

**Armed Forces' Handbook on  
System Safety 2011  
Part 2 – Methods**

**H SystSäk E**

Armed Forces  
Headquarter

2011-10-31

14 910:66344

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

At the same time the 1996 edition of H SystSäkE, M7740-784861, as established with HKV April 20, 1998 14 910:72214, is withdrawn.

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

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

Anders Emanuelson  
Head of Swedish Armed Forces  
Safety Inspectorate

Arne Börtemark

The handbook is published in cooperation with **Sörman Information AB**  
Division: The Armed Forces' Security Inspectorate and Swedish Defence Materiel Administration  
Editor: Mats Lundgren  
**M7739-352032 H SYSTSÄK E D2**

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

## Table of Content

<b>1</b>	<b>Requirements</b>	
1.1	Basics .....	11
1.2	Requirements Numbering .....	12
1.3	Significance of Requirement Level.....	13
<b>2</b>	<b>Material Requirements</b>	
2.1	Design .....	15
2.2	Manufacturing .....	17
2.3	Maintenance .....	19
2.4	Decommissioning .....	19
<b>3</b>	<b>System Safety Activities</b>	
3.1	Requirements for System Safety Activities .....	21
3.2	Selection of Activities (Tailoring) .....	23
	The Selection of Activities .....	23
	Links between Activities.....	25
	Choice of Management-Related System Safety Activities.....	27
	Choice of Requirements for Management Activities.....	27
	Choice of Analytical Methods .....	28
	Choice of Activities for Study Assignments .....	30
	Choice of Activities for Development Assignments.....	30
	Choice of Activities in the Procurement of COTS.....	33
	Choice of Activities for RENO/REMO/HTM .....	34
	Choice of Activities for Adjustment Measures.....	35
	Choice of Activities Prior to Disposal.....	35
	Choice of Activities for the Development of Alternative Repair Methods .....	36
	Choice of Activities for Temporary Repairs and War Damage Repair.....	36
	Choice of Activities for Communication Systems .....	37
	Choice of Activities for Expert Systems .....	37
	Choice of Activities for Training Materials .....	37
<b>4</b>	<b>H SystSäk E and MIL-STD-882C</b>	
4.1	General Interpretation and Guidance for MIL-STD-882C.....	39
4.2	General Description of the Activities in H SystSäk E .....	41
4.3	Overview of all System Safety Activities .....	43
<b>5</b>	<b>Description of Activities</b>	
5.1	System Safety Program (SSP) – Task 101.....	45
	Purpose .....	45
	Deviations .....	45
	Comparable Activities/Documents .....	46
	Further Information .....	46
	Input Data.....	46
	Output Data.....	47

5.2	System Safety Evaluation (SSE) – S10 .....	48
	Purpose .....	48
	Activity Description.....	48
	Input Data.....	49
	Output Data.....	50
5.3	System Safety Requirements in TTEM – S11 .....	51
	Purpose .....	51
	Activity Description.....	51
	Input Data.....	51
	Output Data.....	52
5.4	Determining Requirements for Tender Enquiry (RFP) – S12 ....	53
	Purpose .....	53
	Activity Description.....	53
	Input Data.....	58
	Output Data.....	58
	As Low As Reasonably Practicable (ALARP) .....	59
5.5	System Safety Program Plan (SSPP) – Task 102 .....	60
	Purpose .....	60
	Deviations .....	60
	Comparable Activities/Documents.....	60
	Further Information .....	60
	Input Data.....	61
	Output Data.....	61
5.6	Integration/Management of Subcontractors (IMSC) –	
	Task 103 .....	62
	Purpose .....	62
	Deviations .....	62
	Comparable Activities/Documents.....	62
	Further Information .....	62
	Input Data.....	63
	Output Data.....	63
5.7	System Safety Program Reviews/Audits (SSPR) – Task 104 .....	64
	Purpose .....	64
	Deviations .....	64
	Comparable Activities/Documents.....	64
	Further Information .....	64
	Input Data.....	65
	Output Data.....	65
5.8	System Safety Working Group (SSWG) – Task 105 .....	66
	Purpose .....	66
	Deviations .....	66
	Comparable Activities/Documents.....	66
	Further Information .....	67
	Input Data.....	67
	Output Data.....	68

5.9	Hazard Tracking and Risk Resolution (HTRR) – Task 106 .....	69
	Purpose .....	69
	Deviations .....	69
	Comparable Activities/Documents .....	69
	Further Information .....	69
	Input Data.....	70
	Output Data.....	70
5.10	System Safety Progress Summary (SSPS) – Task 107.....	71
	Purpose .....	71
	Deviations .....	71
	Comparable Activities/Documents .....	71
	Further Information .....	71
	Input Data.....	71
	Output Data.....	72
5.11	Safety Critical Functions (SCF) – S13 .....	73
	Purpose .....	73
	Activity Description .....	73
	Input Data.....	78
	Output Data.....	78
5.12	Preliminary Hazard List (PHL) – Task 201 .....	79
	Purpose .....	79
	Deviations .....	79
	Comparable Activities/Documents .....	79
	Further Information .....	79
	Input Data.....	80
	Output Data.....	80
5.13	Preliminary Hazard Analysis (PHA) – Task 202.....	81
	Purpose .....	81
	Deviations .....	81
	Comparable Activities/Documents .....	81
	Further Information .....	81
	Input Data.....	82
	Output Data.....	82
5.14	Safety Requirements/Criteria Analysis (SRCA) – Task 203.....	83
	Purpose .....	83
	Deviations .....	83
	Comparable Activities/Documents .....	83
	Further Information .....	83
	Input Data.....	84
	Output Data.....	84
5.15	Subsystem Hazard Analysis (SSHA) – Task 204.....	85
	Purpose .....	85
	Deviations .....	85
	Comparable Activities/Documents .....	85
	Further Information .....	86
	Input Data.....	86
	Output Data.....	86

