and Assessment of Munition-Related Computing Systems*

MIL-STD-1472H, (Human Factors)

The MIL-STD-1472H standard, *Department of Defence Design Criteria Standard, Human Engineering* published on September 15, 2020, is intended for use by all military agencies within the *U.S. Department of Defence* (DoD).

The standard specifies criteria for *Human Machine Integration* (HMI) and principles to be applied in the design of military systems, subsystems, equipment and facilities. HMI operations can be conducted based on a *Human Engineering Program Plan* (HEPP), for example, designed according to MIL-STD-46855A.

The standard takes into account the inherent abilities and limitations of the human being based on anthropometric data for 90% of the population of the admitted personnel (militarily dressed and equipped) when handling steering wheels, joysticks and buttons. Furthermore, the necessary control spaces are also assessed.

Designs must be adapted to applicable system and personal safety aspects, including potential human mismanagement during use and maintenance, in particular to be taken into account under stress and in non-routine use. There are detailed requirements for different pieces of equipment such as levers, steering wheels, controls, displays, computer monitors, markings, operating spaces as well as data on the physical dimensions and strengths of potential users. Furthermore, there are detailed requirements regarding dimensions, forces, colours, lighting, etc.

The standard contains examples of other applicable standards and handbooks, both military and civil. Furthermore, it contains what should be considered regarding maintenance and specifies anthropometric measurements (body measurements) as reference data.

British Defence Standards, DEF-STAN

British Defence Standards (DEF-STAN) provide, among other things, specifications to support the delivery of military capabilities. They develop and maintain relevant UK defence standards as well as provide related standardisation advice and guidance, including the status, development, selection and application of the UK defence standards. Collaboration also takes place with NATO.

DEF STAN 00-056, (System Safety)

The DEF STAN 00-056 standard, *Safety Management Requirements for Defence Systems, Issue 7* published on 28 February 2017, is developed by *the Safety Standards Review Committee of the Defence Equipment and Support* (DE&S) of *the UK Ministry of Defence* (UK MOD). The standard will primarily be applied by developing industry in conjunction with the UK Department of Defence UK MOD.

UK MOD's own operations are often governed by various *Joint Service Publication* (JSP) documents according to their own procurement model. The standard sets out requirements on

system safety operations for the entire lifetime of the technical system. The purpose of applying the standard is to provide safety for users and others who may be exposed when using the technical system. The standard can also be used for risk management regarding feared damage to property and the external environment.

The standard is divided into two parts. Part 1 sets out requirements for system safety activities and Part 2 is a guide to Part 1. Furthermore, it is clear from the standard that both the authority UK MOD and industry must comply with national legislation including EU Directives. The standard recommends applying civil open standards with the possible additions defined in Part 2 or in other defined defence standards. Regarding the accident risk of personal injury, the concept of ALARP *(As Low As Reasonably Practicable)* is central. The term is statutory in the UK. It is defined and described when and how ALARP should be applied and the result assessed. Furthermore, the application of *the Safety Case* and *the Safety Case Report* are described.

The standard can be applied in collaborative projects with the UK, but it needs to be supplemented with the Swedish Armed Forces' need for system safety documentation.

DEF STAN 00-251 - Part 3, (Human Factors)

DEF STAN 00-251 standard - Part 3, *Human Factors Integration for Defence Systems Part 3: Human Factors System Requirements*, published on 5 February 2016, by the UK Ministry of Defence (UK MOD). The standard will primarily be applied by developing industry in conjunction with the UK Department of Defence UK MOD.

The purpose of the standard is to ensure that the system design takes into account the role of the human being in the technical system, especially when there is an interface between people, equipment and processes. The standard provides requirements and guidance for the realisation, assurance and management of *Human Factors Integration* (HFI).

NATO Defence Standards, STANAG

NATO's defence standards are referred to as STANAG (*NATO Standardisation Agreement*). Associated with the standard, there may be one or more *Allied publications* (AP) and/or civil publications. *Allied publications* (AP) regulate processes, procedures, conditions and conditions for both joint military activities and for the design and development of military equipment. *Allied publications* (AP) are applied by nations that are either NATO members or who otherwise interact with NATO.

Each NATO member ratifies the relevant *Allied publications* (AP) and implements them within their own defence authority. By jointly applying *Allied publications* (AP), each Member State can benefit from another Member State's already completed development and procurement work for a given technical system as standardisation ensures that the work is in line with its own requirements. *Allied publications* (AP) also form the basis for the technical interoperability of communications and information essential to NATO and its allies' operations. Many *Allied publications* (AP) are in turn based on various civil standards from, for example, ISO. NATO Defence Standards and *Allied Publications* (AP) are published in English and French.

Since STANAG is usually a framework document with an agreement on application for a specific area, further detailed descriptions and guidance are usually provided in related documents such as AOP, AQAP, AECTP, AAS3P, AASTP and others. Relevant associated documents are referenced from the current STANAG.

Swedish Defence Standards, FSD

The Swedish defence standards (FSD) are set by FMV and consist of, among other things, standards for testing, marking, drawing techniques and materials. The material standards regulate different areas, such as paint and varnishes, packaging and distribution, iron and steel, lubricants and surface treatment. The standards are drawn up with the aim of harmonizing the technical requirements imposed on defence equipment.

Within the Swedish Armed Forces and FMV, the focus has for several years been that when choosing standards, the aim should be to minimise the use of Swedish defence standards in order to ensure interoperability.

FSD 9251, (Human factors)

The standard FSD 9251, *Integration of human factors in defence systems*, published on 25 June 2018, sets requirements for and provides guidance on how the integration of human factors is achieved, implemented and followed up in development and acquisition projects regarding defence systems.

The standard originated in the UK Department of Defence (UK MOD) first version of DEF STAN 00-251 dated 5 February 2016, and Sweden has been given permission by the UK to translate and adapt it to Swedish conditions. DEF STAN 00-251 was prepared by *Defence Equipment and Support* (DE&S). The standard has been translated and adapted by FMV within the framework of the National Defence Standardisation Agency, FSD.

The standard is intended for use in the system design of new technical systems and products, as well as in the change (modification) of existing technical systems. The standard contains both user requirements and technical requirements for human factors.

German Defence Standards

BAAINBw, (System Safety)

The *standard BAAINBw, System Safety Demonstration Handbook (01/04/2014)* is developed and published by *the German Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw)*. The standard is available in German, English and French.

The standard is primarily intended for use in the development and modification of weapon systems. The term weapon system is referred to in the standard in its broad sense to also include weapon platforms and other equipment, so the term System Safety can be considered more relevant. The standard relates to EN 61508 (series) and MIL-STD-882E in terms of methodology and definitions. The standard covers both system safety and weapon system safety.

Definitions of probabilities and severity classes are tabulated and based on examples in MIL-STD-882E and STANAG 4297/AOP-15. Furthermore, there are examples of risk matrices. The severity classification is divided into three different categories of materiel related to the size of the installation, for example for ships, combat vehicles, or components.

Standards such as DEF STAN 00-55 and IEC 61508 are related as applicable standards, supplemented by additional parts described. Furthermore, the entire software development process is described with configuration control, development tools with methods, verification and validation, as well as problems such as modularity, interfaces, reuse and monitoring of functions.

The German standard also addresses non-technical factors for system safety, mainly challenges concerning human impact on, and interaction with, a technical system. Guidance for the analysis of human error management is presented, such as probabilities of error handling.

International Electrotechnical Commission, IEC

The International Electrotechnical Commission (IEC) is an international, global standardisation body whose primary purpose is to develop and establish international standards in electrical engineering and electronics. Members are national standardisation bodies. The electricity sector through the IEC has a long tradition of drawing up global standards. IEC standards can be applied directly, but most are transferred to European EN standards through CENELEC. Some IEC standards can also be transferred directly as Swedish standards (SS). Swedish member of IEC is the Swedish Electricity Standard (SEK). In some cases, joint standardisation work IEC-ISO takes place under the leadership of one party.

IEC 61508, (Electrical/Electronic/Programmable Electronic Systems)

The series of standards IEC 61508-x, *Safety Requirements for the Functioning of Electrical, Electronic and Programmable Electronic Safety-Critical Systems,* are globally established standards for safety-critical systems. The standards are developed within *the International Electrotechnical Commission* (IEC) but have also been adopted as European and thus also as Swedish standards and are then designated SS-EN 61508-x.

The standards are generic, independent and covers the entire life cycle. They have no particular civil or military aspect. The standards apply specifically to safety features, but many parts of them, though not all, can be used for the entire technical system. There are no special requirements regarding damage to property or the environment. No connection is made to areas of activity such as land, sea or air. One area that is excluded in the standard series is medical equipment, which is instead covered by standards in the IEC 60601 and IEC 80601 *Electrical equipment for medical use*. The standard series are not harmonised with the Machinery Directive, but most European standards (as EN) in the series are intended to be harmonised with the EU Regulations (MDR, IVDR) on medical devices.

International Organisation for Standardisation, ISO

The International Organisation for Standardisation (ISO) is an international, global standardisation body, represented by national standardisation institutions. ISO operates in the non-electrical field. ISO standards cover both requirements for technical systems, products and services as well as for business management systems such as quality, environment, work environment and information security. CEN relatively often converts ISO standards into European standards (EN), which are to be transferred as Swedish standards (SS) without changes. The Swedish member of ISO and CEN is the Swedish Institute for Standards (SIS). In some cases, joint standardisation work IEC-ISO takes place under the leadership of one party.

Machinery Safety Standards Developed by ISO

A technical standard for machinery safety establishes, among other things, dimensions and sizes, as well as requirements for the function and characteristics of products. The purpose of technical standards is, on the one hand, to harmonise the latest current technical requirements in order to achieve a high level of protection of health and safety, and, on the other hand, to ensure the free movement of products in different markets.

The standards for machinery safety are divided into three categories, A, B and C. The first two categories A and B, are covered by the technical committee on the working area of the machinery safety while the C standards are developed in the respective committees for the particular type of machinery to which the standards relate.

A-standards are overarching standards that define the essential health and safety requirements for all types of machinery. Examples of A-standards are SS-EN ISO 12100, *Safety of machinery - General design principles - Risk assessment and risk reduction*.

B-standards are group standards for safety that address a safety aspect or a type of safety-related device that can be used for a variety of machines. An example of the B-standard is SS-EN ISO 13850, *Safety of machinery - Emergency stop equipment - Design principles*. The fact that it is a B-standard means that it can be applied to all types of machines where an emergency stop eliminates or reduces accident risks. The standard addresses, among other things, symbols of emergency stop devices, stop categories and requirements for the actuator itself.

For those machines that have high sources of risk and need detailed requirements, C-standards have been developed. C-standards are safety standards for machine types that provide detailed safety requirements with risk analysis, risk assessment and risk reduction for a particular machine or group of machines. If a C-standard has conflicting or more stringent requirements than those specified in the A or B standard, then it is the requirements of the C standard that are superior. Examples of areas where there are specific C-standards are lifting accessories and handheld machines.

The standard SS-EN ISO 12100, *Safety of machinery - General design principles - Risk assessment and reduction,* is an internationally accepted standard for the safety assessment of

machinery. The standard only deals with personal injury and not damage to property or the external environment. It also does not cover information security aspects.

The purpose of the standard is to provide an operator with design and production responsibilities with general guidelines and guidance for designing machinery that is safe in its intended use. In addition, it includes a strategy for the preparation of normative standards.

The standard sets out basic terminology, principles and a methodology for achieving the safe design of machinery and sets out principles for risk assessment and risk reduction. The standard refers to SS-EN IEC 60204-1, *Safety of machinery - Electrical equipment of machinery - Part 1: General receivables*, which are necessary for the purposes of this Standard. This standard is harmonised under the EU Directive for machinery as this now includes electrical risks with machines.

The standard SS-EN ISO 12100 can be applied to all types of machines, throughout their entire life cycle. It describes in detail what information is needed to carry out a risk assessment, and it describes methods for identifying, estimating and evaluating accident risks. In addition, it provides guidance on how the risk assessment and risk reduction process should be documented and verified.

Protective measures can be *design-oriented* (integrated safety), *technical protection* and/or *information* to the user. Protective measures must be taken in aforementioned order (referred to as 'integration of safety') and information must not be the only risk mitigation measure. The user can reduce the risk of accidents by practicing the prescribed modes of use and use of personal protective equipment. The system safety analysis must provide the necessary information necessary for risk assessment and to assess whether or not a risk reduction has been achieved. These assessments can be qualitative or quantitative.

SS-ISO 26262, (Road vehicles)

The standard series SS-ISO 26262-x, *Road vehicles - Reliability in electrical and electronic systems* is an international standard intended for the automotive industry. It covers the entire life cycle from concept development, to system design, hardware development, software development, evaluation, and use and maintenance. The standard series consists of ten parts.

The standard series is mainly based on IEC 61508, but are sector-specific versions for the reliability of road vehicles. The standards describe the process from a life cycle perspective. The parts of the series deal with accident risks due to the malfunction of electrical and electronic systems, but do not deal with classic accident risks such as electricity, fire and smoke. The series is solely focused on the safety of persons and does not cover damage to property, the environment or information security.

SS-EN ISO 14971, (Medical Devices)

The standard SS-EN ISO 14971, *Medical devices - Application of risk management system to medical devices* and is primarily intended for use by medical devices including in-depth or standalone software. The standard sets requirements and describes a process for how manufacturers can identify, manage (evaluate, eliminate, reduce, inform) and monitor accident risks associated with the design/use of medical devices. Accident risks are mainly

patient-related, but can also be linked to operators, equipment and the environment. The standard covers all stages of the life cycle of a medical device.

International Telecommunication Union, ITU

The International Telecommunication Union (ITU) is a global standardisation body for information and communication technology (ICT) and is a specialised agency within the United Nations. The work includes the allocation of radio frequencies and conditions, as well as technical standards for communication on land, at sea and via satellites. Publications include the Radio Regulations and Recommendations (standards). Certain publications and conditions can be made mandatory through the Swedish Post and Telecom Authority (PTS). Regarding spectrum use, there are special rules for safety and total defence authorities.

European Standardisation Organisations

European Committee for Standardisation, CEN

The Comité Européen de Normalisation (CEN) is one of the three European standardisation organisations recognised by the EU and EFTA. CEN is responsible for the development of EN standards in all areas and industries except electrical engineering and telecommunications. EN standards must be transferred to Swedish standard (SS) without amendments. CEN is an independent and non-governmental organisation represented by its standardisation bodies. SIS (Swedish Institute for Standards) represents Sweden and is thus a member of CEN. CEN may, by mandate from the Commission, create Harmonised Standards containing detailed specifications of the essential requirements of EU Directives. Much of the work is based on corresponding work and standards developed globally by ISO.

Committee for Electrotechnical Standardisation (Europe), CENELEC

The Comité Européen de Normalisation Électrotechnique, CENELEC (also abbreviated CLC) develops and establishes EN standards in the field of electrotechnical engineering. EN standards must be transferred to Swedish standard (SS) without amendments. CENELEC is an independent organisation represented by its standardisation bodies. SEK (Swedish Electricity Standard) is the Swedish national committee of CENELEC. CENELEC can also, follow a mandate from the Commission, develop Harmonised Standards that specify the essential requirements of an EU Directive. The work is primarily aimed at establishing global electricity standards developed within the IEC, as European standards.

European Telecommunications Standardisation Institute

The European Telecommunications Standards Institute (ETSI) is an independent standardisation body for information and communication technology (ICT). The organisation's members include public authorities, network operators, service providers, manufacturers, research bodies and users. The Swedish Information and Telecommunications Standardisation (ITS) is a member of ETSI and coordinates the standardisation for ICT in

Sweden. Similar to the bodies above, ETSI draws up Harmonised Standards. ETSI has some connections and takes some data from the ITU.

Other Business Standards for System Safety Operations

There are also other industry associations that issue standards in the field of system safety, both general and sector-specific.

GEIA-STD-0010A, (System Safety)

The GEIA-STD-0010A *Standard Best Practice for System Safety Program Development and Execution* (October 2015) was developed and published by *the Information Technology Association of America* (ITAA) *G-48 System Safety Committee*. The standard is also an *American National Standard Institute* (ANSI) standard.

The GEIA-STD-0010A standard is a civil equivalent to the MIL-STD-882E and can be applied in its entirety to military materiel. However, some additions are required such as activities for requirement and decision documents. The standard is intended to be used primarily by an actor with design and production responsibility in the development of technical systems. The standard contains definitions of key terms and concepts as well as a model for summarising accident risks for the technical system. The standard specifies a number of minimum requirements in the form of elements that should always be met for all systems. The term ALARP *(As Low As Reasonably Practicable)* is used.

SAE ARP 4754A, (Aviation)

The standard SAE ARP4754A, *Aerospace Recommended Practice - Guidelines for Development of Civil Aircraft and Systems* applies to system aspects and refers to DO-178C/ED-12C for software development and DO-254/ED-80 for the development of programmable logic (Airborne Electronic Hardware, "*Functions that are allocated to hardware*") and to SAE ARP 4761 for conducting system safety analysis. The standard is developed in collaboration between manufacturers, authorities and research institutions in the USA, Canada and Europe. The standard cannot be used separately but must be used in conjunction with the aforementioned associated standards. The standard does not cover information security aspects.

The SAE ARP 4754A standard is a civil standard for aircraft, but is often also applied to military systems. The standard describes a working method for the development efforts where the system safety impact (airworthiness impact) of each function and component controls which work is to be carried out and with what stringency. This classification occurs through the assignment of *Development Assurance Level,* FDAL to functions and IDAL to components (*items*). It describes which combinations of *Development Assurance Level* (DAL*)* in constituent parts can be accepted for different classes of consequences.

Appendix 3 - Description of System Safety Activities

The purpose of this appendix is to describe the unique Swedish activities and the activities described in the standard MIL-STD-882E. Furthermore, adaptations are described that are needed based on descriptions in the standard MIL-STD-882E standard to suit the work of the Swedish defence authorities.

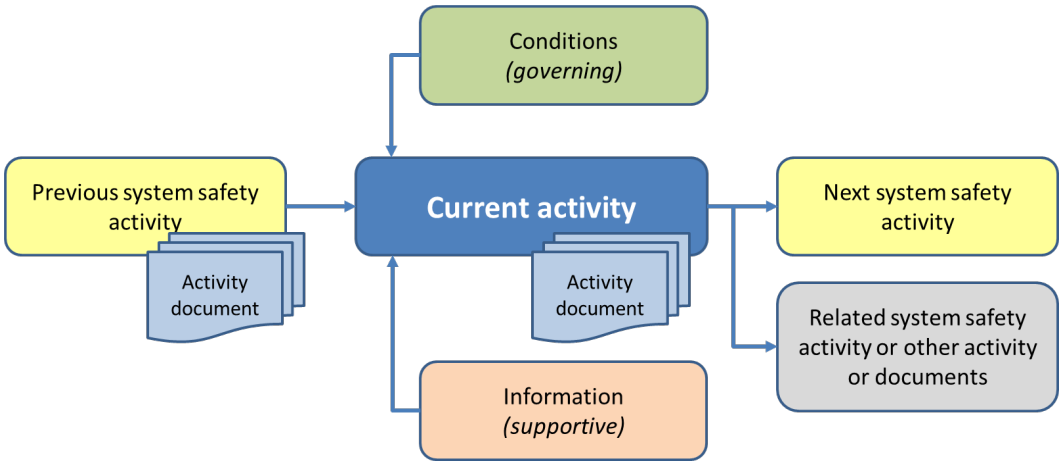
Activity Presentation

The unique Swedish activities are identified by the letter "S" followed by a two-digit number. The other activities, based on MIL-STD-882E, are in some cases adapted to the system safety work of the Swedish defence authorities.

A cursively marked activity is described in MIL-STD-882E, but is not used in the Swedish defence authorities' system safety work.

For each activity, the formations are as below:

- *Purpose and activity description* explain the purpose of the activity and how the activity is appropriately carried out. In some cases, there are checklists to follow. It also includes its Swedish and English designations of the activity and documentation
- *Input, output* and *flowchart* indicate the information needed to carry out the activity and the documentation (activity document) that is produced



Appendix 3, figure 5 *For each activity there is a figure that shows input, activity, activity documents, and output to support upcoming activities.*

Prerequisites (green box) are considered controlling the current activity, while *Information* (orange box) is considered supportive. Gray boxes point to related system safety activities, alternatively to other activities or documents.

Process Description Based on the Stakeholder

Stakeholder, client, *system integrator* and *designer* can basically carry out the same activities and broadly follow the same activity descriptions. The activities can be used on different occasions during system safety work, but also with slightly different purposes and scope.

This means that input, prerequisites (controlling), and information (supporting) can differ between roles, meaning that the amount of work and the volume of output can vary between the *stakeholder, client*, *system integrator*, and *designer*.

The order of activities and the figures in the respective activity primarily support the system safety activities of *the stakeholders*. There are also figures for *the clients*, *system integrators* and *designers* during the majority of the activities, although they are not always presented in a logical process flow for these roles.

Activities - SECTION 100 Planning/Control

TASK 101 - SYSTEM SAFETY PROGRAM (SSP)

This activity is replaced by S11 - System Safety Program (SSP), Task 102 - System Safety Program Plan (SSPP) as well as Chapter 14 Risk Matrix and Tolerable Risk Level.

S11 - SYSTEM SAFETY PROGRAM (SSP)

Purpose and Activity Description

The purpose of this activity is to control and target the system safety activities of the *stakeholder* in a lifecycle perspective for combat force area, product area or in some cases for complex technical systems.

The output/documentation from this activity is *System Safety Management Plan* (SSMP).

The *stakeholder's* system safety work is set out in a *System Safety Management Plan* (SSMP) and then constitutes system safety control documents for various objectives and requirements documents such as *System Objective* (SMS) and *Request for Proposal* (RFP). All technical systems and products must be subject to a *System Safety Management Plan* (SSMP).

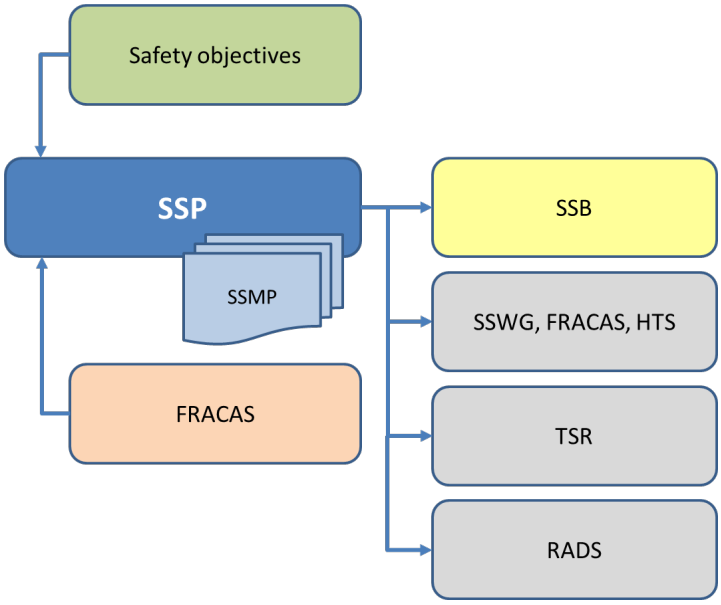
The *stakeholder* identifies overall current EU law, Swedish law and the domains of standards and other regulatory frameworks to apply. Furthermore, commonly occurring accident risks that have dimensional consequences on current equipment in the field are identified. *Tolerable Risk Level* Requirements (TR) expressed in Risk Matrices are set and focus on how to carry out system safety activities based on the mandatory and the selectively chosen activities. The *System Safety Management Plan* (SSMP) also provides instructions for the work that takes place in the *System Safety Working Group* (SSWG).

The *System Safety Management Plan* (SSMP) together with *System Objective* (SMS) control the *stakeholder's* upcoming system safety work for the technical systems in focus.

Input, Output and Flowchart

The input to the *System Safety Program* (SSP) activity consists of safety objectives and experience data from the *Failure Reporting System* (FRACAS).

Output is the *System Safety Management Plan* (SSMP). This provides input to the *System Safety Evaluation* (SSB), *System Safety Working Group* (SSWG), *Training Safety Regulations* (TSR) and *Risk Assessment Prior to Disposal of System* (RADS).



Appendix 3, figure 6 *System Safety Program (SSP).*

A *System Safety Management Plan* (SSMP) should include:

- The arena, product area or technical system covered
- An organisational description of the system safety activities and how they interact with other actors and stakeholders
- What system safety activities are carried out throughout the entire lifecycle
- Actions and acceptance criteria for permitted route selections under the *Route Selection Model* (VVM)
- Which EU and Swedish law and the domains of standards and other regulatory frameworks are to be applied
- System safety objectives including requirements concerning *Tolerable Risk Level* (TR) are expressed in risk matrices
- Requirements for Swedish Armed Forces *stakeholders* and/or *designers* to develop *System Safety Program Plans* (SSPPs) for system safety work in the event of change (modification), system-in-systems work and in the acquisition of technical systems and products
- How completed system safety work must be documented and reported
- Criteria for when to issue system safety decisions
- How safety deficiencies on technical systems and products are managed
- A job description for the *System Safety Working Group* (SSWG)
- Handling of data from accidents, incidents and failure reporting
- How accident risks are managed that may occur during disposal
- A list of commonly occurring accident risks in the product area
- Revision of the *System Safety Management Plan* (SSMP)

S12 - SYSTEM SAFETY EVALUATION (SSB)

Purpose and Activity Description

The purpose of this activity is to prioritise, rank and/or describe the pros and cons of alternative concepts or technology solutions from a system safety point of view.

The output/documentation from this activity is *System Safety Concept Evaluation* (SSKB).

System Safety Evaluation (SSB) is carried out prior to starting technical system requirements to identify, analyse and weigh dimensional system safety aspects against other general factors such as impact and other performance. The activity is intended to provide support in the development of *System Objective* (SMS), but it can also be applied in the *Research and Technology Development* (FOT) activities.

The *stakeholder* identifies potentially intractable system safer aspects on the basis of assessing the possibility of managing these accident risks in technical systems or operations. For example, unproven technology, manageability of certain accident risks and environmental impact during use and disposal should be taken into account.