5.16	System Hazard Analysis (SHA) – Task 205 .....	87
	Purpose .....	87
	Deviations .....	87
	Comparable Activities/Documents.....	87
	Further Information .....	88
	Input Data.....	88
	Output Data.....	89
5.17	Operating and Support Hazard Analysis (O&SHA) – Task 206 .....	90
	Purpose .....	90
	Deviations .....	90
	Comparable Activities/Documents.....	90
	Further Information .....	91
	Input Data.....	91
	Output Data.....	92
5.18	Health Hazard Assessment (HHA) – Task 207.....	93
	Purpose .....	93
	Deviations .....	93
	Comparable Activities/Documents.....	93
	Further Information .....	94
	Input Data.....	95
	Output Data.....	95
5.19	Risk Analysis for External Environment (EHA) – S21 .....	96
	Purpose .....	96
	Activity Description.....	96
	Input Data.....	100
	Output Data.....	100
5.20	Functional Hazard Assessment (FHA) – S22 .....	101
	Purpose .....	101
	Activity Description.....	102
	Input Data.....	103
	Output Data.....	103
	FHA for Civil Airborne Systems .....	104
	Purpose .....	104
	Activity Description.....	105
	Input Data.....	106
	Output Data.....	107
5.21	Safety Assessment Report (SAR) – Task 301 .....	107
	Purpose .....	107
	Deviations .....	107
	Comparable Activities/Documents.....	108
	Further Information .....	108
	Input Data.....	108
	Output Data.....	109
5.22	Test and Evaluation Safety – Task 302.....	109

5.23	Safety Review (SR) – Task 303.....	110
	Purpose .....	110
	Deviations .....	110
	Comparable Activities/Documents .....	110
	Further Information .....	110
	Input Data.....	111
	Output Data.....	111
5.24	Safety Verification (SV) – Task 401.....	112
	Purpose .....	112
	Deviations .....	112
	Comparable Activities/Documents .....	112
	Further Information .....	112
	Input Data.....	113
	Output Data.....	113
5.25	Safety Instructions (SI) – S41 .....	114
	Purpose .....	114
	Activity Description .....	114
	Input Data.....	115
	Output Data.....	115
5.26	Safety Compliance Assessment – Task 402.....	116
5.27	Safety Compliance Assessment (SCA) – S42 .....	116
	Purpose .....	116
	Activity Description .....	116
	Input Data.....	118
	Output Data.....	119
5.28	Failure Reporting, Analysis and Corrective Action System (FRACAS) – S43 .....	120
	Purpose .....	120
	Activity Description .....	120
	The resulting report.....	122
	Input Data.....	123
	Output Data.....	123
5.29	Explosive Hazard Classification and Characteristics – Task 403 .....	124
5.30	Explosive Ordnance Disposal Source Data – Task 404 .....	124
5.31	Safety Statement (SS) – S51 .....	124
	Purpose .....	124
	Activity Description .....	125
	Input Data.....	129
	Output Data.....	130
5.32	Training Safety Regulations (TSR) .....	131
	Purpose .....	131
	Activity Description .....	131
	Input Data.....	133
	Output Data.....	134

## Table of Content

5.33	Central Safety Compliance Decision (CSSB) – S53 .....	135
	Purpose .....	135
	Activity Description.....	135
	Input Data.....	136
	Output Data.....	136
5.34	Risk Assessment prior to Disposal of System (RADS).....	137
	Purpose .....	137
	Activity Description.....	137
	Input Data.....	140
	Output Data.....	141
<b>6</b>	<b>Software Safety</b>	
6.1	General.....	143
6.2	Software Features.....	143
6.3	Safety Requirements for Software.....	146
6.4	Verification of Software .....	148
<b>7</b>	<b>Checklist for Materiel Requirements and Activities</b>	
<b>8</b>	<b>System Safety Analysis</b>	
8.1	Principles for System Safety Analyses .....	153
8.2	Fault Tree Analysis (FTA) .....	155
	Qualitative Fault Tree Analyses.....	156
	Qualitative Fault Tree Analyses.....	158
8.3	Fault Modes and Effects Analysis (FMEA) .....	161
	Qualitative Fault Modes and Effects Analyses.....	162
	Qualitative Fault Modes and Effects Analyses.....	162
8.4	Event Tree Analysis (ETA) .....	164
8.5	Hazard and Operability (HAZOP) Study .....	166
	<b>Appendix 1 Examples of Decision Documents.....</b>	<b>169</b>
	<b>Definitions .....</b>	<b>187</b>
	<b>Acronyms/Abbreviations .....</b>	<b>201</b>
	<b>References .....</b>	<b>209</b>



## PREFACE

*H SystSäk E Part 2 – Methods* – contains all of the system safety activities that are considered suitable to be used during all phases of a technical system's lifetime. Most of these activities are taken from MIL-STD-882C and interpretations and clarifications are made here regarding when and how they should be applied. A full description can only be found in MIL-STD-882C, which is on H SystSäk CDR. In addition, there are unique Swedish materiel requirements and activities which are fully described here in part 2 of *H SystSäk E*. In order to facilitate joint studies of documents, the standard English names for each activity are used, both in the running text and in the titles and contents.

These regulations apply specifically to part 2. For *H SystSäk E* in general, see the preface in part 1.