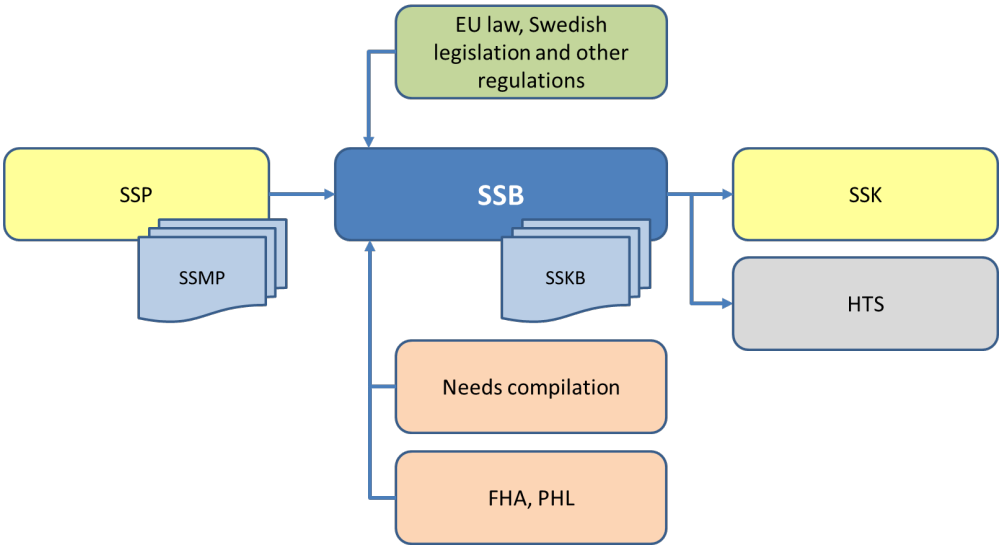
The *stakeholder* identifies dangerous conditions and situations that may occur. In addition, hazardous subsystems, products and chemical products are listed. *System Safety Concept Evaluation* (SSKB) focuses on the most difficult to assess potential accident risks and provides a decision-making basis for the *stakeholder*.

For unproven technology, further study or investigation may be required. For the manageability of accident risks and environmental impact, protection measures may need to be taken such as large risk areas, restrictions on use or the need for Personal Protective Equipment (PPE).

Input, Output and Flowchart

The input to the *System Safety Evaluation* (SSB) activity consists of the *System Safety Management Plan* (SSMP), legislation and documentation from the *Compilation of needs* activity. To identify hazardous conditions and situations, initial risk assessments according to *Functional Hazard Analysis* (FHA) and *Preliminary Hazard List* (PHL) can be applied.

The output is the *System Safety Concept Evaluation* (SSKB). This provides input to *System Safety Requirements* (SSK) and *Hazard Tracking System* (HTS).



Appendix 3, figure 7 *System Safety Evaluation (SSB).*

A *System Safety Evaluation* (SSB) should include:

- The technology covered and its maturity rate
- The data and prerequisites used and the assumptions made
- Description of the risk analysis methods used
- What accident risks may occur and its assessed consequences
- Summary of results
    - Evaluation (different options)
    - Ranked
    - Pros and cons
- Patterning of intractable technology solutions
    - Recommendation on risk-reducing measures
    - Proposal for future system safety testing
- Detailed accounting on the basis of the summary

S13 - SYSTEM SAFETY REQUIREMENTS (SSK)

Purpose and Activity Description

The purpose of this activity is to identify the system safety requirements to be included in various objective and requirements documents.

The output/documentation from this activity is *System Safety Requirement* (SSK).

System Safety Requirements (SSK) are identified in EU law, Swedish law, regulatory framework, *Design Rules* (DR) and based on experience gained. Identified system safety requirements consist, on the one hand, of technical requirements affecting the design and, on the other hand, by system safety requirements to demonstrate that the technical system offers a satisfactory level of safety. To support this activity, the *Route Selection Model* (VVM) is applied.

The *stakeholder's* purpose for this activity is to identify the technical system safety requirements to be included in *System Objective* (SMS 2) for the technical system concerned. Also included are the *stakeholder's* demands on the *client's* system safety work. The *System Objective* (SMS 2) usually refers only to the current *System Safety Management Plan* (SSMP). However, additional technical system safety requirements as well as extended demands for the *stakeholder*'s system safety work may be required on the basis of the current technical system.

The *Stakeholder*'s work is based on the *System Safety Management Plan* (SSMP), the *System Safety Evaluation* (SSB) and the basis of the *Compilation of needs* activity and, if necessary, specifies the requirements for the *client* to be able to demonstrate that a satisfactory level of safety is achieved through the permitted route selections in the *Route Selection Model (VVM)*. Overall acceptance criteria as well as any boundary conditions and restrictions are set for the respective route selections. Complementary technical system safety requirements are set at a principal level without limiting the design of *the stakeholder's* or by extension the *designer's* technical system. All technical systems and products must be subject to some *System Objective* (SMS 2).

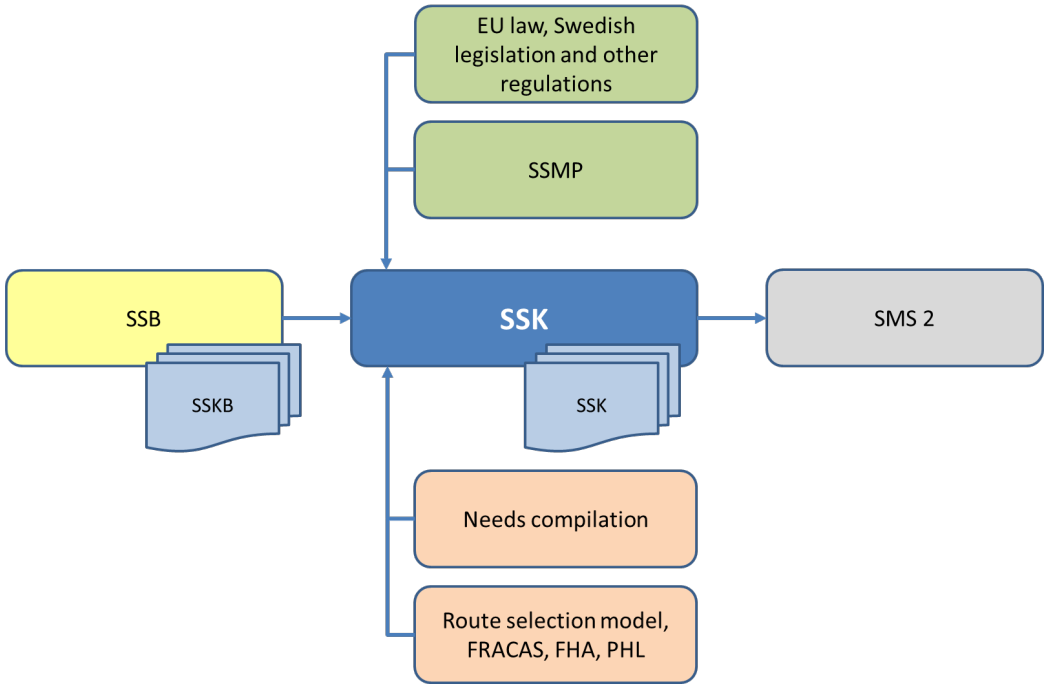
The *stakeholder's* purpose for this activity is to identify the technical system safety requirements to be included in the *Request for Proposal* (RFP) for the technical system concerned. The *stakeholder's* requirements for the *designer's* system safety work must also be included in the *Request for Proposal* (RFP). The system safety requirements of the current *System Objective* (SMS 2) are translated into unambiguous and verifiable requirements in the *Request for Proposal* (RFP). However, additional technical system safety requirements as well as extended demands for the *stakeholder*'s system safety work may be required on the basis of the technical system concerned.

The *client's* work is based on the current *System Objective* (SMS 2) and clarifies the requirements for a satisfactory level of safety through the permissible route selections in the *Route Selection Model* (VVM). Acceptance criteria as well as possibly tightened boundary conditions and restrictions are set out. Complementary technical system safety requirements are imposed at a functional level without limiting the design of the technical system by the designer. All technical systems and products to be procured or changed (modified) must be subject to a *Request for Proposal* (RFP).

Input, Output and Flowchart

The input to the *System Safety Requirements* (SSK) activity for *stakeholders* consists of *System Safety Evaluation* (SSB), legislation and *System Safety Management Plan* (SSMP) as well as data from the activity's *Compilation of needs*, for example studies and experiences from the technical systems and products to be replaced. As additional support, *Functional Hazard Analysis* (FHA) and *Preliminary Hazard List* (PHL) can be applied.

Output is the *System Safety Requirements* (SSK) that the *stakeholder* must include in the *System Objective* (SMS 2).



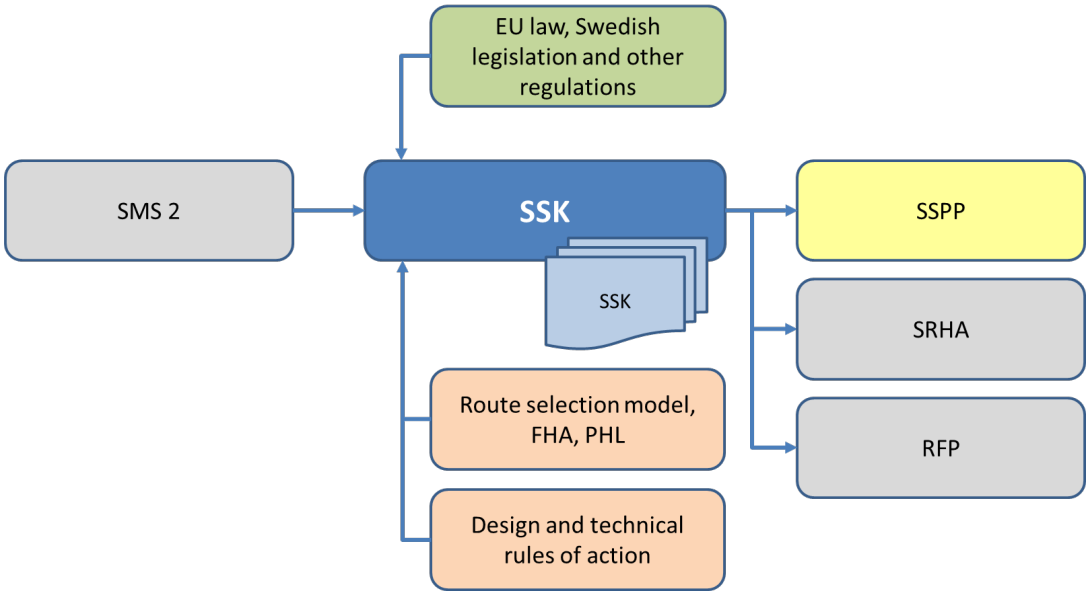
Appendix 3, figure 8 *System Safety Requirements (SSK) for stakeholders.*

System Safety Requirements (SSK) for *System Objective* (SMS 2) should include, in addition to the requirements set out in the *System Safety Management Plan* (SSMP):

- Technical requirements:
  - Any specific requirements on EU law, Swedish legislation and on specific standards and other regulatory frameworks must apply
  - What *Design Rules* (DR) to apply
- Activity commitment:
  - Detailed actions and acceptance criteria for permitted route selections under the *Route Selection Model* (VVM)
  - Any additional requirements for system safety activities to be implemented during the lifecycle

The input to the *System Safety Requirements* (SSK) activity for *clients* consists of *System Objective* (SMS 2), legislation and *Design Rules* (DR) as well as *Technical Rules of Practice* (THR). As additional support, *Functional Hazard Analysis* (FHA) and *Preliminary Hazard List* (PHL) can be applied.

The output is the *System Safety Requirements* (SSK) that the *client* must add to their *System Safety Program Plan* (SSPP) and in the *Request for Proposal* (RFP), respectively. The *System Safety Requirements* (SSK) will also be input to the *Stakeholder's System Requirements Hazard Analysis* (SRHA).



Appendix 3, figure 9 *System Safety Requirements (SSK) for clients.*

System Safety Requirements (SSK) for a *Request for Proposal* (RFP) should include, in addition to the requirements set out in the *System Objective* (SMS 2):

- Technical requirements:
  - Which EU law, Swedish legislature and which domains/specific standards and other regulatory frameworks should be met
  - Principle design requirements (design rules) on the intended technical system
  - System safety objectives including requirements concerning *Tolerable Risk Level* (TR) expressed in risk matrices
- Activity commitment:
  - An organisational description of the system safety activities and how it interacts with other actors and stakeholders
  - Actions and acceptance criteria for permitted route selections under the *Route Selection Model* (VVM)
  - Requirements to develop a *System Safety Program Plan* (SSPP) as part of the contract describing the system safety work to be carried out
  - How completed system safety work must be documented and reported

TASK 102 - SYSTEM SAFETY PROGRAM PLAN (SSPP)

Purpose and Activity Description

The purpose of this activity is to describe the system safety work that the *client* and *designer* plans to carry out for the actual technical system. The activity can be applied, on the one hand, for internal operations and also for system safety work agreed in contracts.

The out data/documentation from this activity is a *System Safety Program Plan* (SSPP). The *System Safety Program Plan* (SSPP) activity includes MIL-STD-882E Task 103, *Hazard Management Plan* (HMP). The activity also includes Task 108, *Hazardous Material Management Plan* (HMMP) regarding health and environmental aspects.

The *System Safety Program Plan* (SSPP) must, on the basis of the route selections made in the *Route Selection Model* (VVM), outline the planned system safety work required to meet the requirements and describe how the results of this work will be documented.

The *client's* internal system safety work for a particular technical system is described in a *System Safety Program Plan* (SSPP) and is part of the *client's* project plan. The *System Safety Program Plan* (SSPP) describes the system safety activities that the client intends to implement and how this is intended to be documented. Further, the system safety documentation is provided to the *stakeholder,* during System Handover (SÖL) as well as the requirements to be placed on the *designer* or *system integrator*.

The *designer's* system safety work for a particular technical system is described in a *System Safety Program Plan* (SSPP) and is part of the designer*'s* project plan. The content and scope of the *System Safety Program Plan* (SSPP) is governed by the contract. The *System Safety Program Plan* (SSPP) describes the system safety activities that are intended to be implemented and how these are intended to be documented. This so that the *designer* can finally reach a point that the technical system offers a satisfactory level of safety.

A preliminary *System Safety Program Plan* (SSPP) may, at a pre-contract stage, evaluate a potential *designer's* understanding and prioritisation of the system safety work required in the development or modification of technical systems.

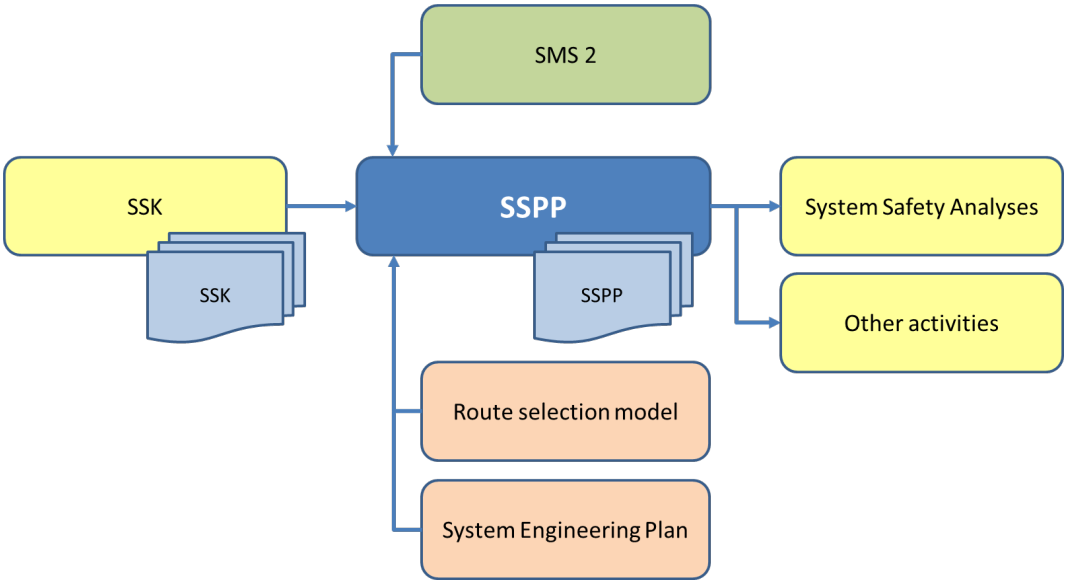
The *designer* can add additional system safety activities than those required by the *client*. Furthermore, the system safety documentation is provided to the *client* in connection with delivery and the requirements for system safety work that it intends to impose on subcontractors. The *System Safety Program Plan* (SSPP) often forms an integral part of the *System Engineering* process with its technical reviews such as the *Preliminary Design Review* (PDR) and *Critical Design Review* (CDR) and should therefore be coordinated with these.

The *System integrator´s* system safety work for a particular system-of-systems is regulated by the *client's System Safety Program Plan* (SSPP). The *client* describes the system safety activities that the *system integrator* least needs to implement and how this is intended to be documented. This is so that the *client* can finally make a stand that the co-operation between technical systems and products into a system-of-system offers a satisfactory level of safety.

Input, Output and Flowchart

The input to the *System Safety Program Plan* (SSPP) activity for the *client* consists of *System Safety Requirements* (SSK) and *System Objective* (SMS 2). To support this activity, the *Route Selection Model* (VVM) is applied.

The output is the *System Safety Program Plan* (SSPP) according to which the *client* will work and identify requirements out of which can be transferred to the *Request for Proposal* (RFP). The *System Safety Program Plan* (SSPP) will also describe which system analyses and other activities the *client* will carry out, which can be found in sections 200 - 500.



Appendix 3, figure 10 *System Safety Program Plan (SSPP) for the client.*

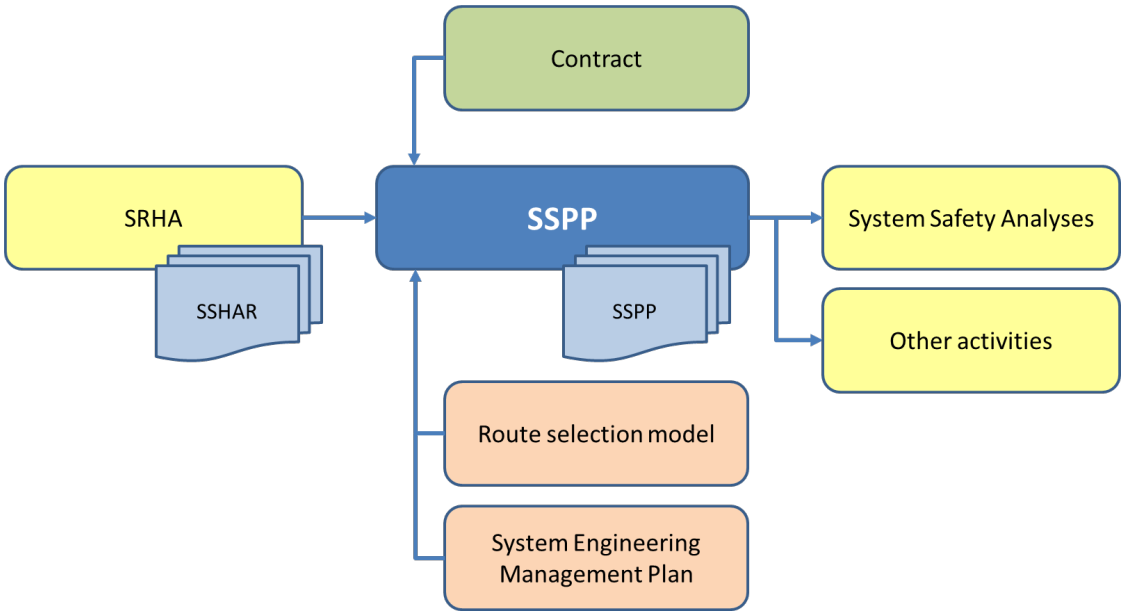
A *System Safety Program Plan* (SSPP) for the *client* should include:

- Purpose, scope and description of the technical system and its use
- An organisational description of the system safety work and how it (internally and externally) interacts with the Swedish Armed Forces, other actors and other stakeholders including interaction with other related areas of expertise (see *Figure 2.7*)
- What EU and Swedish law, standards and other regulatory frameworks are to be applied and how *System Safety Requirements* (SSK) are implemented
- System safety objectives including requirements concerning *Tolerable Risk Level* (TR) are expressed in risk matrices
- Actions and acceptance criteria for permitted route selections under the *Route Selection Model* (VVM)
- Management of Government Furnished Equipment (GFE) and other integration products
- A process description related to the *System Engineering* process of the system safety work to be carried out and how this is to be documented and reported
- Implementation of system safety briefings in the *System Safety Working Group* (SSWG) and the *Integrated Product Team/System Safety Group* (IPT/WG)
- A description of the system safety analyses to be carried out, how they are documented and how experienced data are taken care of
- How verification and validation of system safety requirements are carried out
- A process description for the closure of system safety work for accident risks and procedures for managing restrictions
- How the system safety evaluation is prepared
- How the production of the *System Safety Declaration* (SSD), *Safety Assessment Report* (SAR), *Risk Log* (RL) and other system safety documentation takes place

- How the development of technical information based on system safety work takes place
- How the implementation of training takes place
- How the management of failure reporting takes place
- How audits of the *client's System Safety Program Plan* (SSPP) are managed

The input to the *System Safety Program Plan* (SSPP) activity for the *designer* consists of the *System Requirements Hazard Analysis* (SRHA) and the contract with the *client.* To support this activity, the *Route Selection Model* (VVM) is applied.

The output is the *System Safety Program Plan* (SSPP) that the *designer* will work on. The *System Safety Program Plan* (SSPP) describes which system safety analyses and other activities the *designer* will carry out, which can be found in sections 200 - 500.



Appendix 3, figure 11 System Safety Program Plan (SSPP) for the designer.

A *System Safety Program Plan* (SSPP) for the *designer* should include:

- Purpose, scope and description of the technical system and its use
- An organisational description of the system safety work and how it (internally and externally) interacts with the Swedish Armed Forces, other actors and other stakeholders including interaction with other related areas of expertise (see *Figure 2.7*)
- What EU and Swedish law, standards and other regulatory frameworks are to be applied and how *System Safety Requirements* (SSK) are implemented
- System safety objectives including requirements concerning *Tolerable Risk Level* (TR) expressed in risk matrices
- Actions and acceptance criteria for permitted route selections under the *Route Selection Model* (VVM)

- Management of Government Furnished Equipment (GFE) and other integration products
- A process description related to the *System Engineering* process of the system safety work to be carried out and how this is to be documented and reported
- Implementation of system safety briefings in the *Integrated Product Team/System Safety Group* (IPT/WG)
- A description of the system safety analyses to be carried out, how they are documented and how experienced data are taken care of
- How verification and validation of system safety requirements are carried out
- A process description for the closure of system safety work for accident risks and procedures for managing restrictions
- How the system safety evaluation is prepared
- How the production of the *System Safety Declaration* (SSD), *Safety Assessment Report* (SAR), *Risk Log* (RL) and other system safety documentation takes place
- How the development of technical information based on system safety work takes place
- How the implementation of training takes place
- How the management of failure reporting takes place
- How audits of the *System Safety Program Plan* (SSPP) are managed

TASK 103 - HAZARD MANAGEMENT PLAN (HMP)

This activity is included in TASK 102 - System Safety Program Plan (SSPP).

TASK 104 - SUPPORT OF GOVERNMENT REVIEWS/AUDITS (SGRA)

This activity is regulated partly by the Weapons and Ammunition Safety Handbook (H VAS) for FMV's Weapons and Ammunition Safety Advisory Groups, and by participation in the Swedish Armed Forces' Commission of Inquiry (FMUK) and in the respective client's System Safety Program Plans (SSPPs) for other Government reviews.

S14 –SYSTEM SAFETY WORKING GROUP (SSWG)

Purpose and Activity Description

The purpose of this activity is to be an advisory function to the *stakeholder* in the field of system safety. The *System Safety Working Group* (SSWG) can, on the one hand, monitor technical systems and products during the maintenance phase and also prepare cases related to system safety. The Swedish Armed Forces establish *System Safety Working Groups* (SSWG).

The output/documentation from the activity consists of minutes or meeting notes.

The Chairman of the *System Safety Working Group* (SSWG) maintains a job description based on the requirements of the *System Safety Management Plan* (SSMP). The Chairman directs the operational work to propose staffing for the Working Group, calling meetings and keeping minutes or meeting notes. *The client* can be co-opted to the work group. The *System*

Safety Working Group (SSWG) should have occasional single fixed meeting times, but otherwise meet when necessary.

The *System Safety Working Group* (SSWG) updates *Risk Log* (RL) based on information provided by authorities or manufacturers, information about accidents, incidents or anomalies, and *System Safety Announcement* (SSM) or other user experiences. The working group proposes safety-enhancing measures such as changes (modifications) or awareness campaigns.

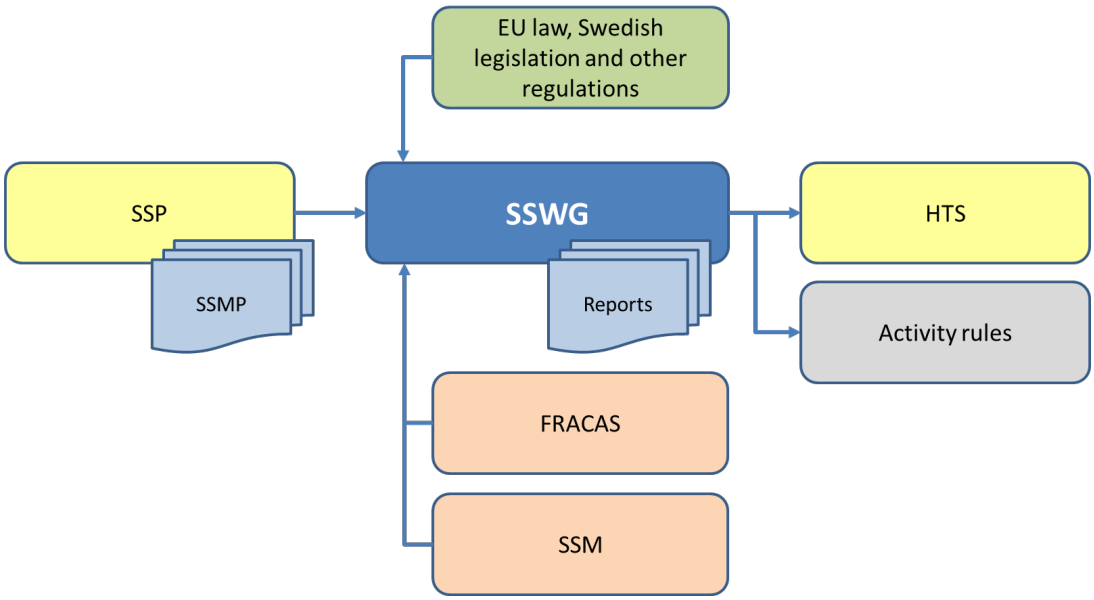
If a *System Safety Announcement* (SSM) only consists of information to clarify that information to clarify, inform or remind the user of conditions related to the intended use, change of use including norm slippage or that operating rules need to be tightened, the case may be closed by the Chairman of the *System Safety Working Group* (SSWG), without new system safety decisions being issued.

If a *System Safety Announcement* (SSM) is withdrawn by the issuer and if the safety deficiency is no longer considered current, this is to be documented. The case is closed by the Chairman of the *System Safety Working Group* (SSWG).

Input, Output and Flowchart

The input to the *System Safety Working Group* (SSWG) is comprised of the *System Safety Management Plan* (SSMP), legislation and experience data from the *Failure Reporting System* (FRACAS), *System Safety Announcement* (SSM) and other user experiences.

Output consists of minutes or meeting notes. These provide input to the *Hazard Tracking System* (HTS) and provide the basis for revision of operating rules.



Appendix 3, figure 12 *System Safety Working Group (SSWG).*

TASK 105 - INTEGRATED PRODUCT TEAM/SYSTEM SAFETY GROUP (IPT/WG)

Purpose and Activity Description

The purpose of this activity is to be a meeting forum between the *client* and the *designer*, on the one hand to follow up on the development work of the technical system, and also to follow up that the *designer* complies with the *System Safety Program Plan* (SSPP). The *stakeholder* can be co-opted to the meeting forum.

The output/documentation from the activity´s system safety briefings are minutes or meeting notes.

In the MIL-STD-882E standard there are two different system safety related groups, are defined *Integrated Product Team* (IPT) and *Working Group* (WG). A *Working Group* (WG) has as its primary task to address system safety aspects. An *Integrated Product Team* (IPT) can handle additional aspects alongside those that are system safety related. Groups can be set up for an individual project and its tasks and authorities are governed by the contractual *System Safety Program Plan* (SSPP).

Parties to the *Integrated Product Team/System Safety Group* (IPT/WG) may conduct preparatory system safety reviews of the technical system in the run-up to the project's technical reviews such as the *Preliminary Design Review* (PDR) and *Critical Design Review* (CDR).

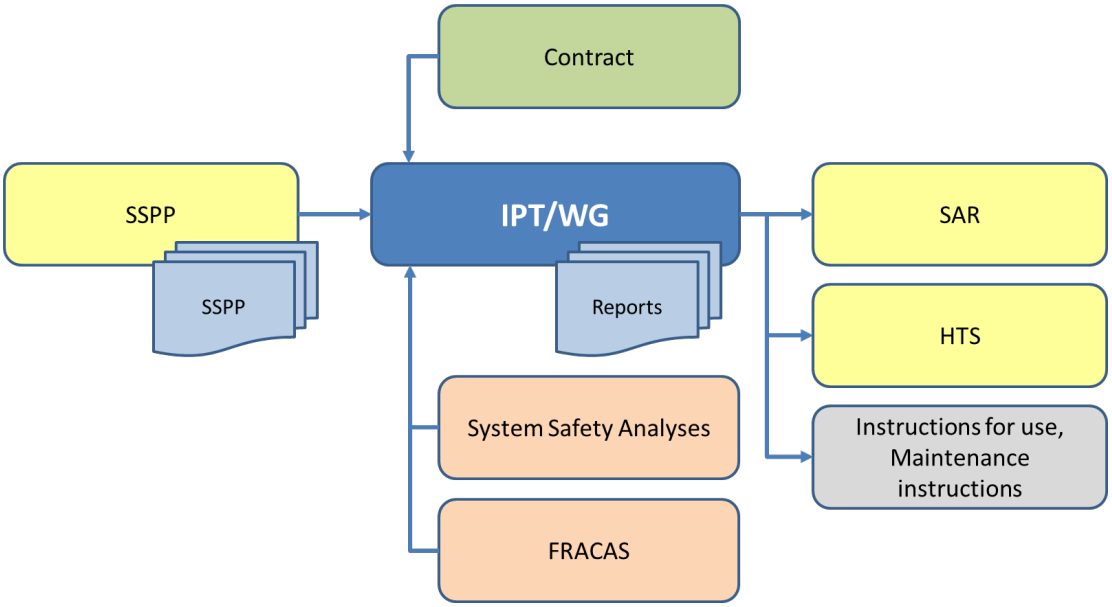
The *Integrated Product Team/System Safety Group* (IPT/WG) handles the following system safety-related parts:

- To agree, within the framework of the contract, on the *System Safety Program Plan* (SSPP) including updates
- Follow-up of system safety work in accordance with the agreed *System Safety Program Plan* (SSPP) and where there is a need for revision
- Reviewing system safety related requirements and requirement verification
- *Risk log* review (RL) of identified accident risks and its status regarding risk-reducing work
- Review of other system safety documentation such as *Safety Assessment Report* (SAR), lists and system safety evaluation
- Management of any problems with risk-reducing measures, which may need to be decided by the project

Input, Output and Flowchart

The input to the *Integrated Product Team/System Safety Group* (IPT/WG) activity consists of the *System Safety Program Plan* (SSPP) and the contract, as well as results from system safety analyses and data from the *Failure Reporting System* (FRACAS).

Output consists of minutes or meeting notes. The information from these is inserted into the *Safety Assessment Report* (SAR) and the *Risk Log* (RL). Furthermore, the information may affect the content of operating instructions and maintenance instructions.



Appendix 3, figure 13 *Integrated Product Team/System Safety Group (IPT/WG).*

TASK 106 - HAZARD TRACKING SYSTEM (HTS)

Purpose and Activity Description

The purpose of this activity is to create a risk management process and carry out ongoing risk monitoring, and have compiled information and overall positional view of all identified accident risks for a particular technical system.

The output/documentation from the activity is a *Risk Log* (RL).

Information on completed and planned accident risk management and the status of the identified accident risks is compiled in a *Risk Log* (RL). The *Safety Assessment Report* (SAR), or the underlying system safety analysis reports, provides the detailed description of the accident risks and the results of the system safety analyses carried out. The *Risk Log* (RL) is a complement to the *Safety Assessment Report* (SAR) and also contains the current status of the ongoing risk-reducing work.

Stakeholder, client and *designer* can have their own *Hazard Tracking System* (HTS) and the *Risk Log* (RL) for various technical systems on an ongoing basis. Contracts between the *client* and the *designer* are the requirements that apply to *Hazard Tracking System* (HTS) with the associated *Risk Log* (RL). It can be advantageous if the *Risk Log* (RL) has the same setup and outline regardless of the actor currently responsible for its content. In this way, the *Risk Log* (RL) can be maintained for the technical system throughout its lifetime.

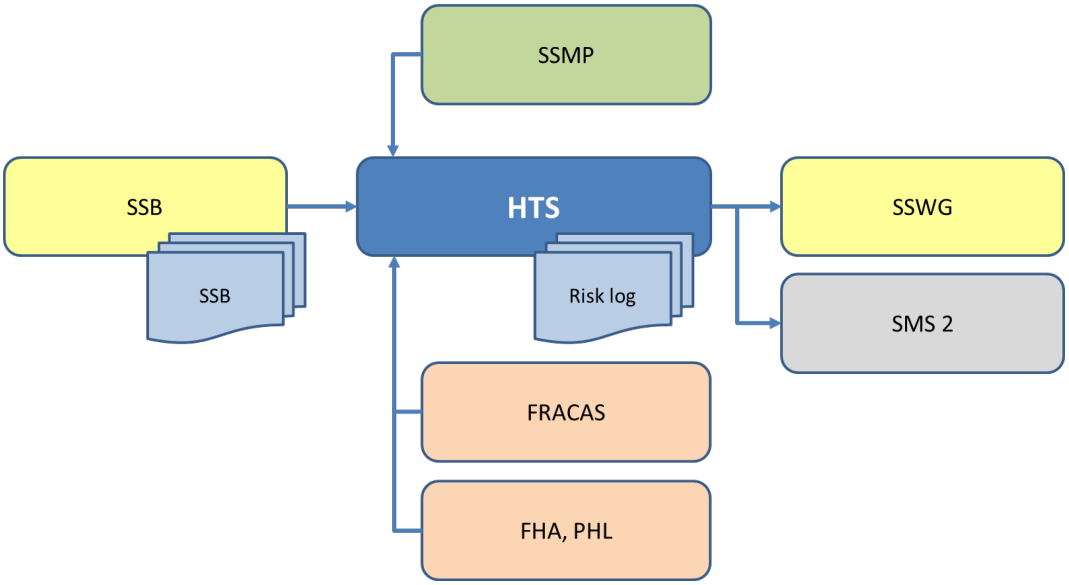
The *stakeholder* lists the most common accident risks in a *Risk Log* (RL) that the *client* needs in order to manage accident risk. The *client* can supplement the *Risk Log* (RL) with additional accident risks and this is attached to the *Request for Proposal* (RFP). The *designer* then adds all identified accident risks to the current technical system. Upon delivery, the *client* receives the *Designer 's Risk Log* (RL) for continued accident risk management. After accident risk management is completed, this is submitted to the *stakeholder* for final accident risk management. The *stakeholder* could in this way provide the *System Safety Working Group*

(SSWG) with the *Risk Log* (RL) for the continuous safety work during the maintenance and disposal phases.

Input, Output and Flowchart

The input to the *Hazard Tracking System* (HTS) activity for the *stakeholder* consists of the *System Safety Evaluation* (SSB) and the *System Safety Management Plan* (SSMP) as well as data from the *Failure Reporting System* (FRACAS) and results from various system safety analyses.

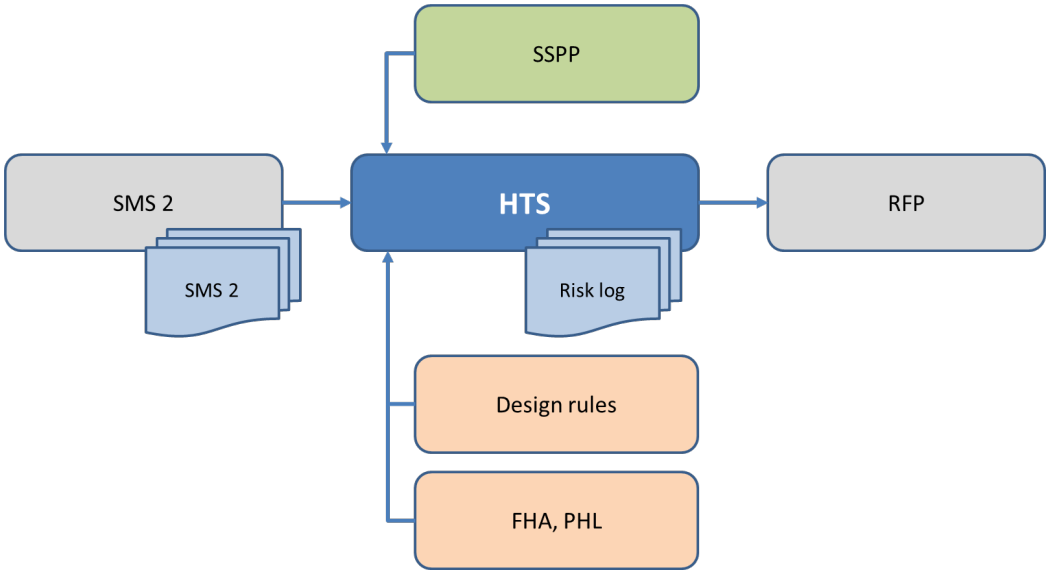
The output is the *Risk Log* (RL). This provides input to the *System Safety Work Group* (SSWG) and *System Objective (*SMS 2).



Appendix 3, figure 14 *Hazard Tracking System (HTS) for Stakeholder.*

The input to the *Hazard Tracking System* (HTS) activity for the *client* consists of *System Objective* (SMS 2) and the *System Safety Program Plan* (SSPP), *Design Rules* (DR) and results from *Functional Hazard Analysis* (FHA) as well as *Preliminary Hazard List* (PHL).

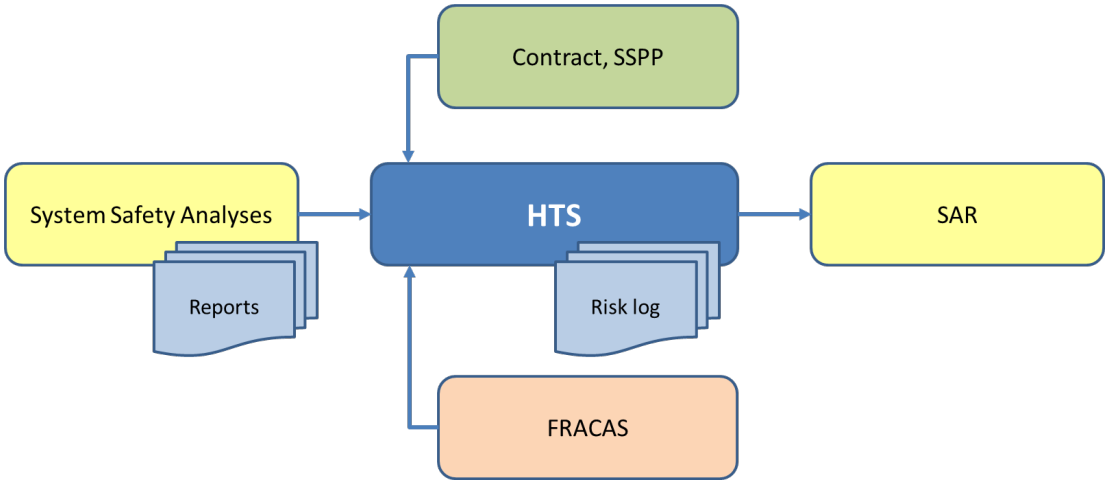
The output is the *Risk Log* (RL). This provides input to the *Request for Proposal* (RFP).



Appendix 3, figure 15 *Hazard Tracking System (HTS) for client.*

The input to the *Hazard Tracking System* (HTS) activity for *the designer* consists of various system safety analyses and the contractual *System Safety Program Plan* (SSPP) as well as data from the *Failure Reporting System* (FRACAS).

The output is the *Risk Log* (RL). This provides input to the *Safety Assessment Report* (SAR).



Appendix 3, figure 16 *Hazard Tracking System (HTS) for designer.*

The *Risk Log* (RL) should contain the following information:

- The technical system or product referred to
- Risk identification (risk number and accident risk and, if necessary, standard scenarios, hazardous events, hazardous conditions, etc.)
- What route selection choices were applied
- Risk assessment before risk-reducing measures
- Risk-reducing measures specifying the verification and validation method
- Risk assessment after risk-reducing measures
- Risk reducing after application of exposure and controllability factors

- Reference number for minutes or meeting notes for decisions taken
- Acceptance decisions (measures introduced and verified respectively)
- Status of risk-reducing work for individual accident risks
- Accident risks removed after risk-reducing measures
- Notes

TASK 107 - HAZARD MANAGEMENT PROGRESS REPORT (HMPR)

This activity is part of the Integrated Product Team/System Safety Group (IPT/WG).

TASK 108 - HAZARDOUS MATERIALS MANAGEMENT PLAN (HMMP)

This activity is included in TASK 102 - System Safety Program Plan (SSPP).

Activities - SECTION 200 - Analyses

TASK 208 - FUNCTIONAL HAZARD ANALYSIS (FHA)

Purpose and Activity Description

The purpose of this activity is, on the one hand, to classify system functions from the point of view of criticality for requirements, and also to identify and evaluate functionally related accident risks for individual technical systems and products or system-of-systems.

The output/documentation from the activity is a *Functional Hazard Analysis* (FHA).

The *Functional Hazard Analysis* (FHA) can be based on developed system architecture and on experience data from the *Failure Reporting System* (FRACAS). The identified system functions are analysed for input, output and interactions with other subsystems, in order to allocate the potential malfunctions to the relevant subsystems and as a basis for the classification of safety-critical functions according to *Safety-Critical Functions* (SCF). For requirements, principled design measures are identified to eliminate or reduce accident risks to the technical system. For the functionally related accident risks inserted in the *Risk Log* (RL), the consequences of these malfunctions are primarily assessed.

When devising a safety architecture, critical system functions can be allocated among or within technical systems. Critical system functions can be split between functional or physical components such as hardware, electronics, or software, but can also affect user interfaces based on usability. The *Functional Hazard Analysis* (FHA) identifies safety-critical software for further management according to the Software in Safety-Critical Applications Handbook (H ProgSäk E).

The *stakeholder* identifies functional accident risks with its dimensional consequences and inserts them into the *Risk Log* (RL). The result is input to the *System Safety Evaluation* (SSB).

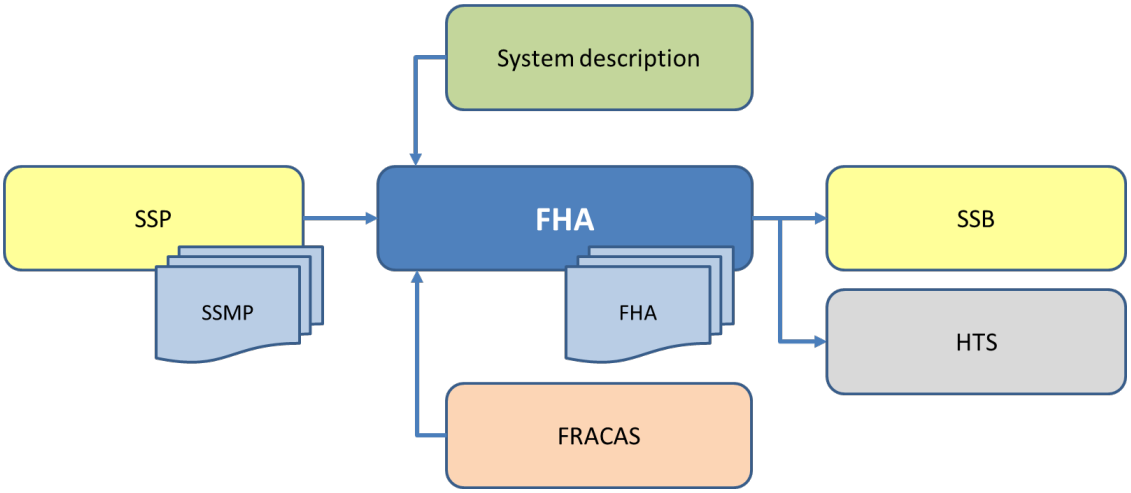
The *client* identifies functional accident risks with its dimensional consequences and inserts them into the *Risk Log* (RL). The result is input to *System Safety Requirements* (SSK).

The *designer* uses the results of the *Functional Hazard Analysis* (FHA), on the one hand, to identify technical system safety requirements as part of the *System Requirements Hazard Analysis* (SRHA) and also as input to the in-depth system safety analyses.

Input, Output and Flowchart

The input to the *Functional Hazard Analysis* (FHA) activity for the *stakeholder* is the *System Safety Management Plan* (SSMP) and the system description and experience data from the *Failure Reporting System* (FRACAS).

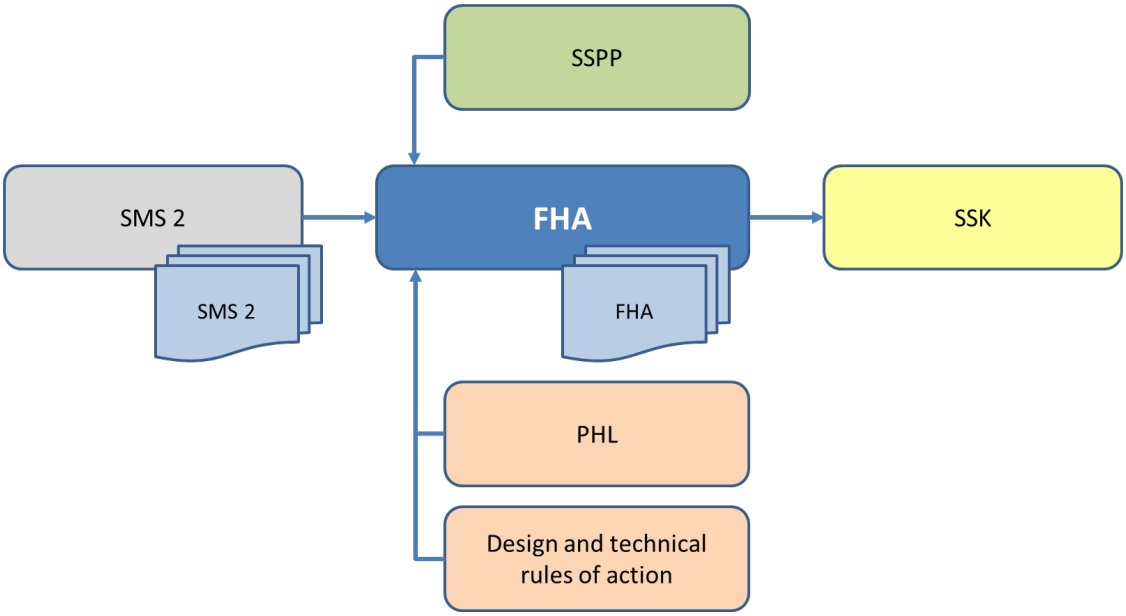
The output is *Functional Hazard Analysis* (FHA). It is input to the *System Safety Evaluation* (SSB) and *Risk Log* (RL).



Appendix 3, figure 17 *Functional Hazard Analysis (FHA) for stakeholders.*

The input to the *Functional Hazard Analysis* (FHA) activity for the *client* is the *System Objective* (SMS 2) and the user's *System Safety Program Plan* (SSPP) and *Preliminary Hazard List* (PHL), *Design Rules* (DR) and *Technical Rules of Practice* (THR).

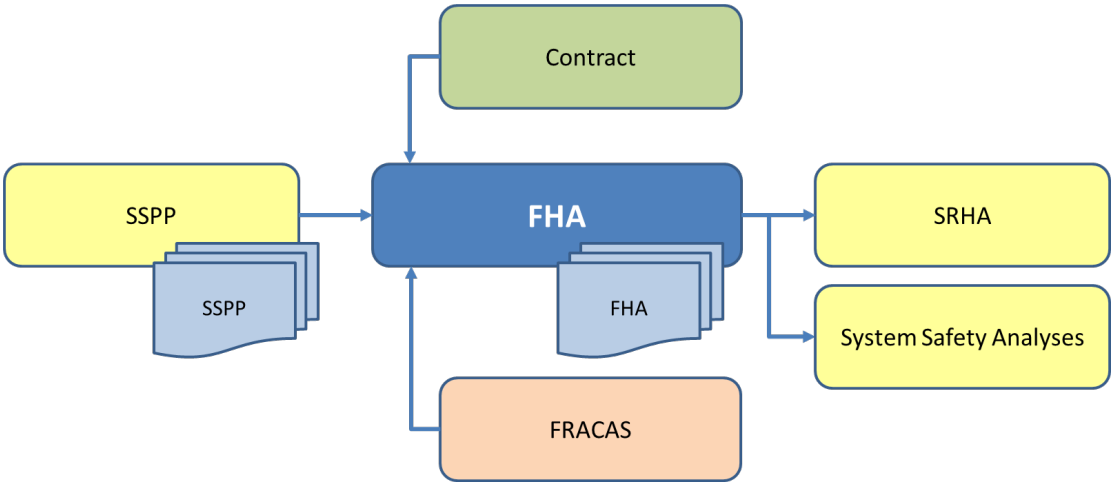
The output is *Functional Hazard Analysis* (FHA). This is input to *System Safety Requirements* (SSK).



Appendix 3, figure 18 *Functional Hazard Analysis (FHA) for clients.*

The input to the *Functional Hazard Analysis* (FHA) activity for the *designer* consists of the contractual *System Safety Program Plan* (SSPP) and the system description in contracts and experience data from the *Failure Reporting System* (FRACAS).

The output is *Functional Hazard Analysis* (FHA). It is input to the *System Requirements Hazard Analysis* (SRHA) and to other system safety analyses.



Appendix 3, figure 19 *Functional Hazard Analysis (FHA) for designers.*

A *Functional Hazard Analysis* (FHA) should include:

- An overall system description of the subsystems including possible software and its main interactions, for example in block diagrams
- A list of system functions and system safety-critical functions, respectively
- A description of which safety-critical features can be realised through software including suggestions for criticality level
- Input to *Risk Log* (RL) in the form of accident risk with impact evaluation
- A list of identified system safety requirements

TASK 201 - PRELIMINARY HAZARD LIST (PHL)

Purpose and Activity Description

The purpose of this activity is to identify sources of risk and/or hazardous situations, which may be physical or functional properties that exist in or are interconnected with the technical system or product.

The output/documentation from the activity is a *Preliminary Hazard List* (PHL).

The *Preliminary Hazard List* (PHL) can be used as input data on the one hand for the requirements definitions and also partly for the in-depth system safety analyses as well as for the *Hazard Tracking System* (HTS).

The *Preliminary Hazard List* (PHL) is a list of the sources of risk and/or hazardous situations currently in or interconnected with the technical system, which means that the contents of the list may need to be updated until the configuration is fixed.

The stakeholder identifies dimensional sources of risk and/or hazardous situations that can be countered by defining system safety requirements in the *System Objective* (SMS 2). This basically means that some design solutions are not allowed, while others are allowed.