# 1

## REQUIREMENTS

### 1.1 BASICS

*Chapter 2* and *3* indicate the material requirements and system safety activities that are common to most technical systems. These activities should be selected carefully to achieve an acceptable level of safety. The concept system refers to the technical system in the handbook and the concept risk relates to the accident risks.

The requirements are divided up into the systems' different phases during their service life.

During its lifetime, a technical system can produce various accident risks during storage, transportation, handling, use, maintenance and decommissioning. Risks are limited during the design and construction stages through the adoption of design measures (analyses, redesign, etc.) and production measures (e.g. quality control).

However, certain accident risks can remain after manufacture. These may include sound pressure, thermal radiation or vibrations. These accident risks must be limited through warnings, safety instructions and training in proper handling.

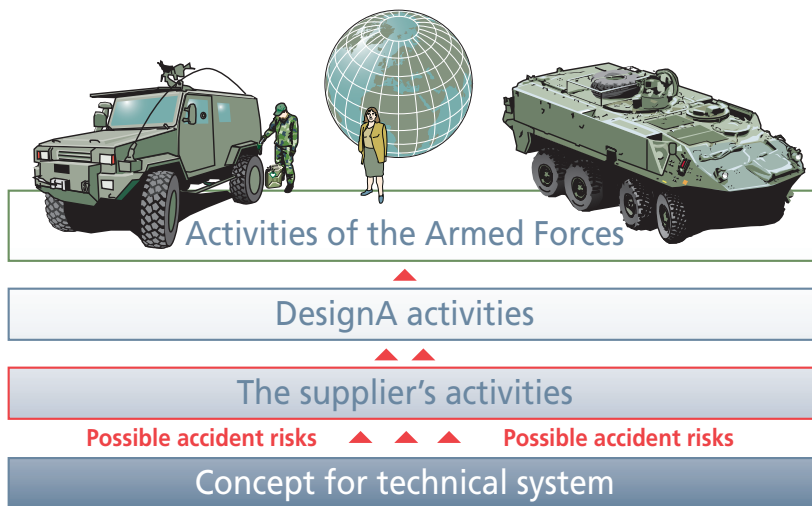


Figure 1:1 System Safety Activities

System safety activities can basically be described as shown in figure 1:1 where all parties involved, such as developers, manufacturers, designers and users, assume their responsibilities and contribute to the prevention of accidents from happening.

The purpose of these activities is to include the requirements in terms of system safety that have been established for technical systems relating to people, property and the external environment.

## 1.2 REQUIREMENTS NUMBERING

The requirements are either mandatory (in bold and with a dark-blue background) or optional (light-blue background).

For the optional requirements, a selection is only made if they are considered relevant to a particular technical system, whereby they are indicated in the requirements specification/system safety plan/quality plan (ISO 9001, [28])/environmental management plan (ISO 14001, [31]) or equivalent.

H SystSäk E includes a number of requirements and operational performance and materiel features. The requirements are intended to be used for procurement purposes, tenders and contracts.

The starting number for a specific requirement specifies where the requirement is derived from, for example, 0 indicates that the requirement is from H SystSäk E Part 2.

The two digits that follow indicate the chapter, for example, 31 indicates that the requirement is from chapter 3, section 1. Finally, there is a serial number that corresponds to each section. For example, the numbers 0.31.001 relate to the first requirement in chapter 3, section 1 of the H SystSäk E Part 2.

The initial numbers are broken down as follows:

- 0 H SystSäk E Part 2
- 1 H VAS-E (Weapons and Ammunition Safety Manual) [24]
- 2 H SystSäk E Part 1
- 3 H FordonSäk (FMV Handbook on Vehicle Safety) [21]
- 6 H ProgSäkE (FM Handbook on Software in Safety-critical Applications) [18]

### 1.3 SIGNIFICANCE OF REQUIREMENT LEVEL

The Armed Forces, as the client, is also the standards authority. When DesignA receives an order from the Armed Forces, DesignA is also the organization that places the order and the standards authority. The handbook's requirements are divided into mandatory and optional requirements. It is for the standards authority that the concepts of mandatory/optional form part of the instruction.

The mandatory requirements are essential for system safety. To comply with laws, regulations and ordinances with an emphasis on system safety activities, all mandatory requirements must be met. If a mandatory requirement cannot be met for tactical reasons or cost reasons, for example, a deviation can be tolerated if it can be shown that an acceptable level of safety can still be maintained. The decision basis for this deviation must be documented.

## 1 Requirements

A control of the system safety activities to be implemented for the technical system by the players in question is described in the Armed Forces' requirements, for example in TTEM, see 5.3. This takes place even if DesignA describes the requirements in the tender enquiry (RFP, see 5.4).

The supplier's system safety plan will describe which activities it intends to perform and the level of ambition.

Please note that the scope of activities should always be adapted to the technical complexity of the system and the demands made on system safety.

For further guidance, see *section 3.2, Selection of Activities (Tailoring)*.

# 2

## MATERIEL REQUIREMENTS

### 2.1 DESIGN

Before the development or procurement of a technical system, the system safety requirements must be defined and documented in the relevant requirements documentation. The system safety requirements that are applicable to the majority of the technical systems are specified below.

Numbering requirements are indicated in *section 1.2*.

Table 2:1 Requirements List

0.21.001	Technical systems should be designed so that safety requirements do not need to be applied for transportation, storage, handling, maintenance, operation and decommissioning. Conditions under which a design solution may be replaced by protective devices, warning systems and training should be regulated, preferably in a System Safety Program Plan (SSPP), see 5.5. See also Safety Instructions (SI) 5.25 and Test and Safety Regulations (TSR) 5.32.
0.21.002	Technical systems must be designed so that single faults do not lead to a hazardous event, unless the likelihood of a hazardous event can be shown to be acceptably low and/or the consequences of a hazardous event can be accepted. For details of a specified requirements risk see the <i>requirements specification</i> or equivalent.
0.21.003	Technical systems should be designed so that the failure of two or more components due to a common cause do not result in a hazardous event, unless the consequence of the hazardous event can be accepted.

- 0.21.004 The design should be able to withstand the abnormal environments that may arise, for example, in the case of accidents and a hostile attack, so that the current design does not increase the technical system's overall vulnerability.
- 0.21.005 A property or component that directly affects the safety (for example, single fault) of the technical system is classified as a safety-critical feature/part. Each characteristic/component should be listed in the product documentation. Deviation from this property or the failure of this component is classified as a critical error, see Safety Critical Functions (SCF) 5.11.
- 0.21.006 A feature or component that affects the safety (for example double faults or faults of a higher order) of the technical system is classified as a safety-related feature/component. Each feature/component should be listed in the product documentation. A deviation from this feature or the failure of this component is classified as major fault, see 5.11).
- 0.21.007 Basic requirements, as described in *chapter 1* must be satisfied by safety-critical software. (The basic requirements are quality requirements for all types of software, both critical and non-critical.)
- 0.21.008 The selection of safety requirements, as described in *chapter 1*, relevant to the safety-critical software in the technology system in question, must be satisfied. The selection will relate to all software parts in the technical system and reflect the highest criticality, unless independence between parts of different criticality can be shown. A selection per criticality partition is allowed for software parts, where independence between elements of different criticality levels can be shown.



- 0.21.009 In order to facilitate the sale of technical systems when decommissioning, exemptions from laws should be made and specific military solutions should be avoided. For components and subsystems that form a part of the technical system CE marking should also be considered (CE marking cannot be done on specific military technical systems as a whole).
- 0.21.010 Bonding methods to prevent dismantling should not be used
- 0.21.011 The identification of plastic materials should be done by labelling the product/component.

## 2.2 MANUFACTURING

Any shortcoming (deficiency) or fault that may cause a hazardous event or hazardous condition must be identified during development. A shortcoming that may arise during manufacture, and which can contribute to a hazardous event or hazardous condition, must be avoided through careful production management and quality assurance.

Table 2:2 Requirements List

- 0.22.001** Production control and general inspection of all characteristics that can lead to critical faults should be made, see SCF 5.11.  
 Comment: There are certain characteristics that cannot be controlled completely due to the fact that destructive testing must be applied. In these instances, the probability of a fault arising in production control is minimal.
- 0.22.002 Production control and a general inspection of all characteristics that can lead to a major fault must be carried out, see SCF 5.11.

- 0.22.003** When checking the characteristics that can lead to major faults, equipment should be used to detect defective parts and prevent them from passing the testing station (inspection point), see 5.11.  
Comment: Automatic test equipment can be used for this type of inspection. In instances where automatic testing equipment is not available, inspection must be repeated to provide the desired effect.
- 0.22004** Verification of characteristics that can lead to a major fault should be performed in the same way as a critical fault, see 5.11.  
Comment: The inspection can be carried out by using automatic testing equipment.
- 0.22.005** Testing equipment must be inspected and calibrated at regular intervals.  
Comment: See calibration systems in accordance with guidelines in SS-EN ISO 9001 [28].
- 0.22.006** The manufacturing process must separate the defective units in an effective way.  
Comment: Defective units must be separated from correct units. The defective units must be marked where possible. See guidelines in SS-EN ISO 9001 [28].

## 2.3 MAINTENANCE

A hazardous event or a hazardous condition that may arise due to a lack of maintenance or incorrectly performed maintenance should be avoided through careful Integrated Logistic Support (ILS) activities.

Table 2:3 Requirements List

- |          |                                                                                                                                                                                                                      |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0.23.001 | A technical system's safety should not depend on specific maintenance procedures.<br>Comment: If maintenance procedures are needed to maintain safety they should be part of planned regular maintenance activities. |
| 0.23.002 | The safety of a technical system will not worsen after performed maintenance.                                                                                                                                        |

## 2.4 DECOMMISSIONING

A hazardous event or hazardous condition that can occur during decommissioning must be avoided through, among other things, risk analysis of the decommissioning operations.

Table 2:4 Requirements List

- |          |                                                                       |
|----------|-----------------------------------------------------------------------|
| 0.24.001 | Requirements for reuse and the degree of recycling should be defined. |
|----------|-----------------------------------------------------------------------|



# 3

## SYSTEM SAFETY ACTIVITIES

### 3.1 REQUIREMENTS FOR SYSTEM SAFETY ACTIVITIES

This section specifies the activity requirements that are relevant for most of the technical systems. The system safety activities are applied during the various phases in the life cycle of a technical system in accordance with *section 3.2*.

The numbers of the requirements are indicated in *section 1.2*.

Table 3:1 Requirements List

0.31.001	System Safety Program (SSP) – Task 101 will be implemented in accordance with <i>section 5.1</i> .
0.31.002	System Safety Evaluation (SSE) – S10 should be implemented in accordance with <i>section 5.2</i> .
0.31.003	System Safety Requirements in Tactical Technical Financial Objectives (TTEM) – S11 shall be compiled in accordance with <i>section 5.3</i> .
0.31.004	System Safety Requirements for the RFP – S12 shall be established in accordance with <i>section 5.4</i> .
0.31.005	System Safety Program Plan (SSPP) – Task 102 shall be established in accordance with <i>section 5.5</i> .
0.31.006	Integration/Management of Subcontractors (IMSC) – Task 103 is carried out in accordance with <i>section 5.6</i> .
0.31.007	System Safety Program Reviews/Audits (SSPR) – Task 104 is to take place in accordance with <i>section 5.7</i> .
0.31.008	System Safety Working Group (SSWG) Support – Task 105 is to be established in accordance with <i>section 5.8</i> .