The *client* identifies possible sources of risk and/or hazardous situations that can be countered by defining system safety requirements in the *Request for Proposal* (RFP). This basically

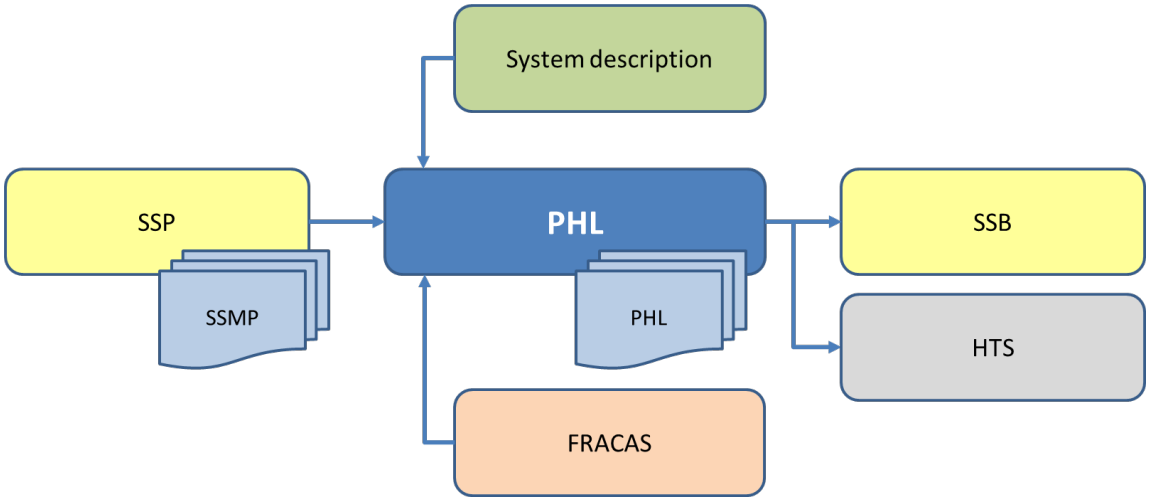
means imposing requirements for certain principled design solutions. For example, there should be (at least) two safety features independent of each other or protective devices.

The *designer* identifies all sources of risk and/or hazardous situations that exist in or are connected with the technical system or product. The result is used partly in the *System Requirements Hazard Analysis* (SRHA) and partly as input to the in-depth system safety analyses.

Input, Output and Flowchart

The input to the *Preliminary Hazard List* (PHL) activity for the *stakeholder* is the *System Safety Management Plan* (SSMP), the system description and experience data from the *Failure Reporting System* (FRACAS).

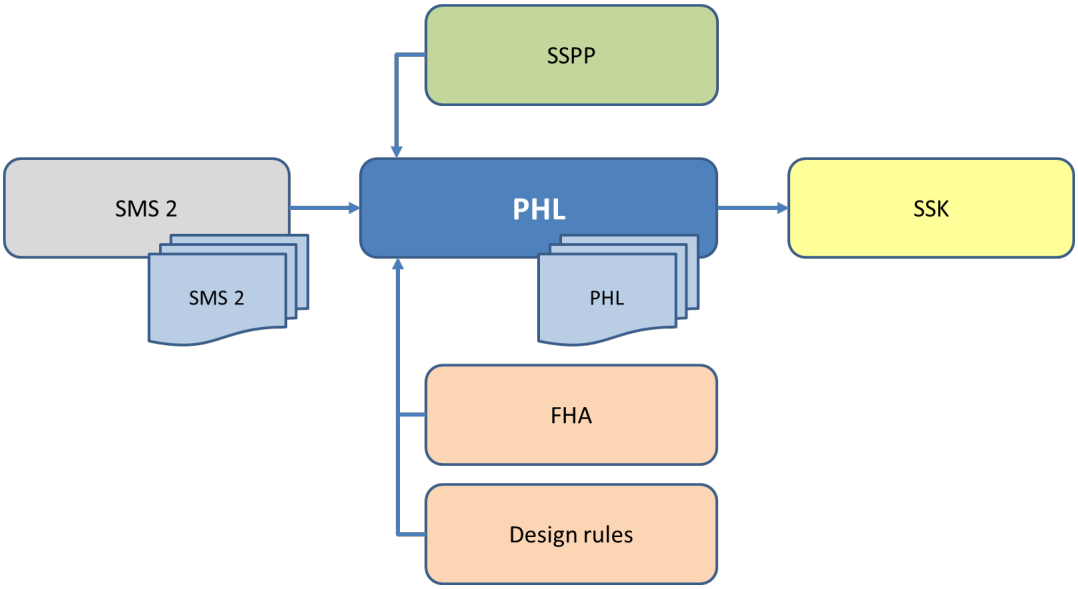
The output is the *Preliminary Hazard List* (PHL). It is input to the *System Safety Evaluation* (SSB) and the *Hazard Tracking System* (HTS).



Appendix 3, figure 20 *Preliminary Hazard List (PHL) for stakeholders.*

The input to the *Preliminary Hazard List* (PHL) activity for the *client* is the *System Objective* (SMS 2), the *client's System Safety Program Plan* (SSPP), the *Functional Hazard Analysis* (FHA) and experience data from the *Failure Reporting System* (FRACAS).

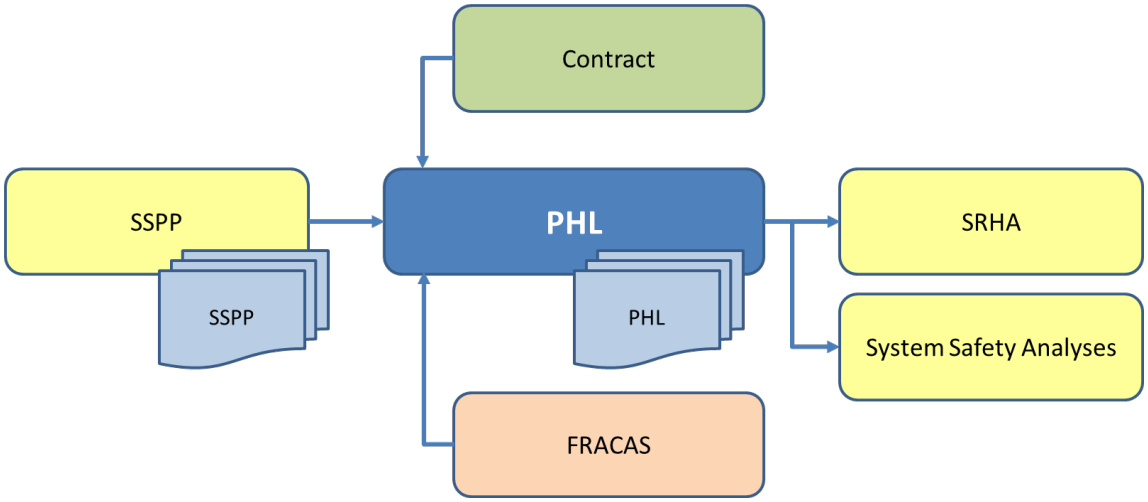
The output is the *Preliminary Hazard List* (PHL). This is input to *System Safety Requirements* (SSK).



Appendix 3, figure 21 *Preliminary Hazard List (PHL) for clients.*

The input to the *Preliminary Hazard List* (PHL) activity for the *designer* consists of the contractual *System Safety Program Plan* (SSPP), contracts and experience data from *Failure Reporting System* (FRACAS).

The output is the *Preliminary Hazard List* (PHL). It is input to the *System Requirements Hazard Analysis* (SRHA) and to other system safety analyses.



Appendix 3, figure 22 *Preliminary Hazard List (PHL) for designers.*

A *Preliminary Hazard List* (PHL) may contain a variety of information depending on the actor's purpose for the list.

A *Preliminary Hazard List* (PHL) should include:

- Reference to a description of the concept or technical system
- A list of components with its sources of risk and/or hazardous situations, as well as where necessary:
    - Hazardous events and/or accident risks with estimated consequences if the accident occurs
    - Easy prioritisation between the sources of risk and the hazardous situations before the in-depth system safety analyses

TASK 202 - PRELIMINARY HAZARD ANALYSIS (PHA)

Purpose and Activity Description

The purpose of this activity is to identify hazardous events and accident risks, related to design or function, that exist in or are interconnected with the technical system or product, based on the identified sources of risk in: *Preliminary Hazard List* (PHL). The activity also includes an initial analysis and assessment of the identified accident risks and provides an opportunity to propose possible risk-reducing measures.

The output/documentation from the activity is a *Preliminary Hazard Analysis* (PHA).

The *Preliminary Hazard Analysis* (PHA) continues where the *Preliminary Hazard List* (PHL) ended.

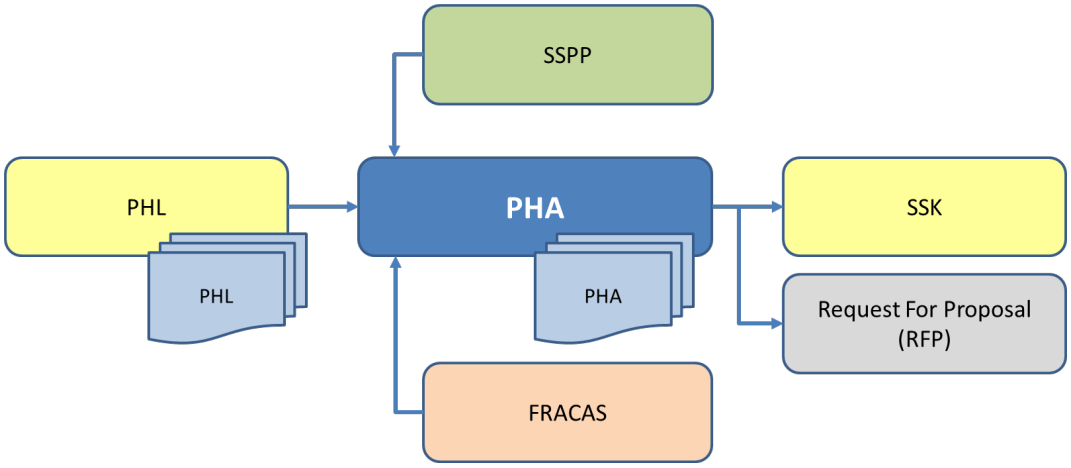
The *Preliminary Hazard Analysis* (PHA) is an initial analysis and evaluation of accident risks where the detail occurs in the in-depth system safety analyses. The *Preliminary Hazard Analysis* (PHA) needs to analyse use, maintenance, storage (transport) and decommissioning. Furthermore, border areas and interaction with other technical systems and products need to be taken into account. The result can also be used in formulating system safety requirements.

The *Preliminary Hazard Analysis* (PHA) can also be used to identify and designate subsystems and components from a point of view of criticality. The designated subsystems or components are further investigated in the *Safety-Critical Functions* (SCF) activity.

Input, Output and Flowchart

The input to the *Preliminary Hazard Analysis* (PHA) activity for the *client* consists of *Preliminary Hazard List* (PHL), the *client's System Safety Program Plan* (SSPP) and experience data from the *Failure Reporting System* (FRACAS) .

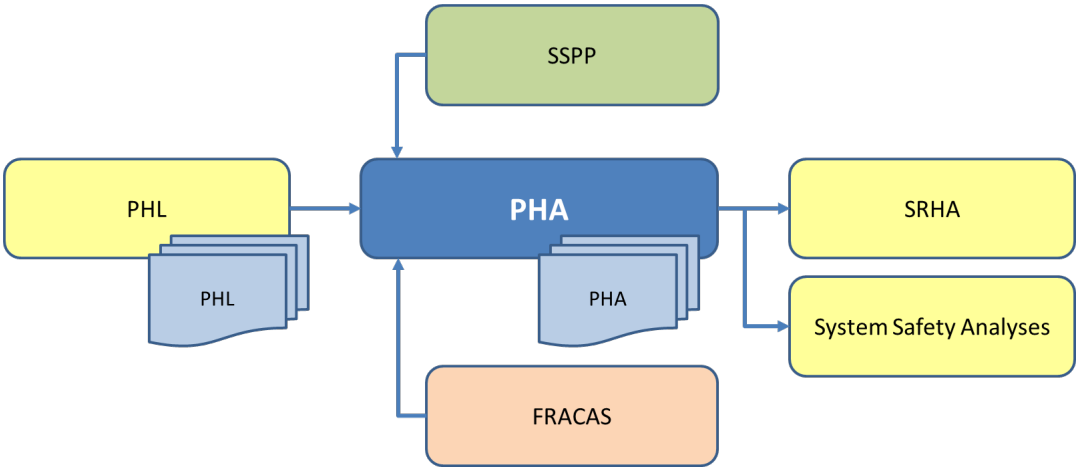
The output is the *Preliminary Hazard Analysis* (PHA). It is input to *System Safety Requirements* (SSK) and *Request for Proposal* (RFP).



Appendix 3, figure 23 *Preliminary Hazard Analysis (PHA) for the client.*

The input to the *Preliminary Hazard Analysis* (PHA) for the *designer* consists of the *Preliminary Hazard List* (PHL), the contractual *System Safety Program Plan* (SSPP) and experience data from the *Failure Reporting System* (FRACAS).

The output is the *Preliminary Hazard Analysis* (PHA). It forms the input to the *System Requirements Hazard Analysis* (SRHA) and other in-depth system safety analyses.



Appendix 3, figure 24 *Preliminary Hazard Analysis (PHA) for the designer.*

A *Preliminary Hazard Analysis* (PHA) is based on the *Preliminary Hazard List* (PHL) and can also be supplemented with descriptive text for the respective accident risk.

A *Preliminary Hazard Analysis* (PHA) should include:

- Reference to a description of the concept or technical system
- Identified hazardous events and accident risks and a first initial assessment of probabilities and severity classes, including health and environmental impacts
- A list of identified safety-critical subsystems and components
- Proposal for risk-reducing measures to counter identified hazardous events and accident risks
- A description of the respective accident risk

S21 - SAFETY-CRITICAL FUNCTIONS (SCF)

Purpose and Activity Description

The purpose of this activity is to identify system safety functions, subsystems or components contained in or interconnected with the technical system or product. The result of the activity shows the characteristics of subsystems or components that during development and manufacture require special measures or quality controls. The equivalent also applies to software that is part of the technical system.

The output/documentation of this activity is *Safety Critical Functions* (SCF).

In control documentation for the development and manufacture of technical systems or products, the *designer* needs to create, document and maintain descriptions of development and manufacturing processes, as well as work instructions for the production operations required for the properties that can be designated as critical from a system safety point of view. Specifying criticality rating in development and product descriptive documents creates prerequisites for using custom methodology, control resources in development and manufacturing, and implementing special quality controls alternatively verification of software.

Safety critical and safety-related subsystems and components may have specific characteristics such as specific features, dimensions, certain tolerances, hardness or surface fineness. In cases where flaws are found in such characteristics, hazardous events or accidents may occur. This applies, for example, if components are missing in an installation.

For subsystems containing software, criticality level requirements are specified in cases where deficiencies are deemed to cause hazardous events or accidents.

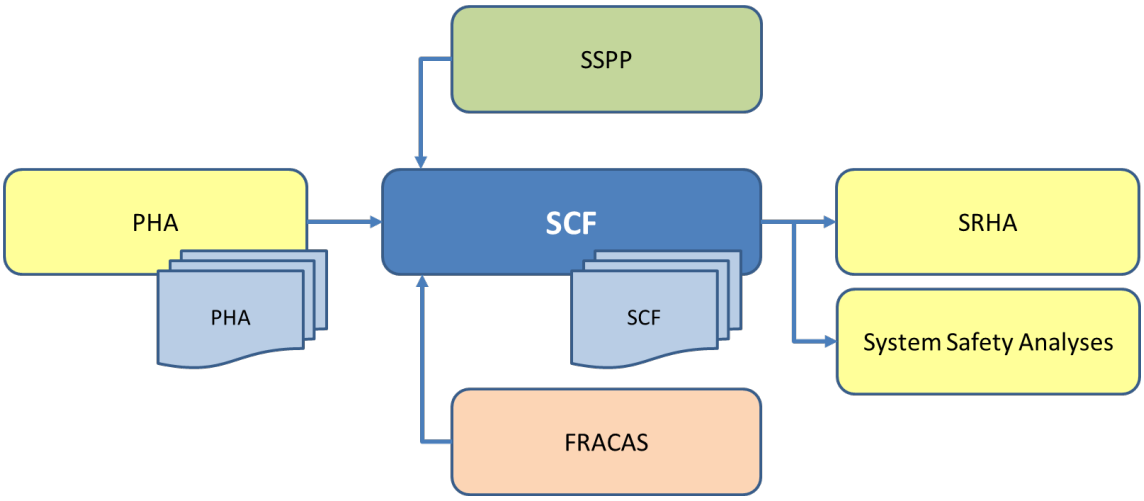
The safety-critical subsystems/components with its characteristics are those that directly affect the system safety of the technical system, for example, allow single failures. The safety-related subsystems/components with their characteristics are those that indirectly affect the system safety of the technical system, for example where double faults or higher order failures are required.

If in subsystems or components there are deficiencies in its properties and if these characteristics are deemed to have a significant impact on the hazardous event, the components need to be marked in drawings or in other design definitions. For hardware or machine-oriented components, the *Critical Item List* (CIL) are designated, for example, according to SS 2222 *Technical documentation - Classification of requirements in the production base*. For software with associated electronics, the criticality classification can be performed according to the methodology in the Handbook on Software in Safety-Critical Applications (H ProgSäk E).

Input, Output and Flowchart

The input to the *Safety Critical Functions* (SCF) activity consists of *Functional Hazard Analysis* (FHA), *Preliminary Hazard Analysis* (PHA) and the contractual *System Safety Program Plan* (SSPP) as well as experience data from the *Failure Reporting System* (FRACAS) .

The output is *Safety Critical Functions* (SCF), which can be a list of *Critical Item List* (CIL) and a list of criticality or reliability levels (*Safety Integrity Levels* - (SIL)), which is used for further requirement definition.



Appendix 3, figure 25 *Safety-Critical Functions (SCF).*

Safety-Critical Functions (SCF) should include:

- References to applied standards for Criticality Classification used for:
  - Hardware
  - Software

TASK 203 - SYSTEM REQUIREMENTS HAZARD ANALYSIS (SRHA)

Purpose and Activity Description

The purpose of this activity is for the *designer* to identify the system safety requirements applicable to the technical system based on EU law, Swedish legislation, standards, the *client's* requirements in the contract and intra-company system safety requirements.

The output/documentation from the activity is *System Requirements Hazard Analysis Report* (SRHAR).

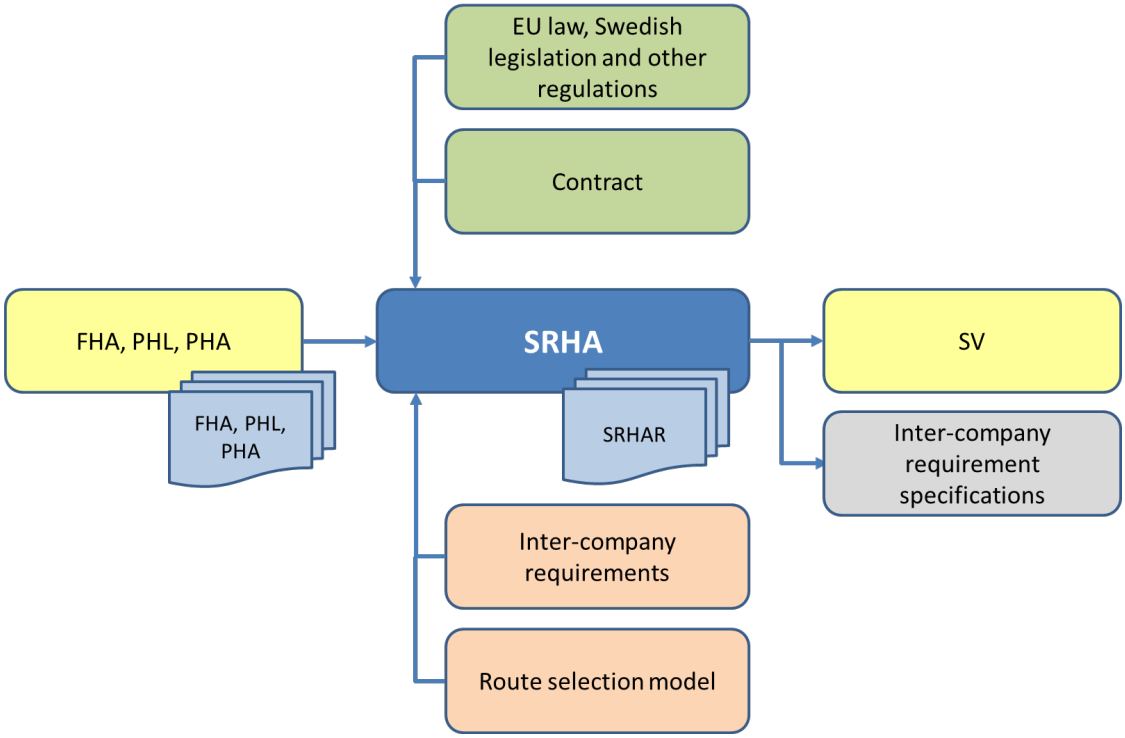
The *designer* prepares system safety requirements to identify risk-reducing measures to counter the accident risks identified in *Functional Hazard Analysis* (FHA), *Preliminary Hazard List* (PHL), and *Preliminary Hazard Analysis* (PHA).

Identified system safety requirements in the *System Requirements Hazard Analysis Report* (SRHAR) consist partly of technical requirements that affect the design, and partly of requirements on system safety work to demonstrate that the technical system offers a satisfactory level of safety. All requirements are transferred and distributed to the *designer's* various requirement specifications. Each requirement needs to be verifiable to later be taken care of in the *Safety Verification* (SV). To support this activity, the *Route Selection Model* (VVM) is applied.

Input, Output and Flowchart

The input to the *System Requirements Hazard Analysis* (SRHA) activity consists of the *Functional Hazard Analysis* (FHA), *Preliminary Hazard List* (PHL) and *Preliminary Hazard Analysis* (PHA) in addition to legislation and contract. Supplier internal requirements for design or development work are also taken into account.

The output is the *System Requirements Hazard Analysis Report* (SRHAR). This forms the input to the *Safety Verification* (SV) and to the *designer's* internal requirements specifications.



Appendix 3, figure 26 *System Requirements Hazard Analysis (SRHA).*

A *System Requirements Hazard Analysis Report* (SRHAR) should include:

- The technical system referred to
- Requirement number (consecutive numbering)
- Source citation (title/document)
    - EU law, Swedish legislation, standards, technical specifications, handbooks (design rules collections) and system safety analyses
- Requirement text (e.g. technical specification requirements and handbooks (design rule collections))
- Any exemption from legislation concerning military material
- Verification criterion
- Marking that the requirement is met

TASK 204 - SUBSYSTEM HAZARD ANALYSIS (SSHA)

Purpose and Activity Description

The purpose of this activity is to primarily influence the design and functionality of subsystems and components that are part of a technical system to achieve a satisfactory level of safety during use. To support this activity, the *Route Selection Model* (VVM) is applied.

The output/documentation from the activity is a *Subsystem Hazard Analysis Report* (SSHAR).

The result of a *Subsystem Hazard Analysis* (SSHA) focuses mainly on design and function, with any associated software, so that a satisfactory level of safety is offered during use, maintenance, storage (transportation) and disposal.

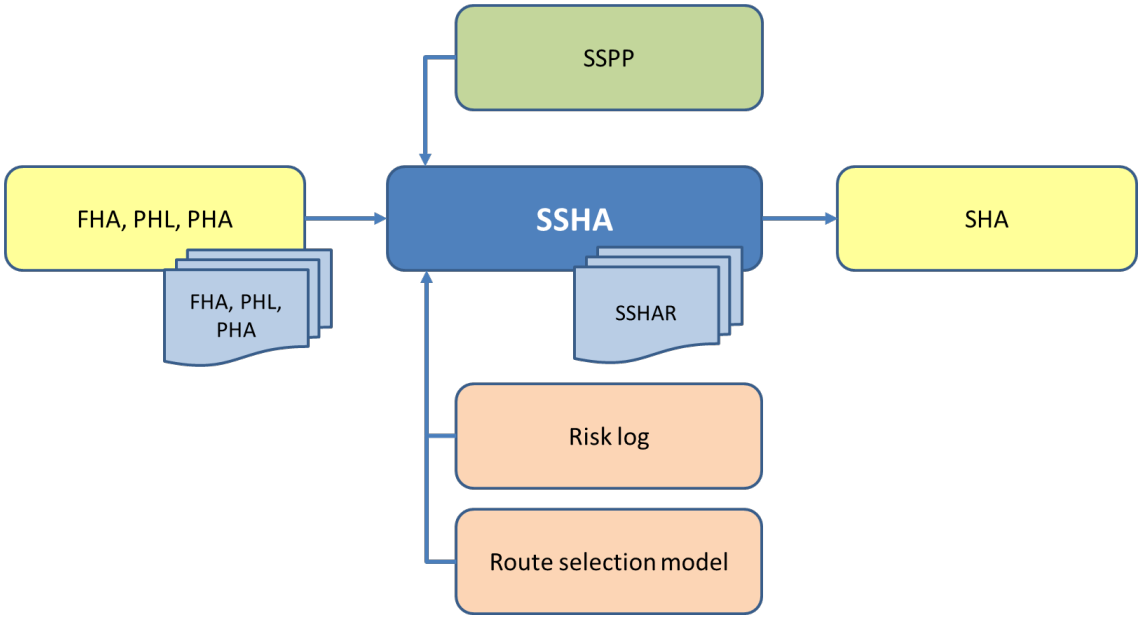
For the accident risks identified in *Functional Hazard Analysis* (FHA), *Preliminary Hazard List* (PHL) and *Preliminary Hazard Analysis* (PHA), and possibly additional accident risks under the *Subsystems Hazard Analysis* (SSHA), these must be analysed, assessed and classified and, if necessary, risk-reducing measures must be introduced. To support this activity, a *Risk Log* (RL) is used.

In the *Risk Log* (RL), both accident risks, the subsystem and system safety-critical components can be listed. By applying the *Route Selection Model* (VVM), accident risks, the sub-system and the system-safety-critical components can be managed through different route selections. See *Chapter 11*. Only those accident risks that have not been managed in Route Selections (VV1 – VV6) must be managed in Route Selection (VV7) and assessed against the *Tolerable Risk Level* (TR) expressed in the risk matrix.

Input, Output and Flowchart

Inputs to the activity *Subsystems Hazard Analysis* (SSHA) are *Functional Hazard Analysis* (FHA), *Preliminary Hazard List* (PHL) and *Preliminary Hazard Analysis* (PHA) as well as the contracted *System Safety Program Plan* (SSPP).

The output is the *Subsystem Hazard Analysis Report* (SSHAR). This forms the input to the *System Hazard Analysis* (SHA).