- 0.31.009 Hazard Tracking and Resolution (HTRR) – Task 106 is to be implemented in accordance with *section 5.9*.
- 0.31.010 System Safety Progress Summary (SSPS) – Task 107 shall be established in accordance with *section 5.10*.
- 0.31.011 Safety Critical Functions (SCF) – S13 shall be implemented in accordance with *section 5.11*.**
- 0.31.012 Preliminary Hazard List (PHL) – Task 201 is to be implemented in accordance with *section 5.12*.
- 0.31.013 Preliminary Hazard Analysis (PHA) – Task 202 is to be implemented in accordance with *section 5.13*.
- 0.31.014 Safety Requirement Criteria Analysis (SRCA) – Task 203 is to be implemented in accordance with *section 5.14*.
- 0.31.015 Preliminary Hazard Analysis (PHA) – Task 204 is to be implemented in accordance with *section 5.15*.
- 0.31.016 System Hazard Analysis (SHA) – Task 205 is to be implemented in accordance with *section 5.16*.
- 0.31.017 Operating and Support Hazard Analysis (O&SHA) – Task 206 is to be implemented in accordance with *section 5.17*.
- 0.31.018 Health Hazard Assessment (HHA) – Task 207 is to be implemented in accordance with *section 5.18*.
- 0.31.019 Risk analysis for the external environment (EHA) – S21 is to be implemented in accordance with *section 5.19*.
- 0.31.020 Functional Hazard Assessment (FHA) – S22 is to be implemented in accordance with *section 5.20*.
- 0.31.021 Safety Assessment Report (SAR) – Task 301 is to be established in accordance with *section 5.21*.
- 0.31.022 Safety Review (SR) – Task 303 is to be implemented in accordance with *section 5.23*.

- 0.31.023 Safety Verification (SV) – Task 401 is to be implemented in accordance with *section 5.24*.
- 0.31.024 Safety Instructions (SI) – S41 is to be designed in accordance with *section 5.24*.
- 0.31.025 Safety Compliance Assessment (SCA) – S42 is to be established in accordance with *section 5.27*.
- 0.31.026 Failure Reporting Analysis and Corrective Action System (FRACAS) – S43 is to be established in accordance with *section 5.28*.
- 0.31.027 Safety Statement (SS) – S51 is to be compiled in accordance with *section 5.31*.
- 0.31.028 Test and Safety Regulations (TSR) – S52 should be established under *section 5.32*.
- 0.31.029 Central Safety Compliance Decision (CSSB) – S53 is to be compiled under *section 5.33*.
- 0.31.030 Risk Assessment at the Disposal of System (RADS) – S61 shall be implemented in accordance *section 5.34*.

### 3.2 SELECTION OF ACTIVITIES (TAILORING)

This section provides instructions for selecting and implementing the various activities that constitute a base for system safety activities.

#### 3.2.1 The Selection of Activities

---

The system safety activity to be conducted for a technical system must be adapted based on the hazards/hazardous conditions the technical system is considered to possess and what the potential risk of an accident occurring is as a result of this. In principle, all activities in accordance with *figure 3:1* are always included in system safety activities even if no activity can be ruled out after careful consideration.

In cases where regulatory requirements in the form of legislation and/or norms and standards are available, for certain technical systems it may form the basis for certain activities to be deselected.

*Table 3:2* is an example of a choice of activities. *Table 4:1* provides guidance as to which stage the various activities are appropriately applied. The client specifies the activities that the supplier will implement and the system safety documents to be delivered, and when this will happen.

The scope of each ordered activity may be adapted by the supplier (to avoid unnecessary costs).

Note that regulatory requirements are sometimes more comprehensive than the requirements in the handbook, see *H SystSäk E Part 1*.

The selection and scope of the activities must often be discussed between the Armed Forces, DesignA and the supplier in question. When an activity has been selected and the scope has been agreed, this is documented in the System Safety Program Plan (SSPP 5.5).

If the technical system contains arms and ammunition, or another product with an explosive device, more activities will be included as described in H VAS-E [24]. The same applies for vehicles and vessels/submarines, see also *H SystSäk E Part 1*.

For the acquisition of COTS, which is intended to be used independently of other technical system, and in accordance with the supplier's operating description, at the tender stage it is usually sufficient to request current safety data sheets and the risk analysis that form the basis for possible CE marking. On acquisition of a complete technological system, a Safety Assessment Report (SAR) 5.21 and Safety Compliance Assessment (SCA) 5.27 must be included at the tender stage. On development of a technical system, with or without integrated COTS, the *H SystSäk E* must be applied in its entirety, see also *H SystSäk E Part 1, section 5.6*.



System safety activities can be divided into activity management, requirements management and risk management. Each part is to be individually adapted with regard to the potential suppliers' experience in system safety activities and, based on the technical system's degree of utilization, of known technology and methods of use. For each activity, documentation from the specified activity is required.

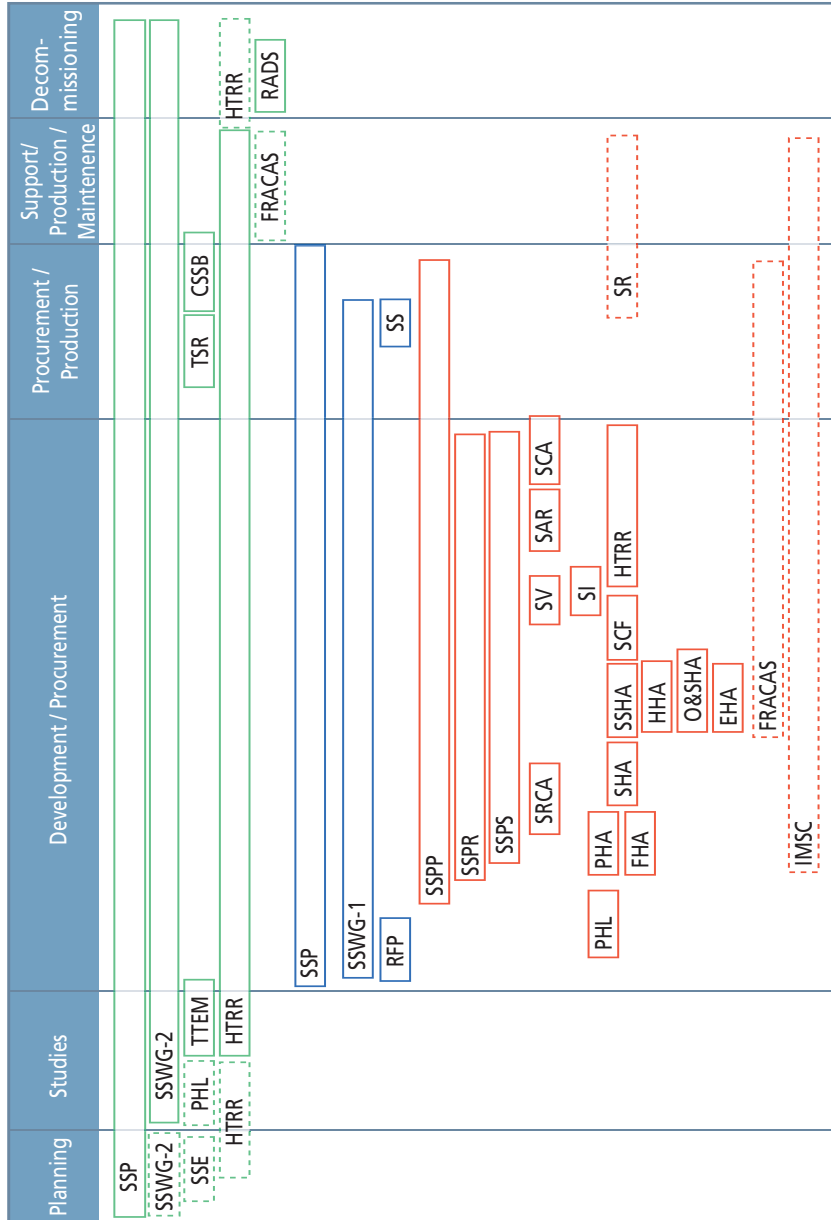
### 3.2.2 Links between Activities

---

From the graphs below (*figure 3:1*) the relationships between the different activities are shown. The graphs also indicate who carries out the particular activities and when they can be carried out. The selection of activities and choice of ambition must be adapted to the technical system's potential risk level.

The significance of the design of the frame around a particular activity.

Broken	Selectively Applicable
Solid	Generally Applicable



Armed Forces activities marked with green, DesignA's activities marked with blue and Supplier's activities marked with red.

Figure 3:1 System Safety Activities – Connection

### 3.2.3 Choice of Management-Related System Safety Activities

The system safety activities are regulated by the following governing documents: System Safety Management Plan (SSMP) and SSPP and through IMSC activities.

The observance of the system safety activities are managed and controlled by System Safety Working Groups 1 and 2: SSWG-1, SSWG-2, and System Safety Program Review (SSPR).

The supplier's continuous reporting takes place via a System Safety Progress Summary (SSPS).

After the activities are completed, business commitments are declared and requirements are fulfilled in terms of SCA, Safety Statement (SS) and Central Safety Compliance Decision (CSSB). SAR is used as a basis for SCA.

For technical systems that may be associated with the risk of an accident, it is necessary that there is always a minimum of SSPP, SCA, SS and CSSB activities implemented.

### 3.2.4 Choice of Requirements for Management Activities

Requirements management is done through Tactical-Technical-Financial Objectives (TTEM), RFP, SRCA and SV. The operational requirements of TTEM are transformed and supplemented in the RFP to function-oriented requirements. RFP makes up a part of the invitation to tender to be responded to by the supplier. The supplier carries out the SRCA in order to supplement, detail and break down requirements into design requirements.

The part that is made up of requirements for activities is generated through the System Safety Program (SSP) and is documented in the SSMP, which is derived from the RFP. These are supplemented and specified in the SSPP.

For technical systems that may be associated with the risk of an accident it is necessary that there is always a minimum of TTEM, RFP, SRCA and SV activities implemented.

### 3.2.5 Choice of Analytical Methods

---

Analysis activities are intended to identify and analyse the causes of potential accident risks. This is done through PHL, PHA and FHA. After identification, the underlying causes of the accident risks are analysed. This can be done with the continued analysis activities in the form of SHA, SSHA, O&SHA, HHA and EHA. Before disposal, a parallel analysis with RADS takes place. Once the causes have been identified, they must be eliminated or reduced so that the requirement standards to counteract the risk of an accident occurring for the technical system are maintained. All identified risks of accidents and mitigation measures are documented in Hazard Tracking and Risk Resolution (HTRR).