Appendix 3, figure 27 *Subsystem Hazard Analysis (SSHA).*

A *Subsystem Hazard Analysis Report* (SSHAR) should include:

- An overall system description and detailed physical and functional description of the subsystems
- What system level requirements have been broken down to the respective subsystems
- Description of the risk analysis methods used
- The data and prerequisites used and the assumptions made
- Summary of results
    - Fulfilment of requirements
    - Recommendation on risk-reducing measures
    - Proposal for future system safety testing
- Detailed accounting on the basis of the summary
- Data transferred to *Risk Log* (RL)

TASK 205 - SYSTEM HAZARD ANALYSIS (SHA)

Purpose and Activity Description

The purpose of this activity is to primarily influence the design and functionality of technical systems and products in order to achieve a satisfactory level of safety during use. Technical systems and products can, in turn, be included in a system-of-systems. To support this activity, the *Route Selection Model* (VVM) is applied.

The output/documentation of this activity is *System Hazard Analysis Report* (SHAR).

The result of a *System Hazard Analysis* (SHA) focuses mainly on design and function, with any associated software, so that a satisfactory level of safety is offered during use, maintenance, storage (transportation) and disposal. Different systems and products may have been approved or met requirements against different regulatory frameworks or standards. This needs to be taken into account in the system safety work of the technical system.

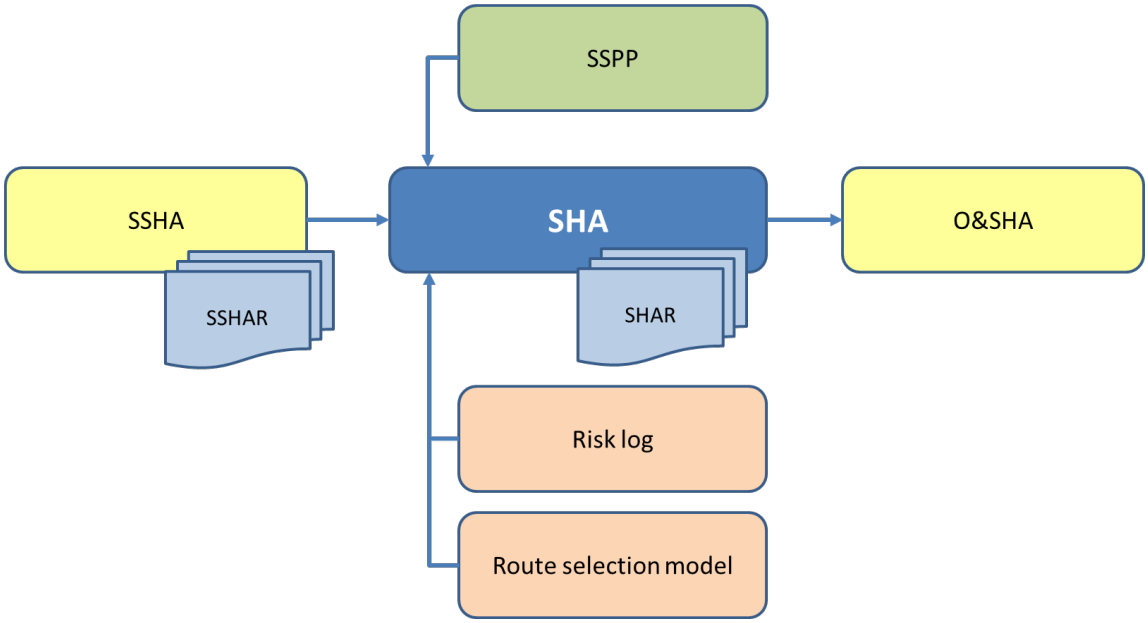
For those accident risks identified in the *Functional Hazard Analysis* (FHA), the *Preliminary Hazard List* (PHL), the *Preliminary Hazard Analysis* (PHA) and the *Subsystem Hazard Analysis* (SSHA), and also additional accident risks under the *System Hazard Analysis* (SHA), these must be analysed, evaluated and classified, and if necessary, risk-reducing measures be introduced. To support this activity, a *Risk Log* (RL) is used.

In the *Risk Log* (RL), both accident risks, the technical system, subsystems and system safety-critical components can be listed. Through applying the *Route Selection Model* (VVM) accident risks, the technical system, the subsystem(s) and system safety critical components can be managed through various route selections. See *Chapter 11*. Only those accident risks that have not been managed in Route Selections (VV1 – VV6) must be managed in Route Selection (VV7) and assessed against the *Tolerable Risk Level* (TR) expressed in the risk matrix.

Input, Output and Flowchart

The input to the *System Hazard Analysis* (SHA) activity consists of *Subsystem Risk Analysis* (SSHA) and the contracted *System Safety Program Plan* (SSPP).

The Output is the *System Hazard Analysis Report* (SHAR). It is input to *Operating & Support Hazard Analysis* (O&SHA).



Appendix 3, figure 28 *System Hazard Analysis (SHA).*

A *System Hazard Analysis Report* (SHAR) should include:

- An overall system description and detailed physical and functional description of the subsystems
- What requirements exist for the system level concerned
- Description of the risk analysis methods used
- The data and prerequisites used and the assumptions made
- Summary of results
    - Fulfilment of requirements
    - Recommendations for risk-reducing measures
    - Proposal for future system safety testing
- Detailed account of the basis of the summary
- Data transferred to *Risk Log* (RL)

TASK 206 - OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA)

Purpose and Activity Description

The purpose of this activity is primarily to influence the handling of technical systems and products with a set configuration in order to achieve a satisfactory level of safety.

The output/documentation is *Operating and Support Hazard Analysis Report* (O&SHAR).

The result *of Operating and Support Hazard Analysis* (O&SHA) focuses mainly on the handling of technical systems and products so that a satisfactory level of safety is offered during use, maintenance and storage (transportation). Thus, scenarios describing different use cases and modes of use need to be defined as well as if other materials or chemical products need to be used, such as a particular tool or cleaning agent during maintenance.

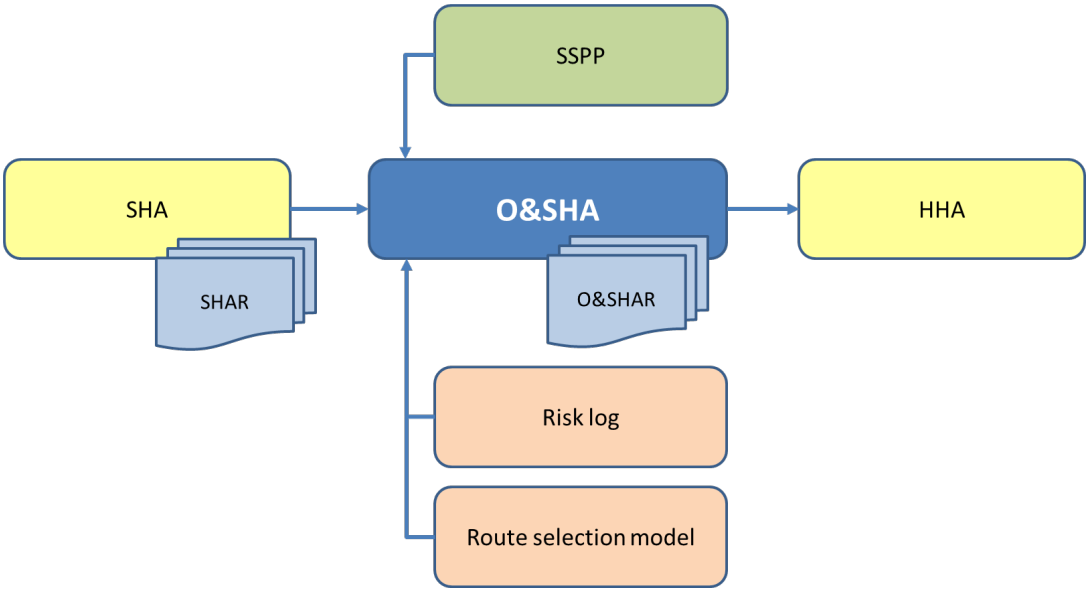
For those accident risks identified in *System Hazard Analysis* (SHA) and, on the other hand, any additional accident risks under *Operating and Support Hazard Analysis* (O&SHA), these must be analysed, assessed and be classified and, where necessary, operating rules must be amended or restrictions imposed. For certain accident risks, proposals may be made for changes (modifications) of the technical system. To support this activity, a *Risk Log* (RL) is used.

In the *Risk Log* (RL), both accident risks and occupational health risks can be listed. By applying the *Route Selection Model (VVM)*, both accident risks and occupational hazards can be addressed through different route selection choices. See *Chapter 11*. Only those accident risks that have not been managed in Route Selections (VV1 – VV6) must be managed in Route Selection (VV7) and assessed against the *Tolerable Risk Level* (TR) expressed in the risk matrix.

Input, Output and Flowchart

The input to the *Operating and Support Hazard Analysis* (O&SHA) activity consists of *Subsystem Hazard Analysis* (SSHA) and the contracted *System Safety Program Plan* (SSPP).

Output is *Operating and Support Hazard Analysis* (O&SHA). This provides input to the *Health Hazard Analysis* (HHA).



Appendix 3, figure 29 *Operating and Support Hazard Analysis (O&SHA).*

An *Operating and Support Hazard Analysis Report* (O&SHAR) should include:

- A detailed physical and functional system description and an overall description of the subsystems
- A description of the usage scenarios
- What requirements exist for the system level concerned
- Description of the risk analysis methods used
- The data and prerequisites used and assumptions made
- Summary of results
    - Fulfilment of requirements
    - Recommendations for risk-reducing measures
    - Proposal for future training
- Detailed account of the basis of the summary
    - Description of proposals for amendments to the technical system or subsystems
    - Recommendations on instructions, warning labels, emergency equipment and Personal Protective Equipment (PPE)
    - Recommendations for transport and storage rules
- Data transferred to *Risk Log* (RL)

TASK 209 - SYSTEM-OF-SYSTEMS HAZARD ANALYSIS (SoSHA)

Purpose and Activity Description

The purpose of this activity is to ensure the co-operation of two or more technical systems and products, with the intention of enabling new capabilities or functions, so that a satisfactory level of safety is achieved during use. For included technical systems and products, system safety decisions are issued. The activity is mostly carried out by the *system integrator*.

The output/documentation from this activity is *System-of-Systems Hazard Analysis Report* (SoSHAR).

The result of *System-of-Systems Hazard Analysis* (SoSHA) focuses mainly on achieving safe interoperability between different technical systems and products, without changing the established configurations. If necessary, various interconnection connectors or interface adapters may be allowed. This so that a satisfactory level of safety is offered during use. In cases where technical systems or products need to be modified, this is done by a *designer*.

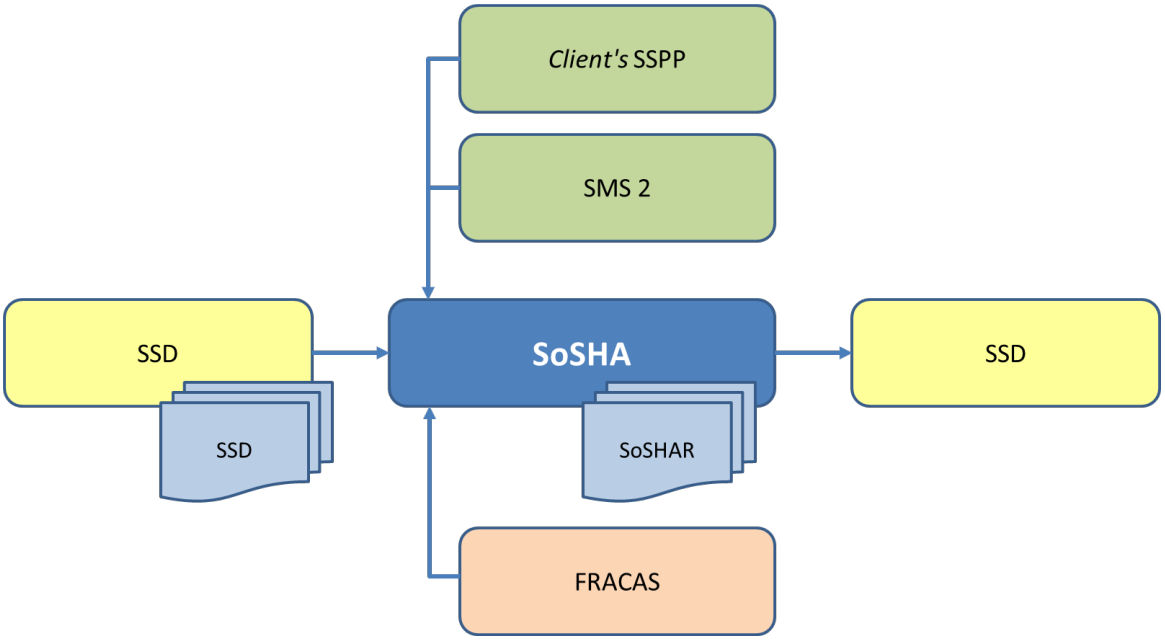
For the accident risks identified for system-of-systems, these must be analysed, assessed and classified and, where necessary, risk-reducing measures must be introduced. To support this activity, *Functional Hazard Analyses* (FHAs), *Preliminary Hazard Lists* (PHLs), in-depth system safety analyses, and *Risk Log* (RL) are used.

System-of-Systems Hazard Analyses (SoSHA) also need to investigate if other accident risks regarding the included technical systems or products are affected and thus need to be re-evaluated, which may also lead to new system safety decisions needing to be issued.

Input, Output and Flowchart

The input to the *System-of-Systems Hazard Analysis* (SoSHA) activity consists of *System Safety Declarations* (SSD), *System Objective* (SMS 2) and the *client´s System Safety Program Plan* (SSPP) as well as experience from the *Failure Reporting System* (FRACAS).

The output is the *System-of-Systems Hazard Analysis Report* (SoSHAR). This provides input to the *System Safety Declaration* (SSD) for system-of-systems.



Appendix 3, figure 30 *System-of-Systems Hazard Analysis (SoSHA).*

A *System-of-Systems Hazard Analysis Report* (SoSHA) should include:

- A description of the new capabilities or functions that are created in the interaction between technical systems and products
- A detailed physical and functional system description of system-of-systems or function chains and overall descriptions of the included systems
- Which interconnection connectors or interface adapters are required for the collaboration function
- What are the requirements for the system- of-systems or the function chain
- A description of the risk analysis methods used
- The data and prerequisites used and assumptions made
- Unique accident risks identified for system-of-systems or functional chains
- Summary of results
    - Fulfilment of requirements
    - Recommendations for risk-reducing measures
    - Proposal for future system safety testing
- Detailed account of the basis of the summary
- Data transferred to *Risk Log* (RL)

TASK 207 - HEALTH HAZARD ANALYSIS (HHA)

Purpose and Activity Description

The purpose of this activity is to identify health-related accident and occupational hazards with technical systems and products by evaluating, among other things, noise, emissions and hazardous substances that produce any degree of immediate injury or ill health. This activity should be coordinated with the *Environmental Hazard Analysis* (EHA).

The output/documentation from this activity is *Health Hazard Analysis Report* (HHAR).

The result of the *Health Hazard Analysis* (HHA) also provides information to the person who has employer and delegated occupational health and safety responsibilities in the organisation where the technical system is to be used. Long-term health impacts, for example where accumulated doses over time produces harm, as well as psychosocial aspects are addressed in systematic occupational health and safety work.

Examination and evaluation should be carried out in compliance with EU law, Swedish legislation and the regulations of various authorities, for example published by the Swedish Labour Environment Authority, the Agency for Chemicals or the Swedish Radiation Safety Authority.

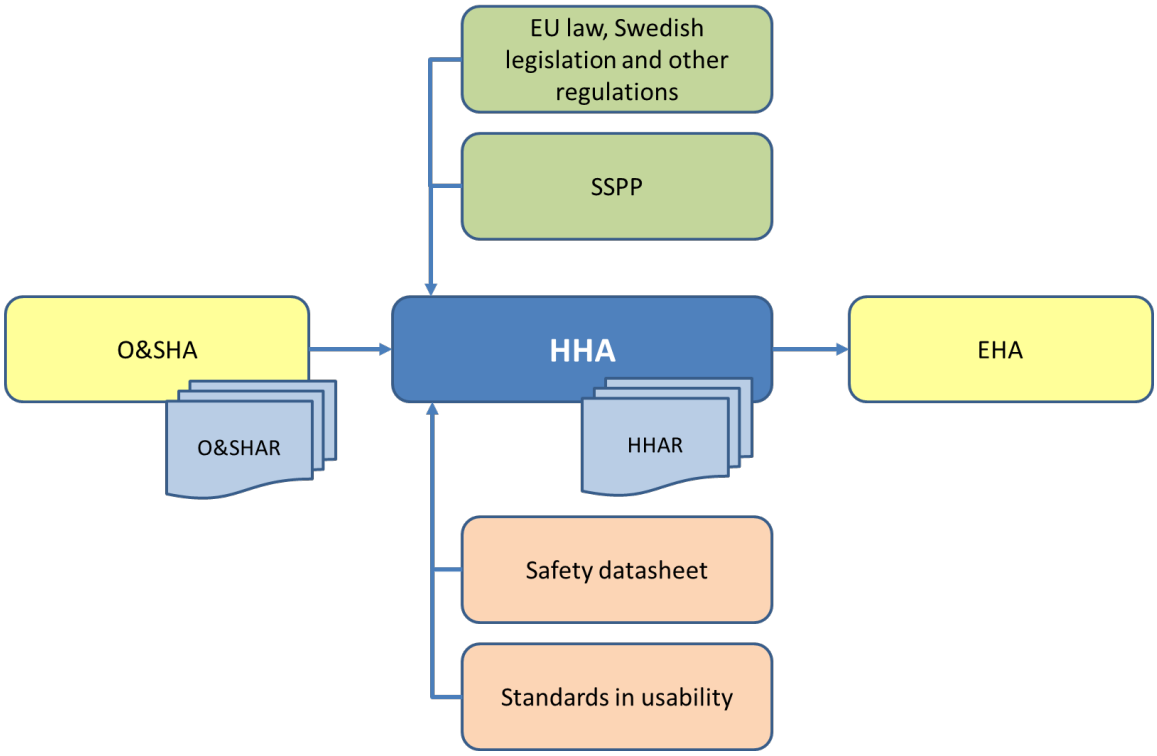
The *Health Hazard Analysis* (HHA) identifies hazardous conditions and situations for which users may be exposed to noise, emissions, hazardous substances and chemical products during all use situations of the technical system. The analysis also includes analysing biological risks such as micro- and microbial organisms, ergonomic risks such as heavy lifting and incorrect working positions, and risks of ionised and non-ionised radiation such as radioactive substances and radar radiation. In addition, hazardous substances that can form in abnormal environments, for example during fire, are analysed.

In the *Health Hazard Analysis Report* (HHAR), risk-reducing measures may be proposed, on the one hand, on the technical system for the design or selection of chemical products, on the other hand for the provision of Personal Protective Equipment (PPE) and for the activities expected to be carried out. Furthermore, the possibility of care for exposed persons may be taken into account, for example during an operation.

Input, Output and Flowchart

The input to the *Health Hazard Analysis* (HHA) activity consists of *Operating and Support Hazard Analysis* (O&SHA), legislation, the contractual *System Safety Program Plan* (SSPP), and Safety Data Sheets as well as standards in the field of usability.

The Output is the *Health Hazard Analysis Report* (HHAR). It provides input to the *Environmental Hazard Analysis* (EHA).



Appendix 3, figure 31 Health Hazard Analysis (HHA).

A *Health Hazard Analysis Report* (HHAR) should include:

- The technical system referred to
- The possibilities, requirements and limitations that legislation provides
- What other restrictions have been taken into account, such as contract requirements
- The data and prerequisites used and assumptions made
- Summary of results
    - Fulfilment of requirements
    - Recommendations for risk-reducing measures
    - Proposals for in-depth usability analyses
- Detailed account of the basis of the summary
- Data transferred to *Risk Log* (RL)

TASK 210 - ENVIRONMENTAL HAZARD ANALYSIS (EHA)

This activity is replaced by S22 - Environmental Hazard Analysis (EHA).

S22 - ENVIRONMENTAL HAZARD ANALYSIS (EHA)

Purpose and Activity Description

The purpose of this activity is to identify environmental accidents and other environmental impacts with technical systems and products by evaluating, among other things, noise, emissions and hazardous substances that produce any degree of immediate damage or environmental impact on both flora and fauna. This activity should be coordinated with the *Environmental Hazard Analysis* (EHA).

The output/documentation from this activity is *Environmental Hazard Analysis Report* (EHAR).

The result of the *Environmental Hazard Analysis* (EHA) also provides information to the person who has employer and delegated occupational health and safety responsibilities in the organisation where the technical system is to be used. Long-term environmental impacts, such as where emissions over time contribute to global warming, or environmental impacts relating to a specific geographical location are addressed in the sustainability work of the Swedish Armed Forces.

Examination and evaluation should be carried out in compliance with EU law, Swedish legislation and regulations of various authorities, for example published by the Swedish Environmental Protection Agency or Chemicals Inspectorate.

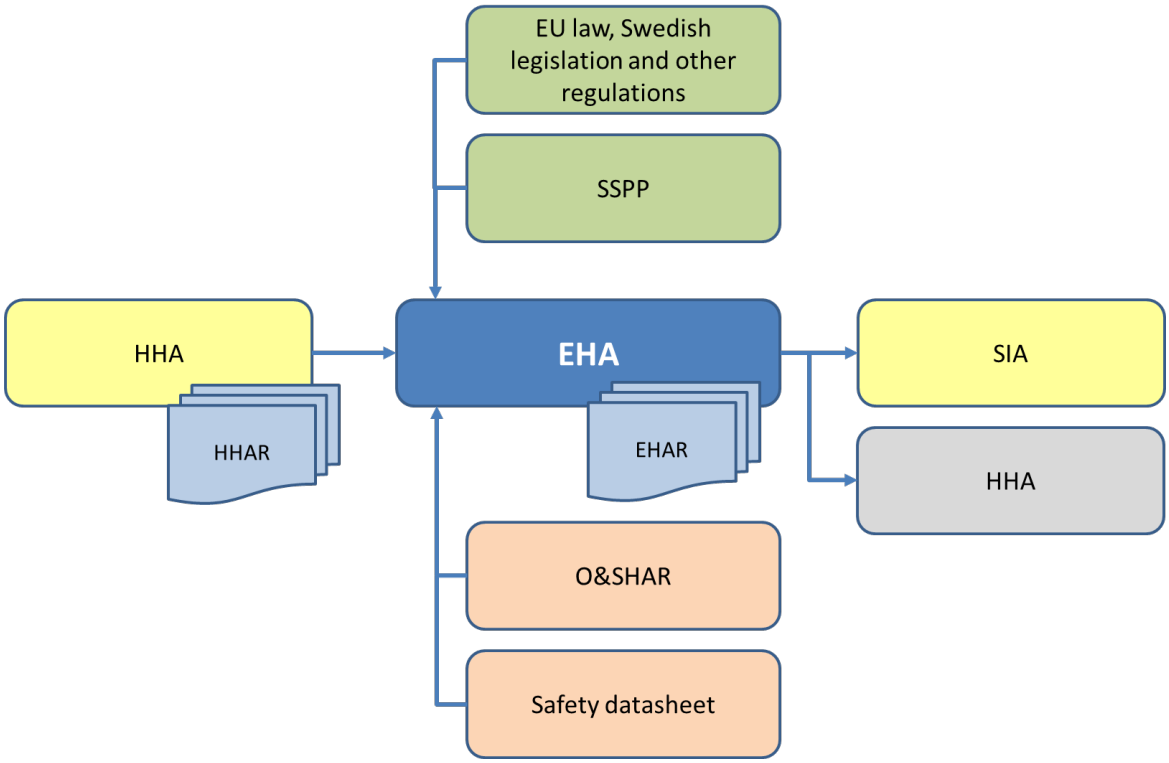
The *Health Hazard Analysis* (HHA) identifies hazardous conditions and situations for which flora and fauna may be exposed to noise, emissions, hazardous substances and chemical products during all use situations of the technical system. In addition, hazardous substances that can form in abnormal environments, for example during fire, are analysed.

In the *Health Hazard Analysis Report* (HHAR), risk-reducing measures may be proposed, on the one hand, for the technical system for the design or selection of chemical products, on the other hand for the provision of, for example, a canvas for collecting hazardous spills and thirdly, for the activities expected to be carried out. Furthermore, the possibility of decontamination of exposed flora may be taken into account, for example during missions.

Input, Output and Flowchart

The input to the *Environmental Hazard Analysis* (EHA) activity consists of *Health Hazard Analysis* (HHA), legislation and the contractual *System Safety Program Plan* (SSPP), as well as the *Operational and Support Hazard Analysis Report* (O&SHAR) and Safety Data Sheets.

Output is the *Environmental Hazard Analysis Report* (EHAR). It provides input to *Safety Instructions Analysis* (SIA) and *Health Hazard Analysis* (HHA).



Appendix 3, figure 32 *Environmentally Hazard Analysis (EHA).*

An *Environmental Hazard Analysis Report* (EHAR) should include:

- The technical system referred to
- The possibilities, requirements and limitations that legislation provides
- What other restrictions have been taken into account, such as contract requirements
- The data and prerequisites used and assumptions made
- Summary of results
    - Fulfilment of requirements
    - Recommendations for risk-reducing measures
    - Proposal for in-depth environmental analyses
- Detailed account of the basis of the summary
- Data transferred to *Risk Log* (RL)

S23 - SAFETY INSTRUCTIONS ANALYSIS (SIA)

Purpose and Activity Description

The purpose of the *Safety Instructions Analysis* (SIA) activity is to provide the safety instructions, warnings and warning labels needed for technical systems and products to provide a satisfactory level of safety in use, maintenance and storage (transport).

The output/documentation from this activity is *Safety Instructions* (SI).

The *designer* draws up *Safety Instructions* (SI) after risk-reducing measures such as design and protection measures are no longer possible. *Safety Instructions* (SI) affect, on the one hand, the safety instructions required for safe handling, the use restrictions and warnings that

need to be inserted in the operating instructions and maintenance instructions, also the warning labels to be affixed to technical systems and products.

Requirements for warning labels and their design are often regulated in various laws and regulations. Warning markings may be in the form of signs, stickers and other markings such as glow-in-the-dark emergency evacuation plates.