From the analysis, it is important to identify how critical the information system's various features and elements are. This identification and subsequent actions are governed by Safety Critical Functions (SCF). When there are changes in design or deviations in the critical features/components the Safety Review (SR) must be applied.

If the risk-reducing measures consist of warnings or other safety regulations, Safety Instructions (SI) and Test and Safety Regulations (TSR) will apply.

If errors occur during use or testing, Failure Reporting, Analysis and Corrective Action (FRACAS) should be used. If these errors are safety related they must be documented in accordance with Hazard Tracking and Risk Resolution (HTRR) for further action as per SSWG.

Whichever of the above activities is to be applied it must be adapted to the technical system in question. *Table 3:2*, below, provides guidance as to how this can be done for various applications and procurement assignments. The left column (Application) describes activities or situations and the cross indicates the analytical technique/activity that is most applicable.

Table 3:2 Applications

Analysis technique/Activity	SSE S10	PHL 201	PHA 202	FHA S22	SRCA 203	SSHA 204	SHA 205	O&SHA 206	HHA 207	EHA S21	RADS S61	SAR 301
Completed technical systems												x
Concept studies	x											
System description		x	x	x	x	x	x	x	x	x		
System analyses		x	x	x	x	x	x	x	x	x		
Hazards/Hazardous conditions		x										
Hazardous event			x									
Functional analyses				x								
Requirements analyses					x							
Subsystem analyses						x						
Interactions							x					
Operative phases								x				
System events			x			x	x					
User instructions								x			x	
Identification of hazardous substances		x	x						x	x		
Identification of risks with hazardous substances						x	x	x	x	x	x	
Identification of hazardous events for users			x					x	x		x	
Effect of hazardous event			x			x	x	x	x	x	x	
Risk evaluation	x		x	x		x	x	x	x	x	x	
Effect of planned action		x	x	x	x	x	x	x	x	x		
Impact of measures introduced			x			x	x	x	x	x		
Outcome (fault) of similar technical systems		x	x			x	x	x	x	x		
Changes			x			x	x	x	x	x	x	
Manuals								x			x	
Decommissioning											x	

### 3.2.6 Choice of Activities for Study Assignments

---

A study assignment usually occurs in the early stages of materiel procurement. The study assignment can include studies of different techniques, such as prototypes/demonstrators of technical systems. A study assignment does not include the production of series-like technical systems. The study assignment is normally initiated by the Armed Forces. The prototypes/demonstrators that are developed in conjunction with study activities can only be used to a minor extent by military units and will normally not be used in operations.

In the planning and study stage different concepts are compared so that during the development/acquisition phase they can be turned into a technical system. During these early stages the level of detail of the concepts may vary. The activities that are most relevant, from a system safety point of view, in order to evaluate different concepts, include the System Safety Evaluation (SSE) and the PHL. The other activities that should be pursued include the initialisation of system safety activities, SSP, and the formation of a work group for the control and monitoring of the overall system safety work, SSWG.

### 3.2.7 Choice of Activities for Development Assignments

---

Each development assignment is unique, so an adaptation must always be done so that the right activities are carried out at the right level. This means that the relevant activities must be selected and that the level of each activity must be adapted so that it covers the requirements in order to obtain an acceptable safe technical system.

In those instances when a study should precede the development, activities under *section 3.2.6* should also be implemented. In addition, the overall system safety requirements of the TTEM should be formulated and a risk follow-up system (HTRR) established for the technical system. This risk follow-up system should be used throughout the technical life of the system.

An SSWG-1 is to be established at DesignA. This group must return all information to the Armed Forces' SSWG-2. In practice, this can take place via the temporary fusion of these groups into one group.

DesignA formulates the system safety requirements from TTEM to requirements for RFP.

In connection with the supplier responding to the call for tenders, an analysis in the form of a PHL is often carried out in order to identify potential accident risks with the offered technical system. In the requirements specification which the supplier establishes, requirements must be inserted in order to verify that these accident risks are identified. Furthermore, additional system safety requirements, such as those governed by law, must be identified (SRCA) and included in the requirements specification. The range of activities that a supplier must implement in the development assignment must be described in the SSPP. A SSPP must be included in the tender documents from suppliers.

After the order is received the selected supplier usually establishes an internal working group on system safety issues, or participates in DesignA's SSWG-1. This group conducts assessments and attempts to deal with safety-related issues relevant to the project. More important issues can be taken up in the Armed Forces' SSWG-2. The supplier provides a report on developments in the agreed safety reports (SSPS).

The supplier responsible manages its subcontractors and partners through IMSC.

The actual risk analysis activities are carried out with the initial analyses (PHL, PHA, FHA) and are followed by the more in-depth analysis activities (SHA, SSHA, HHA, EHA and O&SHA).

The purpose of the PHL is to first identify all hazards/hazardous conditions in the technical system in order to remove or replace them with less dangerous hazards.

A deepening of the PHL is the PHA and the FHA, which are used to identify potential hazardous events which could then be further analysed to identify the root causes of these hazardous events. These root causes and dangerous conditions are looked into or eliminated through effective design changes.

As a result of risk analysis activities, critical characteristics and critical elements of the technical system (SCF) are identified. These critical or system safety-related features should be identified on the manufacturing documentation, such as drawings and specifications, in order to select an appropriate manufacturing method that ensures that as few as possible faults can be expected at the manufacturing stage.