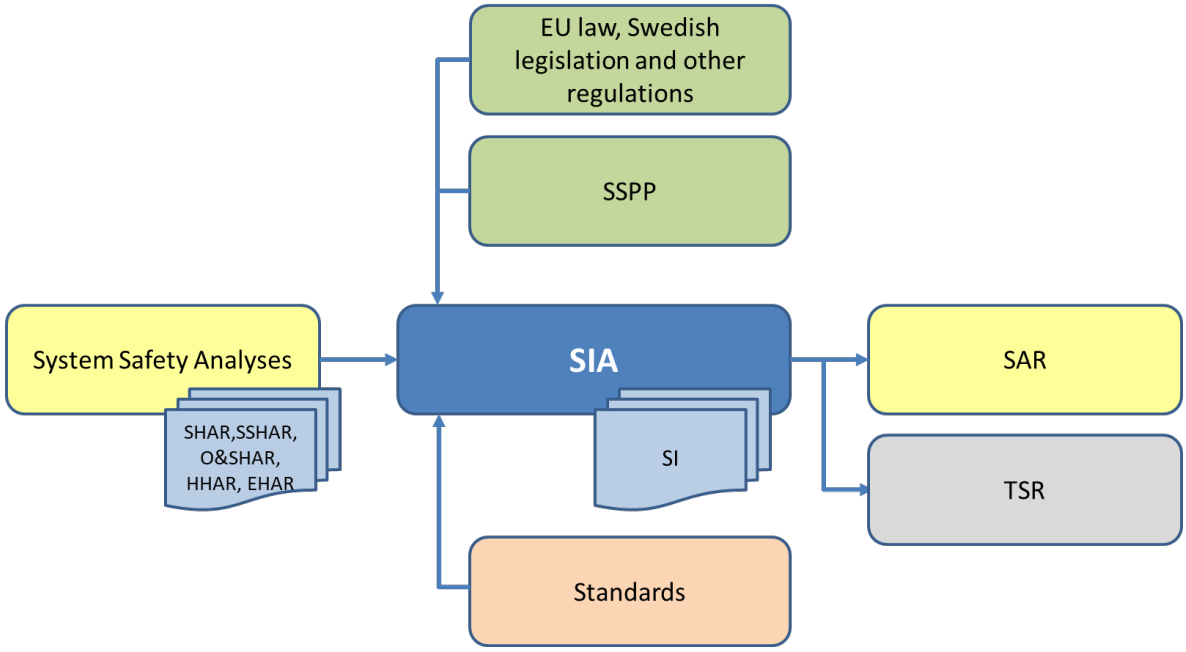
Instructions for use and maintenance instructions mainly contain descriptions of safe usage. In some cases, these descriptions need to be supplemented with warning texts. Warning texts should include:

- What is the danger and how to protect oneself, i.e. why should the instruction be followed?
- What can happen if an accident occurs?
- What will be the consequence if the accident occurs?

Input, Output and Flowchart

The input to the *Safety Instructions Analysis* (SIA) activity consists of the system safety analyses carried out, legislation and the contractual *System Safety Program Plan* (SSPP) as well as standards.

The output is *Safety Instructions* (SI). These provide input to the *Safety Assessment Report* (SAR) and *Training Safety Regulations* (TSR).



Appendix 3, figure 33 *Safety Instructions Analysis (SIA).*

The *Safety Instructions* (SI) should include:

- Usage restrictions
- Risk Areas and Restriction Areas
- Permissible ambient environment when used (temperature, humidity, electromagnetic fields, etc.)

- Permissible storage environment and co-storage restrictions (lifetime in unbroken and broken packaging, etc.)
- Permitted modes of transport (road, sea transport, air transport, rail transport)
- Permissible packaging requirements, stacking and inter-transport restrictions (transport securing equipment, accelerations, pressure and temperature changes, etc.)

S24 - RISK ASSESSMENT PRIOR TO DISPOSAL OF SYSTEMS (RADS)

Purpose and Activity Description

The purpose of this activity is to identify accident risks that may occur during the physical disposal of technical systems and products.

The output/documentation from this activity is *Risk Assessment Prior to Disposal of Systems Report* (RADSR).

The *Risk Assessment* (RADS) is carried out during the development of technical systems and products and also prior to actual disposal. Depending on the disposal method such as transfer, sale or destruction, the *Risk Assessment* (RADS) may have different focus. The *Risk Assessment* (RADS) includes accident risks that can harm both person and/or external environment.

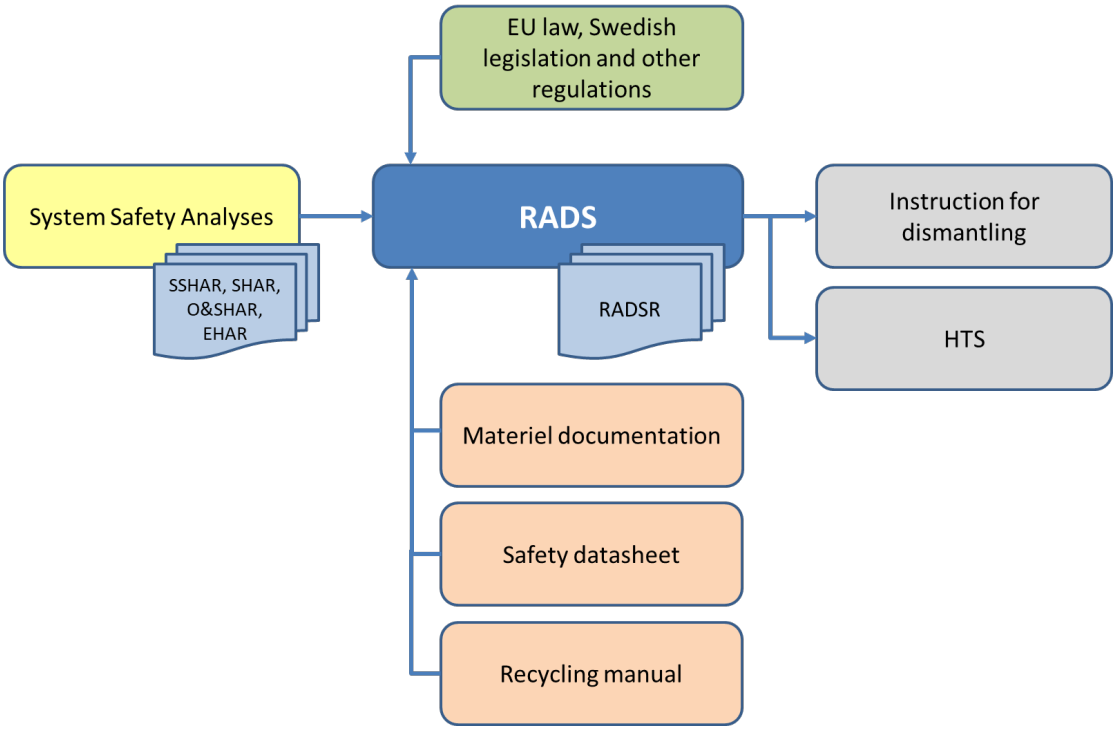
The *Risk Assessment Report* (RADSR) produced during the development phase focuses primarily on the design and on accident risks that may occur during the removal and disassembly of subsystems and products. This means, for example, that the choice of materials and chemical products, finishes and joints of different materials are taken into account from a destruction perspective. Furthermore, for accident risks which may be caused by stored energy, for example in the form of pressurised vessels, tensioned springs, reactive substances and energy in electrical components, safe methods for eliminating or reducing these accident risks of accident must be indicated.

The *Risk Assessment Report* (RADSR) updated or produced during the disposal stage analyses regulatory requirements including applicable manufacturer liability. For the removal of subsystems and components, the material documentation is based on corrective maintenance and identifies such elements that have not previously been analysed from a system safety perspective.

Input, Output and Flowchart

The input to the *Risk Assessment Prior to Disposal of Systems* (RADS) activity consists of the system safety analyses, legislation, materiel documentation focusing on corrective maintenance, Safety Data Sheets as well as recovery handbook.

The output is the *Risk Assessment Prior to Disposal of Systems Report* (RADSR). This provides input to an Instruction for Disposal and to the *Hazard Tracking System* (HTS).



Appendix 3, figure 34 *Risk Assessment prior to Disposal of Systems (RADS).*

A *Risk Assessment Prior to Disposal of Systems Report* (RADSR) should include:

- A physical system description with the included subsystems and other possible equipment such as spare equipment or tool kits
- The possibilities, requirements and limitations that legislation provides
- What other restrictions have been taken into account, such as end-user certificates
- Description of proposed modes of disposal such as transfer, sale, destruction and any museum or display items
- The data and prerequisites used and assumptions made
- Summary of results
    - Proposed modes of disposal of the technical system
    - Fulfilment of requirements
    - Recommendations for risk-reducing measures
    - Proposal for in-depth system safety analyses, for example for transfer, sale or for any museum or display items
- Detailed account of the basis of the summary
- Data transferred to *Risk Log* (RL)

Activities - SECTION 300 - Evaluation

TASK 301 - SAFETY ASSESSMENT REPORT (SAR)

Purpose and Activity Description

The purpose of this activity is to summarise the completed System Safety Work and report its conclusions, provide information on compliance with legislation and contracts, and provide a detailed description of the respective accident risk with any additional information. If the *Safety Assessment Report* (SAR) is supplemented with expanded information on the included materials, it also complies with Task 302, *Hazard Management Assessment Report* (HMAR).

The output/documentation from this activity is *Safety Assessment Report* (SAR).

The *Safety Assessment Report* (SAR) can either contain all the information, alternatively constitute a summary with references to underlying system safety analysis reports or other risk documentation. For technical systems and products approved, for example, by Route Selections (VV1 and/or VV3), the corresponding information may be presented directly in the System Safety Decision.

The *Stakeholder's* summary of system safety work and requirements fulfilled in compliance with legislation, the *System Safety Management Plan* (SSMP) and *System Objective* (SMS 2) do not always need to be documented in a specific *Safety Assessment Report* (SAR) and can be included directly in the *System Safety Approval* (SSG).

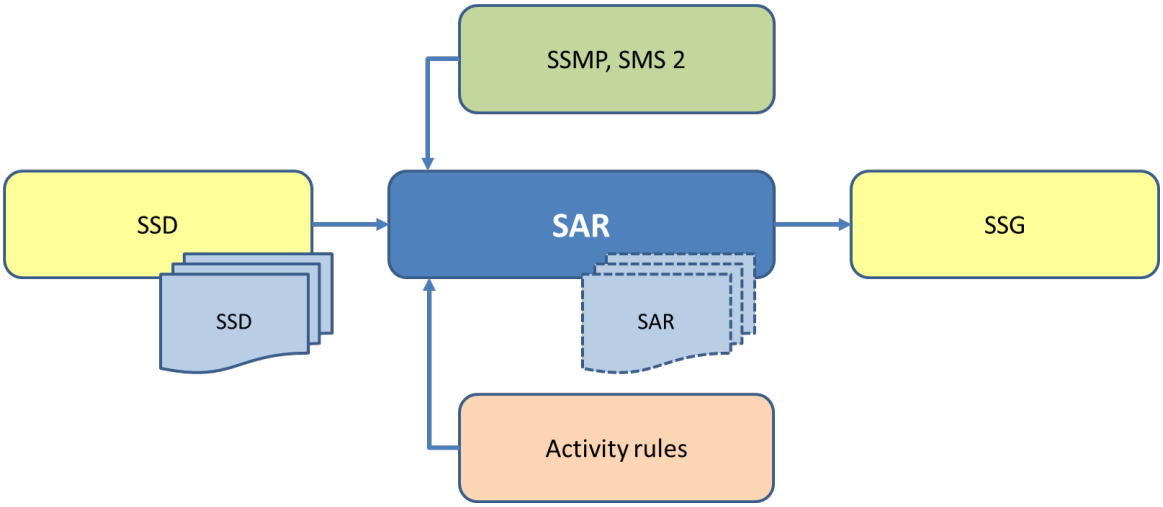
The *client's* summary of the completed system safety work and regulatory requirements and *System Objective* (SMS 2), based on the designer's *Safety Compliance Assessment* (SCA), does not always need to be documented in a separate *Safety Assessment Report* (SAR) and can be included directly in the *System Safety Declaration* (SSD).

The *designer's Safety Assessment Report* (SAR) is based on the checklist below.

Input, Output and Flowchart

The input to the *Safety Assessment Report* (SAR) activity for the *stakeholder* consists of the *client's System Safety Declaration* (SSD), *System Safety Management Plan* (SSMP) and *System Objective* (SMS 2) as well as operating rules.

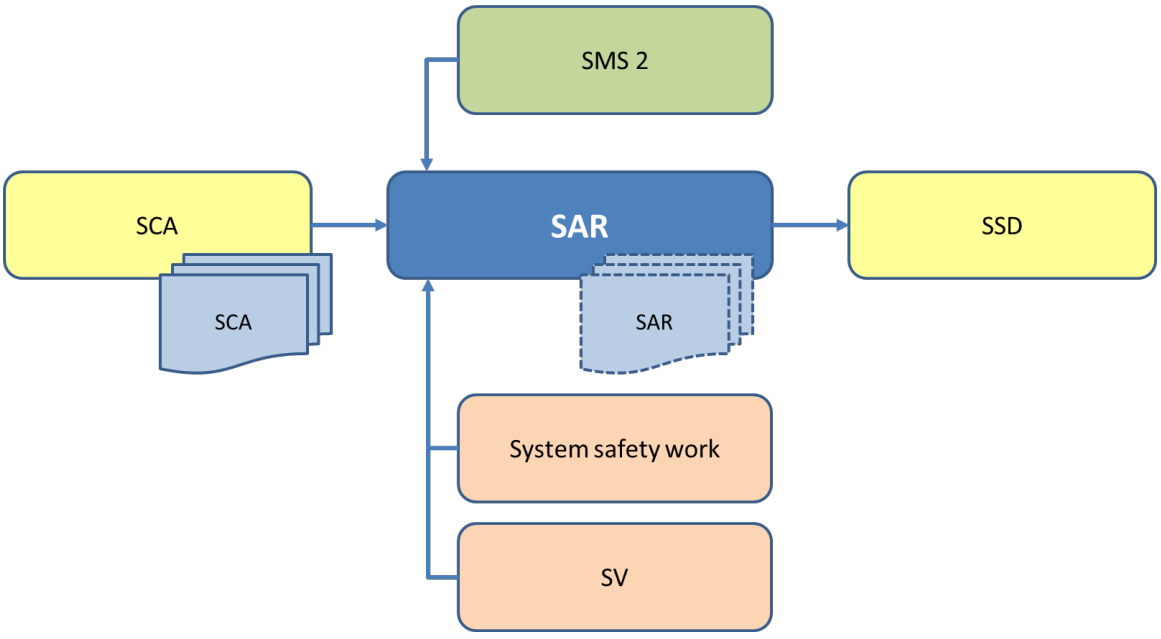
The output is a *Safety Assessment Report* (SAR). The report is input to the *System Safety Approval* (SSG).



Appendix 3, figure 35 *Safety Assessment Report (SAR) for the Stakeholder.*

The input to the *Safety Assessment Report* (SAR) activity for the *client* consists of the *designer's Safety Compliance Assessment* (SCA) and *System Objective* (SMS 2), as well as its own system safety work and *Safety Verification* (SV).

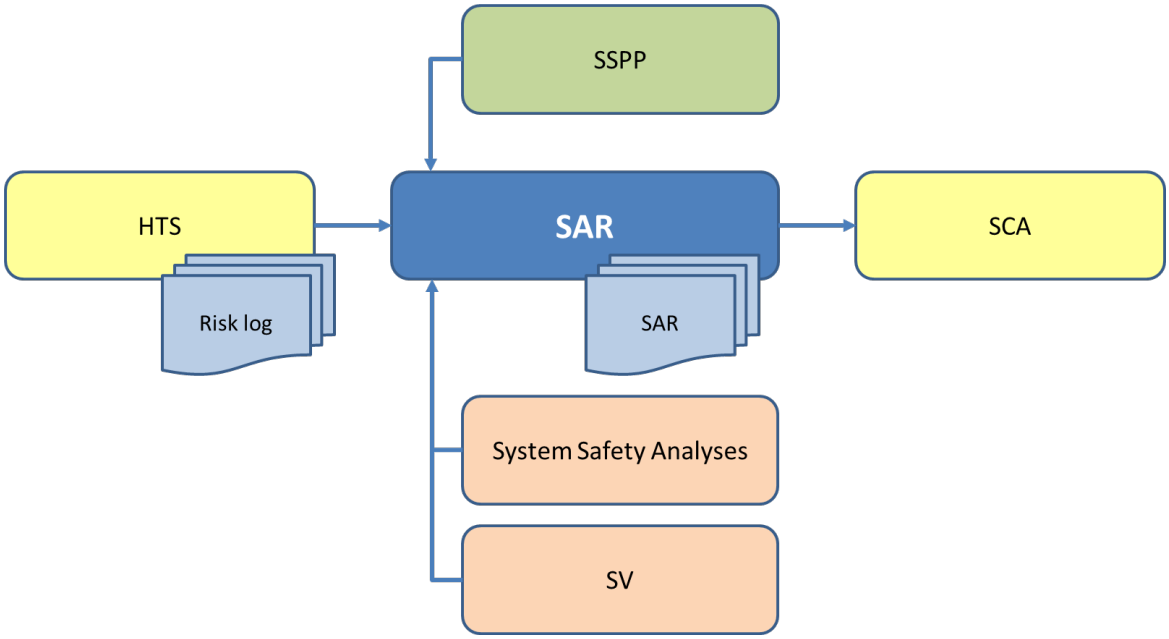
The output is a *Safety Assessment Report* (SAR). It is input to the *System Safety Declaration* (SSD).



Appendix 3, figure 36 *Safety Assessment Report (SAR) for the Client.*

The input to the *Safety Assessment Report* (SAR) activity for the *designer* is the *Hazard Tracking System* (HTS) and the contracted *System Safety Program Plan* (SSPP), as well as the completed system safety analyses and results from the *Safety Verification* (SV).

The output is a *Safety Assessment Report* (SAR). The report is input to the *Safety Compliance Assessment* (SCA).



Appendix 3, figure 37 *Safety Assessment Report (SAR) for the designer.*

A *Safety Assessment Report* (SAR) should include:

- A physical system description with the included subsystems and other possible equipment such as spare equipment or tool kits
- A specification of the permissible configurations of the technical system, allowable configurable parameter ranges and interfaces
- References to operating instructions and maintenance instructions and technical data
- A description of the intended use environment and operating conditions
- The data and prerequisites used and assumptions made
- An account of requirements in legislature, contracts and *System Safety Program Plan* (SSPP)
- The authority decisions in place to bring the technical system into service
- Accounting of applied civil and military standards
- An account of which route selections (VV) have been used, the motives for the route choices and acceptance criteria for when they are considered relevant and sufficient
- Accident risks managed with Route Selection (VV7) are accommodated within the *Tolerable Risk Level* (TR)
- A summary of dimensional accident risks and reference to *Risk Log* (RL)
- References to other system safety reports and risk documentation used
- References to system safety tests and a conclusion based on the results
- Remaining accident risks with restrictions and criteria for lifting restrictions
- A system safety evaluation as the basis for the conclusion
- Attachments, such as Safety Data Sheets

TASK 302 - HAZARD MANAGEMENT ASSESSMENT REPORT (HMAR)

This activity is fully regulated by the Safety Assessment Report (SAR) activity.

TASK 303 - TEST AND EVALUATION PARTICIPATION (TEP)

Purpose and Activity Description

The purpose of this activity is to present a conclusion regarding the system safety of the technical system or subsystems prior to the test to be carried out against standards, contracts or other requirements carried out within one's own organisation.

The output/documentation from this activity is *System Safety Certificate* (SSI).

Test and Evaluation Participation (TEP) is based on the current configurations of the technical system or subsystem. In addition, the test activities specified in the standards, alternatively in the test programs or test plans, to be carried out must be analysed. Based on the development status of the technical system, accident risks are identified and proposals are given for risk-reducing measures before the test. To support this activity, *Preliminary Hazard Analysis* (PHA), *Safety Instructions Analysis* (SIA) and, if necessary, the in-depth system safety analyses can be applied.

The *System Safety Certificate* (SSI) is a statement made by the *client,* the *system integrator* or the *designer* of their own testing organisation, which confirms compliance with legislation, rules and regulations. The *System Safety Certificate* (SSI) constitutes a summary of the system safety work carried out to date and that any deviations or uncertainties surrounding the test are managed by risk-reducing measures and that the technical system or subsystems offer a satisfactory level of safety, given that the proposals for *Safety Instructions* (SI) are complied with.

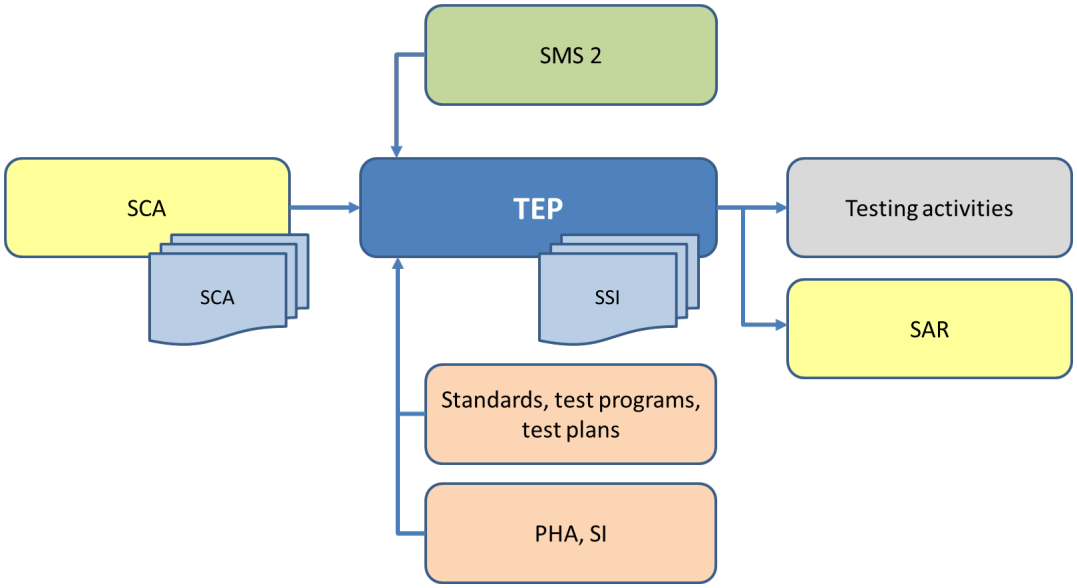
The *System Safety Certificate* (SSI) can basically have the same structure and content as a corresponding system safety decision, such as the *Safety Compliance Assessment* (SCA) or the *System Safety Declaration* (SSD). The *System Safety Certificate* (SSI) is signed by a competent person outside the part of the organisation that will carry out the test.

A System Safety Certificate (SSI) can be issued for organisational and methodological tests performed by the Swedish Armed Forces.

Input, Output and Flowchart

The input to the *Test and Evaluation Participation* (TEP) for the *client* and *system integrator* is the *Safety Compliance Assessment* (SCA) *and System Objective* (SMS 2) as well as standards, test programs or test plans.

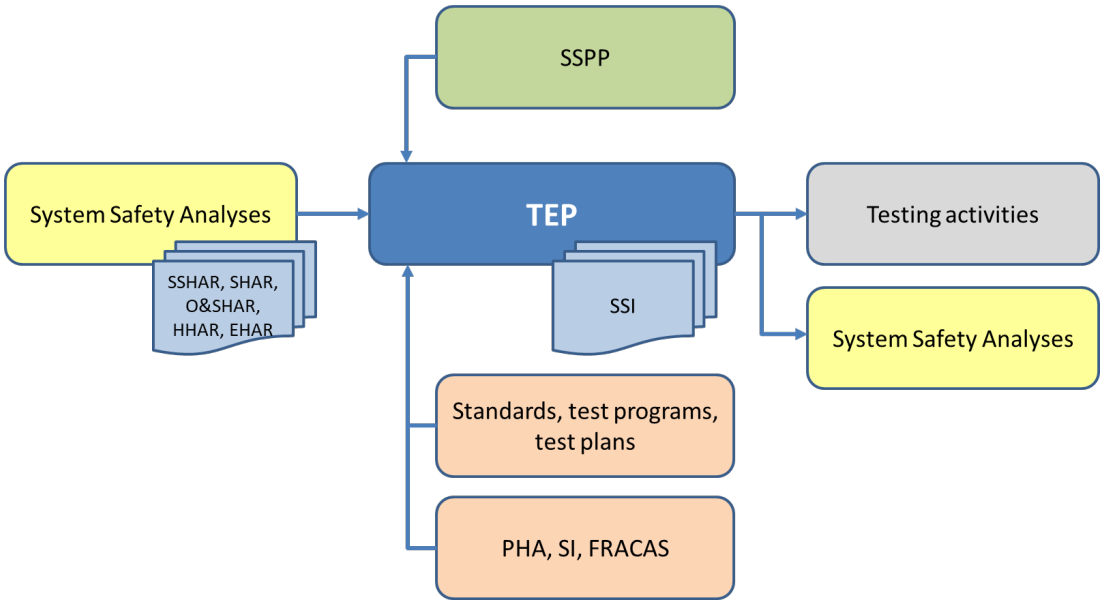
The output is a *System Safety Certificate* (SSI). This provides input into test operations and to the *Safety Assessment Report* (SAR).



Appendix 3, figure 38 *Test and Evaluation Participation (TEP) for client and system integrator.*

Inputs to the activity *Test and Evaluation Participation* (TEP) for *designers* consists of system safety analyses and the contracted *System Safety Program Plan* (SSPP) as well as standards, test plans and experience data from the *Failure Reporting System* (FRACAS) .

The output is a *System Safety Certificate* (SSI). This provides input to test operations and to the *Safety Assessment Reports* (SAR).



Appendix 3, figure 39 *Test and Evaluation Participation (TEP) for designer.*

If a *Safety Assessment Report* (SAR) exists containing the information below, reference may be made to this document. A *System Safety Certificate* (SSI) should include:

- A specification of the permissible configurations of the technical system, allowable configurable parameter ranges and interfaces
- What operating instructions and S*afety Instructions* (SI) exist
- A description of the intended test environment
- Reference to test program or test plan
- That the legislation is complied with at the time of testing
- System safety analyses carried out to identify, analyse, assess accident risks and proposals for risk-reducing measures for the test
- Which environmental and health hazardous substances/materials are present in the technical system and which persons or external environment that can be exposed during the test. For chemical products, Safety Data Sheets must be provided
- Recommended training for the test personnel

S31 - Failure Reporting Analysis and Corrective Action System (FRACAS)

Purpose and Activity Description

The purpose of this activity is to return incident and accident-related information in order to prevent a similar accident, under the corresponding conditions, from occurring again. The activity can be applied, on the one hand, for incident and accident reporting in internal operations and also by contract agreement to change the design before the technical system has been put into service.

The complete term is *Failure Reporting, Analysis and Corrective Action System* (FRACAS), also called *Failure Reporting System*) and the output/documentation is *Action Reports*.

The *Failure Reporting System* (FRACAS) should be in place from the first test or use until the technical system is decommissioned. Data from the *Failure Reporting System* (FRACAS) and its compiled information can be used both for the current technical system and for similar technical systems using, for example, the same subsystem or components.

Data from the *Failure Reporting System* (FRACAS) forms part of the basis for the various system safety analyses. Experience-related information can be used to analyse the real impact of possible modifications and to assess the impact of proposed risk-reducing measures in the technical system or in its use.

Data from the *stakeholder's Failure Reporting System* (FRACAS) is suitably analysed by the *System Safety Working Group* (SSWG) during the maintenance and decommissioning stage, which also has to propose corrective actions or influence the content of future *System Objective* (SMS).

Data from the *designer's Failure Reporting System* (FRACAS) are suitably analysed by the *Integrated Product Team/System Safety Group* (IPT/WG) during the development stage of the technical system, which also proposes risk-reducing actions.

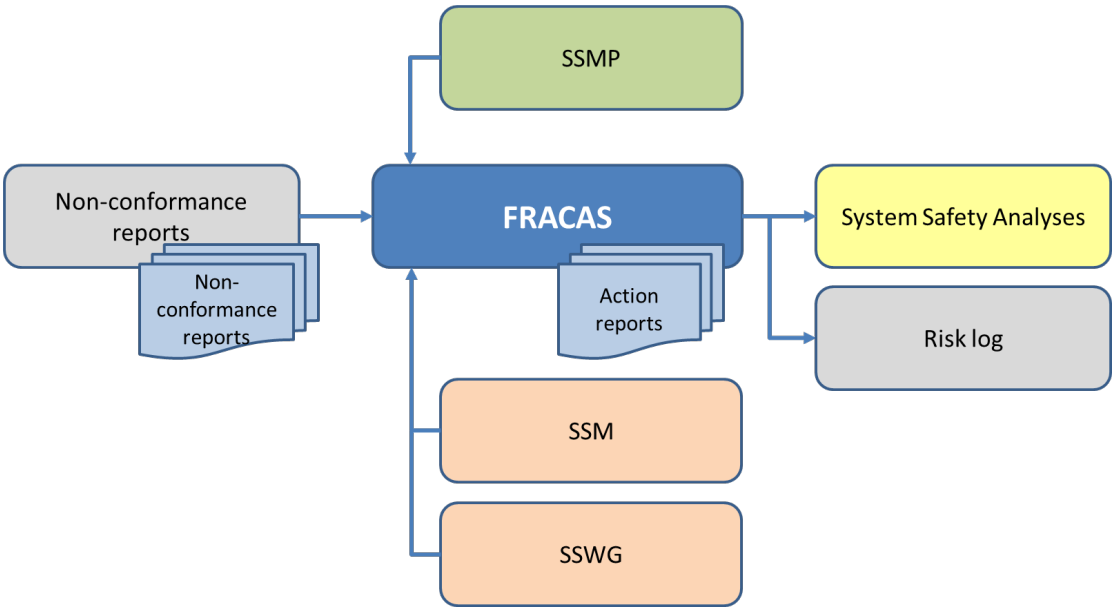
The *Failure Reporting System* (FRACAS) provides different stakeholders with data or compiled information regardless of the lifecycle stage the technical system is in. The *Failure Reporting System* (FRACAS) needs to be able to classify incoming discrepancy reports a severity point of view of system safety.

The cause of accidents and incidents is usually not a single cause of failure but a chain of events with a number of unfortunate circumstances consisting of both causes of failure and natural conditions. The synthesis of a variety of data along with certain conditions can prevent future accidents.

Input, Output and Flowchart

The input data for the activity *Failure Reporting System* (FRACAS) for the *stakeholder* consists of deviation reports from the Swedish Armed Forces' usage, maintenance and storage (transport) as well as *System Safety Management Plan* (SSMP). A *System Safety Announcement* (SSM) may also exist. The *System Safety Working Group* (SSWG) can prepare action reports.

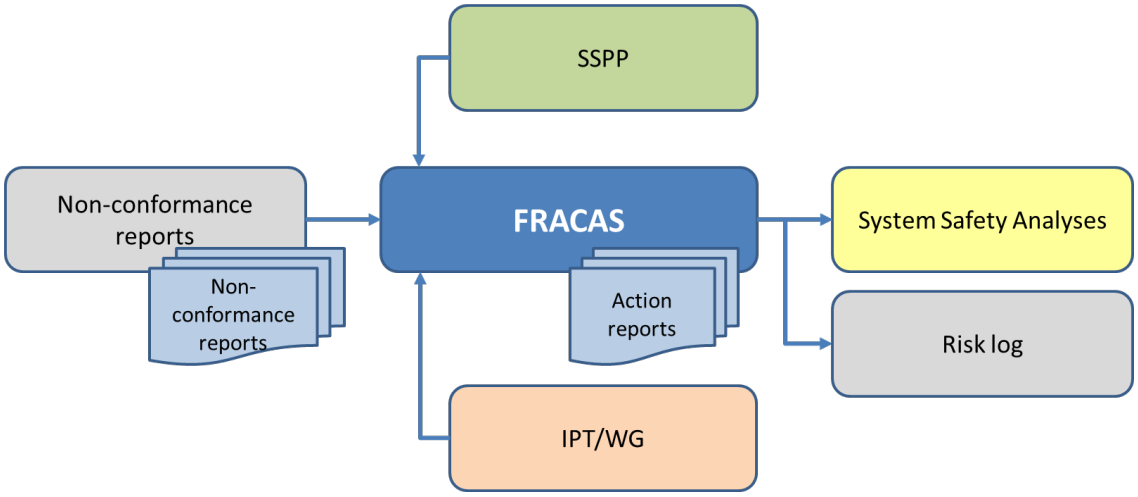
Output is *Action Reports.* These may constitute input to in-depth system safety analyses and *Risk Log* (RL).



Appendix 3, figure 40 *The Failure Reporting System (FRACAS) for stakeholders.*

Data input to the activity (FRACAS) for the *designer* consists of the deviation reports from use, testing, maintenance, storage (transport) and other management as well as the contracted *System Safety Program Plan* (SSPP).

Output is *Action Reports* that constitute input to the *designer's* various in-depth system safety analyses and *Risk log* (RL).



Appendix 3, figure 41 The Failure Reporting System (FRACAS) for designers.

The *Failure Reporting System* (FRACAS) should include:

- Reporting party with contact details
- Identity of the technical system and the status of materiel documentation
- The *Safety Instructions* (SI) included where applicable
- Description of the course of events and consequence of the occurrence
    - Location and date of the event
    - The activities carried out at the time of the incident, such as use, movement, combat, care, maintenance or storage (transport)
    - Any damage to person, property or external environment, including third party or its property
    - What damages/injuries could have potentially occurred
    - Miscellaneous
- Feedback to the reporting party

TASK 304 - SAFETY REVIEW (SR)

The purpose of this activity is to evaluate, from a system safety point of view, proposed changes (modifications) to established configurations of technical systems and products. It may relate to amendments to requirements documents and proposed modifications to hardware, electronics and/or software. The activity should be coordinated with the configuration plan of the technical system.

Activities- SECTION 400 - Verification

TASK 401 - SAFETY VERIFICATION (SV)

Purpose and Activity Description

The purpose of this activity is to demonstrate that system safety requirements are met by verification and to demonstrate that the technical system corresponds to the required need through validation.

The output/documentation from this activity is *System Safety Verification Report* (SVR).

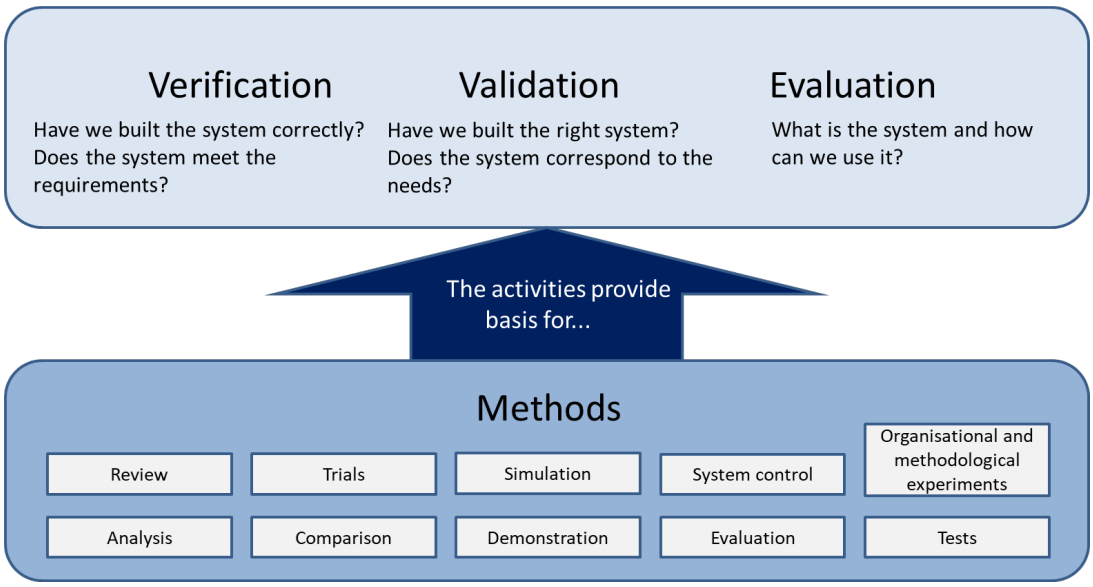
There are a number of different methods that can provide the basis for analysis if the respective requirements are met. The result of the verification and validation can be used as support and to substantiate the evidence in the system safety evaluation.

Safety Verification (SV) methods should be an integral part of the verification of the technical system and be part of the overall planning for all verification activities.

Introducing mechanical failures or injecting errors into the software can be used to demonstrate that safety systems including error detection, work as intended and that the overall robustness of risk-reducing measures can be considered sufficient. This also means that interfaces need to be adapted so that a faulty injection is possible on the technical system.

In the event of design changes, re-verification of system safety requirements must take place.

Evaluation falls outside verification and validation and is applied to examine how the technical system is possible to use before determining the final configuration.

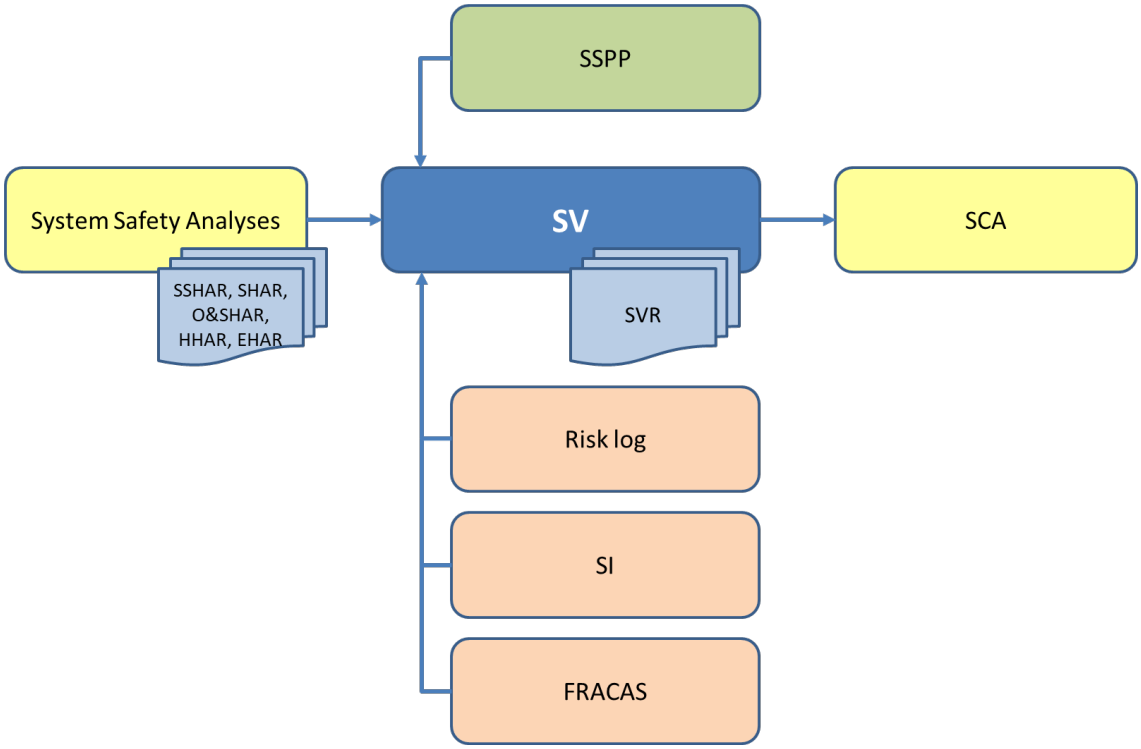


Appendix 3, figure 42 Methods of verification and validation.

Input, Output and Flowchart

The input to the *Safety Verification* (SV) activity consists of completed system safety analyses, the contractual *System Safety Program Plan* (SSPP) and experience data from the *Failure Reporting System* (FRACAS) as well as *Safety Instructions* (SI).

The output is *System Safety Verification Report* (SVR). It forms a basis for the *Safety Compliance Assessment* (SCA).



Appendix 3, figure 43 Safety Verification (SV).

A *System Safety Verification Report* (SVR) should include:

- Configuration and status of the technical system
- The purpose of verification and the specific system safety requirements covered
- Reference to standards used or description of other methods of verification
- A summary and conclusions from the test results obtained
- Motives for which accident risks supported by the results of the test carried out, may demonstrate compliance or contribute to demonstrating the system safety of the technical system

TASK 402 - EXPLOSIVES HAZARD CLASSIFICATION DATA

This activity is completely regulated by the Weapons and Ammunition Safety Handbook (H VAS).

TASK 403 - EXPLOSIVE ORDNANCE DISPOSAL DATA

This activity is completely regulated by the Weapons and Ammunition Safety Handbook (H VAS).

Activities - SECTION 500 - Decisions

S51 - SAFETY COMPLIANCE ASSESSMENT (SCA)

Purpose and Activity Description

The purpose of the *Safety Compliance Assessment* (SCA) activity is for the *designer* to report their conclusion regarding the system safety of the technical system before delivery.

The output/documentation from this activity is *Safety Compliance Assessment* (SCA).

The *Safety Compliance Assessment* (SCA) constitutes a summary of the *designer's* completed system safety work for a particular technical system, which is based on the contractual *System Safety Program Plan* (SSPP). The *Safety Compliance Assessment* (SCA) declares that current legislation at the time of delivery is met, compliance with the *client's* system safety requirements and that the technical system offers a satisfactory level of safety.

The *Safety Compliance Assessment* (SCA) contains the *designer's* position which assumes compliance with the operating instructions, maintenance instructions and *Safety Instructions* (SI) when the technical system is put into service. The *designer's* position is based on a conducted system safety evaluation.

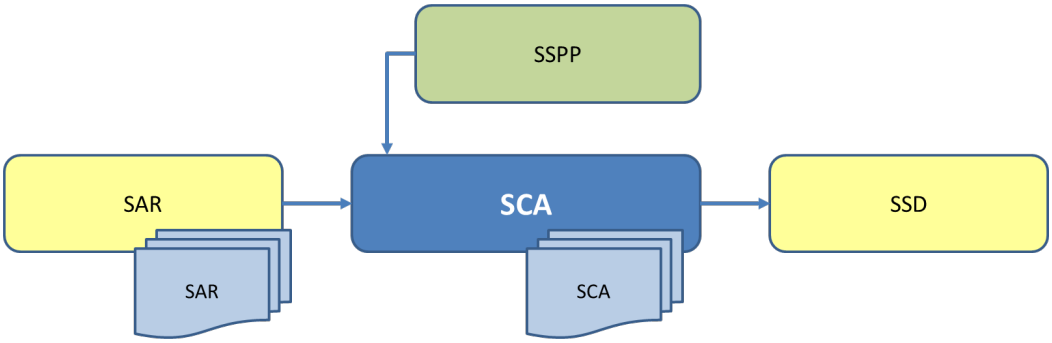
As a basis for the system safety evaluation, with its arguments and evidence, all system safety activities undertaken are in the course of the development of the technical system. The results of these activities have been documented as they have been carried out. The compilation of the *Safety Compliance Assessment (SCA*) is most often documented in a *Safety Assessment Report* (SAR) together with a *Risk Log* (RL). The *Safety Compliance Assessment (*SCA) refers to these documents as well as to other risk documentation.

The *Safety Compliance Assessment* (SCA) is signed by the company signatories of the *designer* or one of their delegates, as regulated in the contracted *System Safety Program Plan* (SSPP).

Input, Output and Flowchart

The input to the *Safety Compliance Assessment* (SCA) activity consists of the *Safety Assessment Report* (SAR) with *Risk Log* (RL) and the Contracted *System Safety Program Plan* (SSPP).

The output is the *Safety Compliance Assessment* (SCA). It is input to the *System Safety Declaration* (SSD).



Appendix 3, figure 44 *Safety Compliance Assessment (SCA).*

If a *Safety Assessment Report* (SAR) exists containing the information below, reference may be made to this document. The *Safety Compliance Assessment* (SCA) should include the following:

- A specification of the design of the technical systems, permissible configurations, changeable parameter ranges, interfaces and associated technical data
- Which operating instructions, maintenance instructions and S*afety Instructions* (SI) are available
- A description of the intended usage, environment and operating conditions
- That the legislation is complied with at the time of delivery
- Certificates or approvals such as DoC, CoC or CA exist
- Physical markings such as CE and wheel markings exist
- That possible exemptions for military materiel are documented
- The authority decisions in place to bring the technical system into service
- What civil and military system safety measures are applied
- The route selections used and justification why they have been considered relevant and adequate
- What system safety requirements with their criteria have been met and how the requirements on the design have been verified
- System safety analyses and system safety tests carried out to identify, analyse, assess, classify and address accident risks and their causes
- *Risk Log* (RL) with any identified accident risk that may occur during both expected use and in abnormal conditions, together with risk-reducing measures, recommendations and S*afety Instructions* (SI), exist
- What accident risks are managed
- What accident risks remain with restrictions

- Which environmental and health hazardous substances/materials present in the technical system and to which persons or the external environment may be exposed during use, maintenance, storage (transport) or disposal. For chemical products, Safety Data Sheets must be provided
- Recommended training for users
- References to protocols or meeting notes from the *Integrated Product Team/System Safety Group* (IPT/WG)

S52 - SYSTEM SAFETY DECLARATION (SSD)

Purpose and Activity Description

The purpose of the *System Safety Declaration* (SSD) activity is for the *client* to presents their conclusion regarding the system safety of the technical system prior to handover.

The output/documentation from this activity is *System Safety Declaration* (SSD).

The *System Safety Declaration* (SSD) constitutes a summary of the completed system safety work of both the *client* and the *designer* of a particular technical system, which is based on the requirements of *System Objective* (SMS 2) translated into the *client's System Safety Program Plan* (SSPP). The *System Safety Declaration* (SSD) declares that current legislation at the time of delivery is met, compliance with the *stakeholder's* system safety requirements and that the technical system offers a satisfactory level of safety.

The *System Safety Declaration* (SSD) contains the conclusion of the *client*, who assumes compliance with materiel publications and *Safety Instructions* (SI) when the technical system is put into service. The *client's* conclusion is based on the completed system safety evaluation using the *designer's Safety Compliance Assessment* (SCA) as the basis.

As a basis for the *client's* system safety evaluation, with its arguments and evidence, are all the system safety activities carried out by both the *designer* and the *client* during the development of the technical system. The results of these activities have been documented as they have been carried out. The compilation of the *System Safety Declaration* (SSD) is most often documented in a *Safety Assessment Report* (SAR) together with a *Risk Log* (RL). The *System Safety Declaration* (SSD) refers to these documents as well as to other risk documentation.

The *System Safety Declaration* (SSD) may also contain restrictions, which are temporary limitations on the authorised use of the technical system, in order to temporarily manage a certain remaining accident risk, thereby imposing system safety requirements.

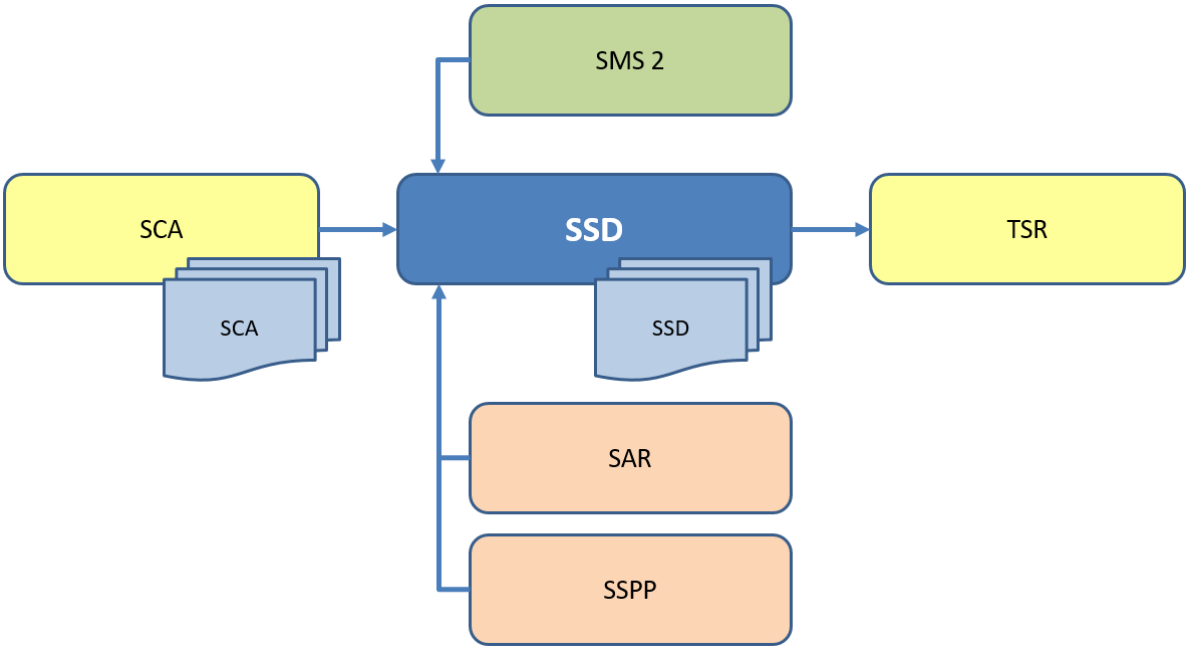
For munitions, minutes of the FMV Advisory Groups must be attached and implemented actions must be annotated. If a certain individual advice has not been followed, this must also be stated and justified.

The *System Safety Declaration* (SSD) is signed by the authorised person of the *client*.

Input, Output and Flowchart

The input to the *System Safety Declaration* (SSD) activity consists of the designer*'s Safety Compliance Assessment* (SCA) and *System Objective* (SMS 2), as well as the *client's System Safety Program Plan* (SSPP) and *Safety Assessment Report* (SAR) with *Risk Log* (RL).

Output is *System Safety Declaration* (SSD). It is input to *Training Safety Regulations* (TSR).



Appendix 3, figure 45 *System Safety Declaration (SSD).*

If a *Safety Assessment Report* (SAR) exists containing the information below, reference may be made to this document. The *System Safety Declaration* (SSD) should include the following:

- A specification of the permissible configurations of the technical system, allowable configurable parameter ranges and interfaces
- What materiel publications, technical data and *Safety Instructions* (SI) exist
- Description of the intended use of environment and operating conditions
- That the legislation is complied with at the time of delivery
- Certificates or approvals such as DoC, CoC or CA exist
- Physical markings such as CE and wheel markings exist
- That possible exemptions for military materiel are documented
- The authority decisions in place to bring the technical system into service
- What civil and military system safety measures are applied
- The route selections used and justification why they have been considered relevant and adequate
- What system safety requirements with their criteria have been met and how the requirements on the design have been verified
- System safety analyses and system safety tests carried out to identify, analyse, assess, classify and address accident risks and their causes

- *Risk Log* (RL) with any identified accident risk that may occur during both expected use and in abnormal conditions, together with risk-reducing measures, recommendations and S*afety Instructions* (SI), exist
- What accident risks are managed
- What accident risks remain with restrictions and the criteria for lifting restrictions
- Which environmental and health hazardous substances/materials present in the technical system and to which persons or the external environment may be exposed during use, maintenance, storage (transport) or disposal. For chemical products, Safety Data Sheets must be provided
- Recommended training for users
- Response to any request regarding the exclusion of an accident risk that is *Not Tolerable* (NT)
- If the technical system contains weapons, ammunition or explosives:
    - Minutes from FMV Advisory Groups exist and that advisories are commented and justified
    - Lists of approved ammunition that may be used in the weapon system exist, alternatively that the ammunition is approved against certain weapons systems

S53 - TRAINING SAFETY REGULATIONS (TSR)

Purpose and Activity Description

The purpose of the *Training Safety Regulations* (TSR) activity is for the *stakeholder* to approve the materiel documentation, complete training and provide the operating rules required for the safe handling of the technical system. Handling refers to the use, maintenance, storage (transport) and disposal.

The output/documentation of this activity is *Training Safety Regulations* (TSR).

Approval of materiel documentation and operating rules is a prerequisite for issuing *System Safety Approval* (SSG). Completion of training should take place before the *Decision on Use, Central Level* (BOAC) is taken. The information is derived from, among other things, the *Safety Instructions* (SI)

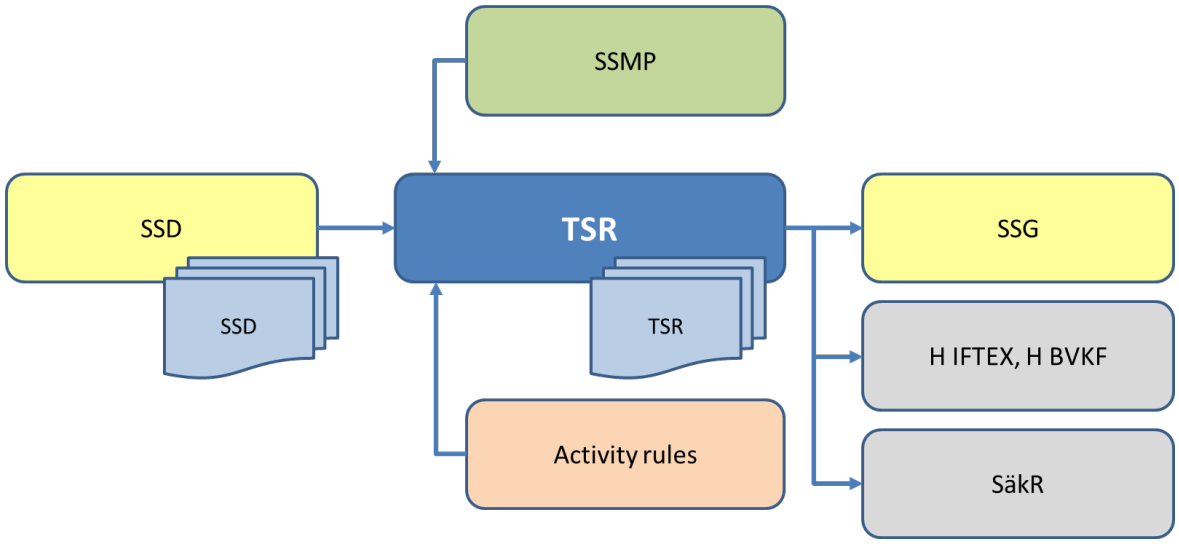
Specific instructions may exist for transporting and storing explosives (IFTEX), fire and rescue instructions (BRI) and for use, such as the Safety Regulation (SäkR).

Regulations for the transport and storage of technical systems or products containing explosives are established by the Swedish Civil Contingencies Agency (MSB), including classification code under the *United Nations Recommendations on the Transport of Dangerous Goods* (UN system). The code consists of a United Nations class and a UN number and is applied in various transport rules, such as ADR-S. For further details, see H IFTEX.

Input, Output and Flowchart

The input to the *Training Safety Regulations* (TSR) activity consists of the *System Safety Declaration* (SSD) and the *System Safety Management Plan* (SSMP) as well as operating rules.

The output is *Training Safety Regulations* (TSR). It provides the basis for the regulations and supplementary handbooks, such as the *Swedish Armed Forces´ Handbook Storage and Transport of Munitions and Other Explosives (*H IFTEX), *Swedish Armed Forces´ Handbook for Action against Fire and Explosion Hazards, Water Pollution and chemical health effects from flammable goods* (H BVKF) and the Safety Regulatory documentation (SäkR).



Appendix 3, figure 46 Training Safety Regulations (TSR).

S54 - SYSTEM SAFETY APPROVAL (SSG)

Purpose and Activity Description

The purpose of the *System Safety Approval* (SSG) activity is that the *stakeholder* accounts on the one hand their conclusion on the system safety of the technical system and also that risk-reducing measures have been taken prior to the time the technical system is put into service.

The output /documentation from this activity is *System Safety Approval* (SSG).

The *System Safety Approval* (SSG) constitutes a summary of the completed system safety work of both the *client,* the *designer* and the *stakeholder* for a particular technical system, which is based on the requirements of the *System Safety Management Plan* (SSMP) and *System Objective* (SMS 2). The *System Safety Approval* (SSG) states that current legislation at the time of the delivery of the equipment is met, that the *stakeholder's* own system safety requirements are met and that the technical system offers a satisfactory level of safety for the activities to be carried out.

The *System Safety Approval* (SSG) contains the *stakeholder's* own position, which assumes compliance with materiel documentation and operating rules when the technical system is put into service. The *stakeholder's* own conclusion is based on the completed system safety

evaluation using the *client's System Safety Declaration* (SSD) as the basis. The *System Safety Approval* (SSG) is valid for permitted configurations, including the configurable parameter ranges, of the technical system. If changes (modifications) occur, a new *System Safety Approval* (SSG) may need to be issued.

As a basis for the *stakeholder's* system safety assessment, with its arguments and evidence, are all the system safety activities carried out by both the *designer* and the *client* during the development of the technical system. The compilation of the *System Safety Approval (SSG*) is most often documented in a *Safety Assessment Report* (SAR) together with a *Risk Log* (RL). The *System Safety Approval* (SSG) refers to these documents and possibly to other risk documentation.

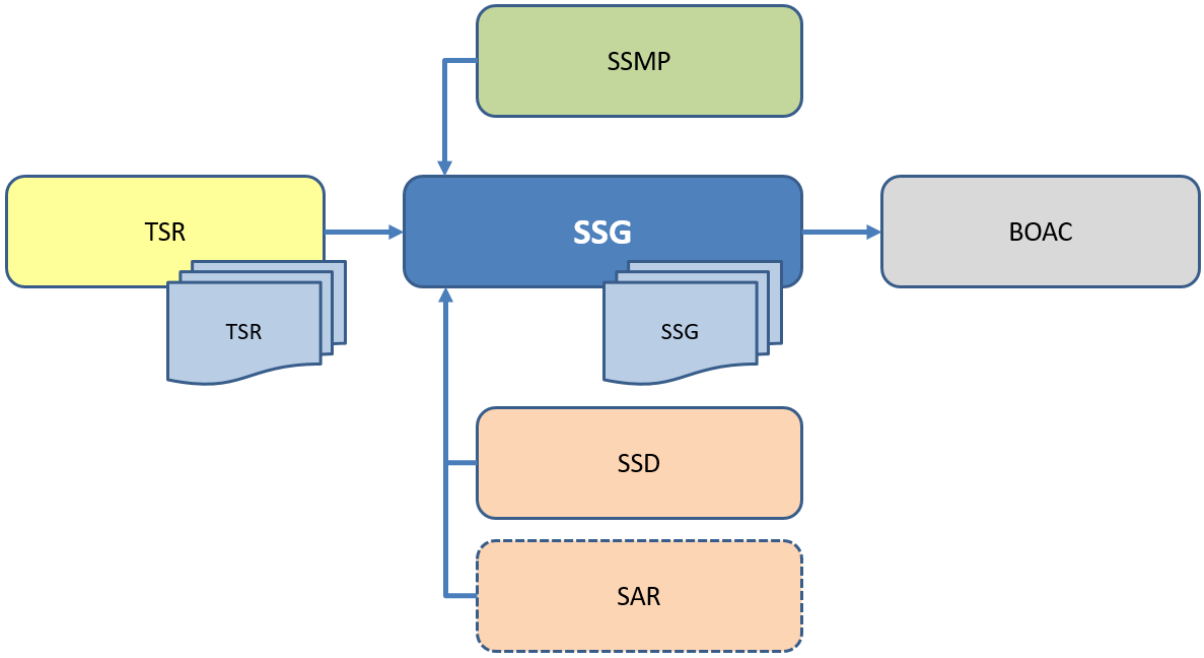
The *System Safety Approval* (SSG) may also contain restrictions, which are temporary limitations on the authorised use of the technical system, in order to temporarily manage a certain remaining accident risk, thereby fulfilling system safety requirements.

The *System Safety Approval* (SSG) is signed by the authorised person of the *stakeholder*. For the scope and content of the *System Safety Approval* (SSG), see *section 17.5*.

Input, Output and Flowchart

The input to the *System Safety Approval* (SSG) activity consists *of* the *Training Safety Regulation* (TSR), the *System Safety Management Plan* (SSMP) as well as the *client's System Safety Declaration* (SSD) and, if necessary, the *stakeholder's* own *Safety Assessment Report* (SAR) with *Risk Log* (RL).

The output is the *System Safety Approval* (SSG). This provides input to the *Decision on Use, Central Level* (BOAC).

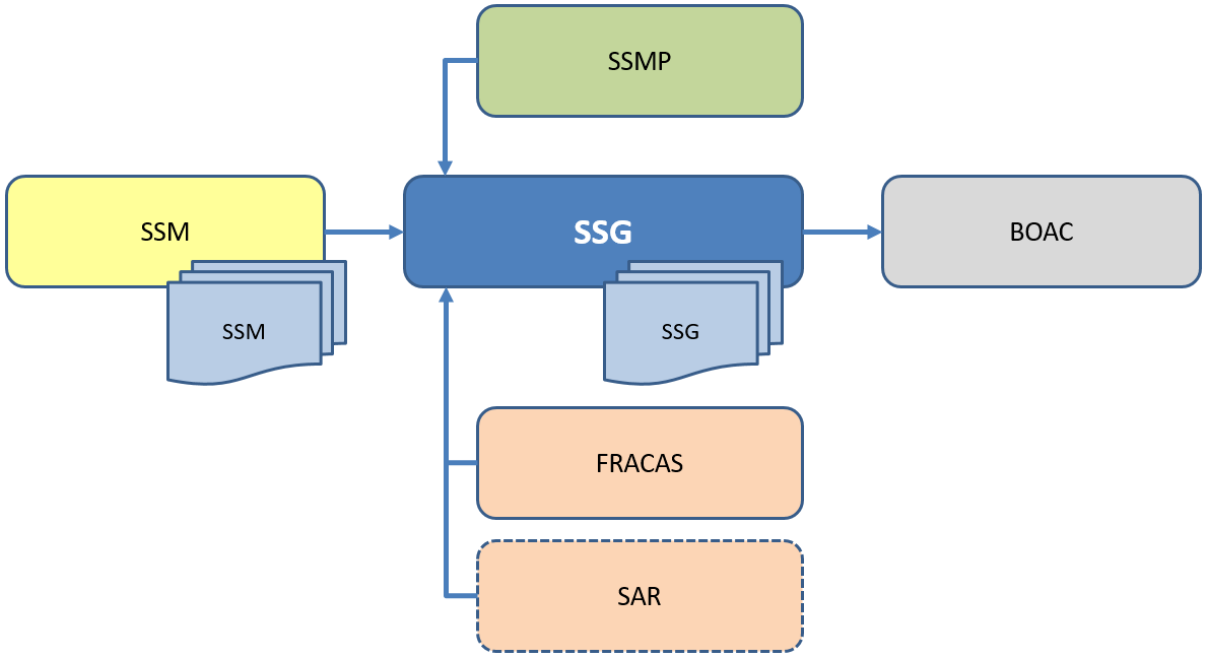


Appendix 3, figure 47 *System Safety Approval (SSG) based on System Safety Declaration (SSD).*

In cases where the *stakeholder* receives *System Safety Announcements* (SSM), these may require changes (modifications) to technical systems and that new system safety decisions from the *client/designer* need to be issued.

The input to the *System Safety Approval* (SSG) activity consists of *System Safety Announcements* (SSM) and *System Safety Management Plan* (SSMP) as well as data from *Failure Reporting System* (FRACAS) and, if necessary, the *stakeholder's* own *Safety Assessment Report* (SAR) with *Risk Log* (RL).

The output is the *System Safety Approval* (SSG). This provides input to the *Decision on Use, Central Level* (BOAC).



Appendix 3, figure 48 *System Safety Approval (SSA) based on System Safety Announcements (SSM).*

S55 - SYSTEM SAFETY ANNOUNCEMENTS (SSM)

Purpose and Activity Description

The purpose of the *System Safety Announcement* (SSM) activity is for an actor wishing to issue information about a safety deficiency in a technical system or product, or about deficiencies and inaccuracies in its use, maintenance or handling, without reclaiming an issued system safety decision.

The output/documentation of this activity is *System Safety Announcement* (SSM).

By issuing a *System Safety Announcement* (SSM) to the *stakeholder*, the actor concerned may get leeway to carry out initial preparation and propose measures such as changes (modifications), and/or modification of other documentation or restrictions. A *System Safety Announcement* (SSM) applies until the safety deficiency has been rectified.

If several different events or observations exist for the same technical system or product, it is recommended that one *System Safety Announcement* (SSM) be issued per observation. This simplifies the administration when deciding that the safety deficiency has been rectified.

If a *System Safety Announcement* (SSM) means that information to clarify, inform or remind the user of conditions related to the intended use, change of use including normal slippage or that operating rules need to be tightened, the case may be closed by the Chairman of the *System Safety Working Group* (SSWG), without new system safety decisions being issued.

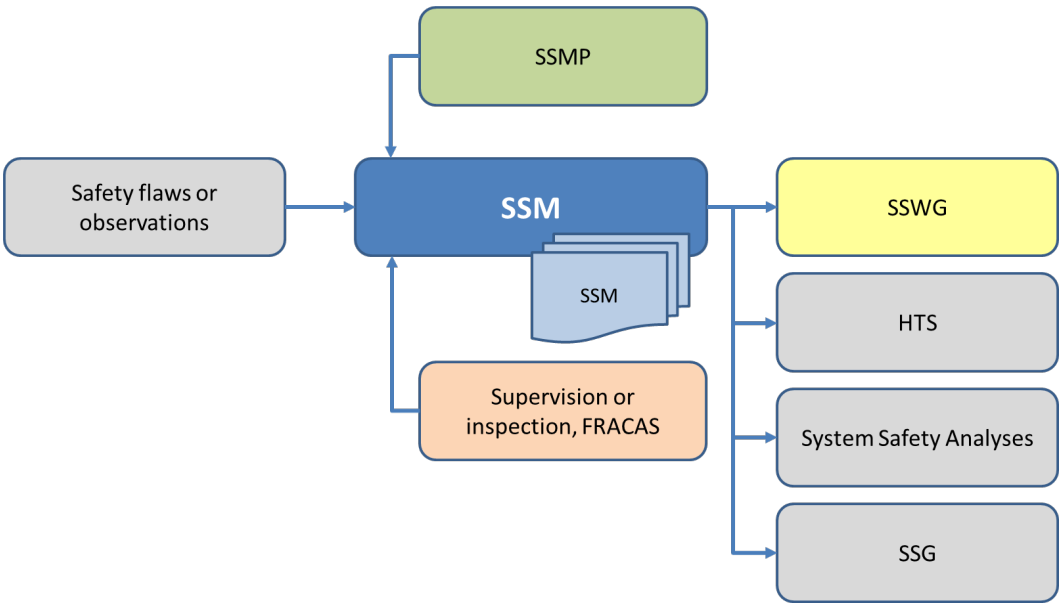
If a *System Safety Announcement* (SSM) means that a change (modification) needs to be implemented to address the safety deficiency, new system safety decisions need to be issued.

A *System Safety Announcement* (SSM) may be recalled by the issuer if the safety flaw is no longer considered current. Such action is documented by the Chairman of the *System Safety Working Group* (SSWG) in minutes or meeting notes.

Input, Output and Flowchart

The input to the *System Safety Announcement* (SSM) activity consists of the knowledge of safety deficiencies by the client, designer or by observations, as well as *System Safety Management Plan* (SSMP). Input data may also consist of reports from supervision or inspections or data from the *Failure Reporting System* (FRACAS).

The output is a *System Safety Announcement* (SSM). It provides input to the *System Safety Working Group* (SSWG) for the preparation of the case.



Appendix 3, figure 49 *System Safety Announcement (SSM).*

A *System Safety Announcement* (SSM) should include at least:

- Identification of a technical system or product
- Analysis of the occurrence or observations
- Risk assessment
- Proposal for recommendations (e.g. use prohibitions)

Editorial Information

The revision of the System Safety Handbook has been carried out with the aim of making it more efficient and modernise the system safety activities at the Swedish Armed Forces and FMV.

The previous version of the handbook has been used both in equipment procurement projects at the Swedish Armed Forces, FMV, industry and consulting companies both nationally and internationally, as well as at the FMV System Safety course. During the use of the handbook, it has become apparent that an overall rework of the handbook's content was needed. Furthermore, a new version of MIL-STD-882 has been issued.

SÄKINSP commissioned FMV to submit a proposal for a new System Safety Handbook in the assignment "Samordning Systemsäkerhet 2017–2019" with continuation in the assignment " Samordning Systemsäkerhet 2020–2022".

The main editorial work has been carried out by FMV.

Workgroup at FMV:

Lars Lange, Project manager

Mikael Lindbergh, Deputy Project Manager

Bo Höjdefors

Johan Niemi

Peter Djervbrant

System matter experts:

Martin Dalaryd

Jan Jacobson

Pär-Anders Wallentin

HKV PROD constituted a Swedish Armed Forces joint steering group in September 2018, with C RPE MTRL Joakim Sellén as chairman, to manage workgroup at FMV. The steering group has held 15 meetings.

Anchoring of the handbook's design and content has been carried out by FMV together with a reference group of around 45 people who represented the Swedish Armed Forces, FMV, industry and consulting companies. Relevant content in the previous handbook, System Safety Handbook 2011, has been taken care of in this edition.

The first reference group meeting was held on 22 November 2018 (approx. 40 participants) with the aim of obtaining opinions and experiences from the application of the System Safety

Handbook 2011 and to ensure the content of the Handbook with regards to breadth, depth and quality so that the new edition would be well established with all participants.

The second reference group meeting was held on 21 November 2019 (approx. 35 participants) where participants received a first draft of the handbook where suggestions on disposition and the methodology for the life cycle, accident risk and road choice model were presented. The reference group then had the opportunity to study the content and come back with remarks during the first quarter of 2020.

The workgroup processed the remarks received and produced a broader and more comprehensive draft for a new handbook, which was then sent out for formal referral within the Swedish Armed Forces and FMV during the second quarter of 2021. The workgroup handled the remarks and had ongoing coordination with representatives from the reference group and with FLYGI and SÄKINSP.

A final referral within the Swedish Armed Forces and FMV was carried out during the first quarter of 2022. The referral prompted only minor adjustments and clarifications. C RPE MTRL, also chairman of the steering group, Joakim Sellén, together with representatives from HKV PROD and FMV, presented the System Safety Handbook 2022 for C RPE, Jonas Lotsne, on May 20, 2022.

The Swedish Armed Forces´ Publications Coordinator has endorsed the formal approval on 22 June 2022.

List of Figures

This publication contains no figures of originality.

List of Sources

In this version of the handbook, the following sources have been used.

Sources Outside the Swedish Armed Forces

- EU Regulation 1907/2006, Registration, evaluation, authorisation and restriction of chemicals (REACH)
- EU Regulation 765/2008, Setting out the requirements for accreditation and market surveillance relating to the marketing of products
- EU Regulation 1272/2008, Classification, labelling and packaging of substances and mixtures (CLP)
- EU Directive 2006/42/ on machinery
- EU Directive 2013/35/EU on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields)
- EU Directive 2014/90/EU on marine equipment
- EU Directive 2021/555/EU on control of the acquisition and possession of weapons (codification)
- LVD (Low Voltage Directive) 2014/35/EU
- RED (Radio Equipment Directive) 2014/53/EU
- Swedish Environmental Code (SFS 1998:808)
- Work Environment Act (SFS 1977:1160*)*
- The Electrical Safety Act (SFS 2016:732)
- The Ship Safety Act (SFS 2003:364)
- Vehicle Ordinance (SFS 2009:211)
- Vehicle Act (SFS 2002:574)
- Act on Flammable and Explosive Goods (SFS 2010:1011)
- Act on marine equipment (Lag om marin utrustning) (SFS 2016:768)
- Aviation Act (SFS 2010:500)
- Product liability legislation (EU Directive 85/374/EEC, SFS 1992:18)
- Product Safety Act (SFS 2004:451)
- Ordinance on safety for naval vessels (Förordning om säkerheten på örlogsfartyg) (SFS 2003:440)
- Ordinance on International Law Review of Arms Projects (SFS 2007:936)
- Ordinance on market control of goods and related supervision (Förordning om marknadskontroll av varor och närliggande tillsyn) (SFS 2014:1039)
- Ordinance on marine equipment (Förordning om marin utrustning) (SFS 2016:770)
- Ordinance on Civil Aviation (SFS 2010:770)
- Ordinance on military traffic (Militärtrafikförordning) (SFS 2009:212)
- Use of work equipment (AFS 2006:4)
- Machinery Directive (AFS 2008:3)
- The Swedish Post and Telecommunications Authority's regulations on requirements etc. for Radio equipment (Post- och telestyrelsens föreskrifter om krav m m på Radioutrustning) (PTSFS 2016:5)

- General advice on occupational health and safety on warships (TSFS 2011:91)
- Regulations on Vehicles and Trailers Towed by Vehicles (TSFS 2016:22)
- The Swedish Transport Agency's regulations on marine equipment (Transportstyrelsens föreskrifter om marin utrustning) (TSFS 2016:81)
- The Swedish Transport Agency's regulations and general advice on operating an approved airport (Transportstyrelsens föreskrifter och allmänna råd om drift av godkänd flygplats) (TSFS 2019:19)
- DEF STAN 00-055 Requirements for Safety of Programmable Elements (PE), Software etc in Defence Systems (series)
- DEF STAN 00-056:Part 1 Safety Management Requirements for Defence Systems, Issue 7, 2017 (UK)
- DEF STAN 00-251:Part 3 Human Factors Integration for Defence Systems: Human Factors System Requirements, 2016 (UK)
- DO-178C/ED-12C Software Considerations in Airborne Systems and Equipment Certification, 2012
- DO-254/ED-80 (Design Assurance Guidance for Airborne Electronic Hardware, (Functions that are allocated to hardware), 2016
- Integration of human factors in defence systems (Integration av humanfaktorer i försvarssystem, 2018) (FSD 9251)
- GEIA-STD-0010A Standard Best Practice for System Safety Program Development and Execution, 2015
- Medical Electrical Equipment and Systems (IEC 60601) (series)
- Reliability of electrical/electronic/programmable electronic safety-related systems (IEC 61508) (series)
- Medical electrical equipment (IEC 80601 / ISO 80601) (series)
- ISO/IEC/IEEE 15288 Systems and software engineering - System life cycle processes
- MIL-STD-882E Department of Defence Standard Practise System Safety, 2012
- MIL-STD-1472H Department of Defence Design Criteria Standard, Human Engineering, 2020
- MIL-STD-46855A Department of Defence Standard Practice: Human Engineering Requirements for Military Systems, Equipment and Facilities, 2011
- SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems, 2010
- SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996
- Maritime navigation and radio communication equipment and systems - General requirements - Methods of testing and required test results (SS-EN 60945)
- Reliability of electrical/electronic/programmable electronic safety-related systems (SS-EN 61508) (series)
- Safety of machinery - Electrical equipment of machines - Part 1: General requirements (SS-EN IEC 60204-1)
- Safety of machinery - General principles for design - Risk assessment and risk reduction (SS-EN ISO 12100:2010)
- Safety of machinery - Emergency stop function - Principles for design (ISO 13850:2015)

- Medical devices - Application of risk management to medical devices (ISO 14971:2020)
- Technical documentation - Classification of requirements on manufacturing documentation (SS 2222)
- STANAG 2310 Technical Performance Specification Providing for the Interchangeability of 7.62 mm x 51 Ammunition, 2020
- STANAG 4297/AOP-15 Guidance on the Assessment of the Safety and Suitability for Service of Non-Nuclear Munitions for Nato Armed Forces, 2001
- STANAG 4518, edition 1 Safe disposal of munitions, design principles and requirements and safety assessment, 2001
- BAAINBw, System Safety Demonstration Handbook (01/04/2014), Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (Germany)
- FMV Handbook EMMA (Electromagnetic Environment Handbook, EMMA)
- Vehicle Safety Handbook (H FordonSäk E)
- Handbook on Software in Safety Critical Applications (H ProgSäk E)
- Handbook Safe Field-Based Workplaces (H SäkFältmArb E)
- Handbook Safe electrical products and systems (H SEPS)
- Weapons and Ammunition Safety Handbook (H VAS E)
- The Swedish Rescue Services Agency Handbook for risk analysis (Räddningsverket Handbok för riskanalys) (Utgivningsår 2003, Beställningsnummer: U 30-626/02, ISBN 91-7253-178-9)
- SEES Handbok Miljötålighetsteknik (Swedish Environmental Engineering Society, Environmental Engineering Handbook)

Sources within the Swedish Armed Forces

- The Swedish Armed Forces' decision-making system for technical systems (FM BMTS), FM2017-22065:1
- Collaboration Agreement SAMO (FM–FMV) FM2019-4243:4, 19FMV5660-1:1

Regulatory Control that Affected the Content of this Handbook

- The Swedish Armed Forces regulations on military air traffic (FFS Försvarsmaktens föreskrifter om militär luftfart) (FFS 2019:10)
- Handbook goal setting for units (Handbok Målsättningsarbete förband 2011, gällande från och med 2011-01-01)
- Handbook goal setting for technical systems (Handbok Målsättningsarbete Tekniska system 2015, gällande från och med 2015-04-01)
- Handbook governing documents and handbooks (Handbok Styrande dokument och handböcker 2021, gällande från och med 2021-11-01)
- Handbook disposal of equipment (Handbok Förnödenhetsavveckling 1997, gällande från och med 1997-10-01)
- Handbook Storage and transport of ammunition and other explosive goods, part 1 (Handbok Förvaring och transport av ammunition och övriga explosiva varor del 1 2011, gällande från och med 2011-01-01)
- Handbook Measures against the risk of fire and explosion, water pollution and chemical health effects from flammable goods (Handbok Åtgärder mot brand- och

explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor 2014, gällande från och med 2014-09-01)

The Swedish Armed Forces must meet requirements for work environment and safety for its personnel as well as safety for third parties, property and external environment. The materiel must comply with the legislation and at the same time meet the required performance.

The Swedish Armed Forces' system safety activities aim to ensure that the accident risks in operations are kept as low as possible. In order to ensure this, system safety requirements must exist for equipment that is acquired or modified.

The handbook describes the Swedish Armed Forces' process from goal setting to disposal as well as describes other participants´ system safety work.

FÖRSVARSMAKTEN

107 85 Stockholm
www.forsvarsmakten.se

H SYSTSÄKE 2022
M7739-352031
Versionsnr: 3.0 Ä0