All identified hazardous events and hazardous conditions with related accidents, and the measures taken and planned to manage the associated risks of accidents, should be managed via risk management activities (HTRR). A report of the risk follow-up should be made in supplier-intern work groups or in DesignA's SSWG-1 for the identification of suitable risk-reducing measures.

The agreed system safety activities are reviewed through audits such as normal quality audits or in SSPR, in accordance with the order. The result of the audits should be reported back to the SSWG-1.

If safety-related faults occur during testing these should be reported in accordance with agreed fault reporting system (FRA-CAS). The information in the fault reporting system is taken over by the Armed Forces from the supplier upon completion of development and production.

Restrictions on the use of a technical system must sometimes be introduced, based on:

- legislation/regulations
- risk-reducing measures.

Limitations imposed by SI also form the basis for the supplier's SCA and the basis for the Armed Forces' various instructions (TSR).

All system safety requirements from RFP and SRCA must be verified. This verification is described in the SV.



The results of the risk analysis activities (SHA, SSHA, HHA, EHA and O&SHA) and the SV, together with the SI, form the basis of the SAR.

The SAR collects all essential system safety-related information about the technical system. The system safety report forms the basis of the supplier's SCA, in which the supplier declares that the technical system is safe enough for use, subject to the SI being complied with.

The SCA forms the basis of DesignA's SS and the Armed Forces' CSSB.

After the technical production documentation has been completed, changes are reported according to the service change (included in SR where changes are described) in terms of the position taken by DesignA.

The above briefly describes the overall system safety activities during a development assignment. A number of activities will be conducted several times throughout the iteration process used during development. For technical systems with little impact in the event of an accident, not all activities need to be implemented as described above. The activities that usually need to be implemented include some form of early risk identification (PHL, PHA, FHA) a simple analysis at the subsystem level (SSHA) in the form, for example, of a fault effect analysis (FMECA), verification of system safety requirements (EN) and a SCA, which includes a summary of all system safety activities. Further, DesignA must issue a SS and the Armed Forces must issue a central CSSB.

### 3.2.8 Choice of Activities in the Procurement of COTS

In the acquisition of commercial products it is often difficult to obtain sufficient information on previously conducted risk analyses. Depending on how these products are to be used, they can be safety critical, see also *chapter 1* regarding software such as COTS.

If the product is planned to be used outside the scope of CE marking, formal analysis activities, such as PHA, FHA, SHA, SSHA, O&SHA, HHA and EHA, must be carried out. The results of the analysis work are to be reported in a SAR, which forms the basis for a SS and CSSB. In these instances, this activity should be performed by DesignA unless the supplier responsible can carry out the activity.

If the product is planned to be used outside the scope of CE marking, formal analysis activities, such as PHA, FHA, SHA, SSHA, O&SHA, HHA and EHA, must be carried out. The results of the analysis work are to be reported in a SAR, which forms the basis for a SS and CSSB. In these instances, this activity should be performed by DesignA unless the supplier responsible can carry out the activity.

When a COTS product is integrated into a technical system it must be regarded as a type of subsystem that can be used anywhere in the total technical system, and therefore activities should be applied, as with development assignments, in accordance with *section 3.2.7*. See also *H SystSäk E Part 1, section 5.8*.

#### 3.2.9 Choice of Activities for RENO/REMO/HTM

---

Renovation and modification can be very different for different technical systems. Therefore, it is difficult to give a general guideline when selecting appropriate activities. A safety assessment must always be carried out irrespective of whether the proposed measures have any impact on system safety or not. This safety assessment should be carried out by SSWG-2 as it has the knowledge and experience of the technical system in question. For a more extensive renovation/modification, activities such as those required for development assignments in accordance with *section 3.2.7* apply. If minor modifications are implemented, a system safety analysis must be made of the potential impact on other subsystems to determine if this may entail additional accident risks.

### 3.2.10 Choice of Activities for Adjustment Measures

---

If a change is needed, or in the event of a reported deviation, this should be done according to agreed procedures. Any proposed amendment and any reported deviation must be analysed and evaluated in terms of system safety. The methodology for this is described in the SR 5.23.

### 3.2.11 Choice of Activities Prior to Disposal

---

Before the disposal of a technical system any accident risks associated with the overall disposal process are identified and, if possible, eliminated. If the risks cannot be eliminated they must be resolved to an acceptable level in accordance with the Work Environment Authority's regulations. Disposal is usually performed by civilian personnel in civilian firms.

One of the activities related to disposal is the RADS. Its purpose is to systematically analyse a defined disposal process with regard to the inherent risks of accidents. If the technical system is relatively modern, that is to say that H SystSäk E has been applied during development/procurement of the system, there will be a lot of information already identified about the system's potential accident risks in connection with the planned disposal. This analysis is done as part of the regular analytical work. Similarly, the requirements specification in the TTEM and RFP have ensured that the technical system is specially designed to allow for safe and cost-effective disposal.

If the technical system has not been developed in accordance with the methodology set out in H SystSäk E, RADS must be fully applied. The methodology used by the activity RADS indicates that potentially hazardous materials contained in the technical system must be identified and safety measures taken if hazardous or environmentally harmful substances are found. In addition, the planned disposal process is analysed with regard to any risk of accidents directly related to the technical system, the disposal method, tools and waste products.

### 3.2.12 Choice of Activities for the Development of Alternative Repair Methods

---

Instructions for alternative repair methods are developed and processed continuously.

New ways are then developed as well as new components (replacement for original spare parts and used for repairs). The support documentation for the development of alternative repair methods can be shown from repairs already reported using unconventional methods. For the preparatory work, system safety activities in accordance with *section 3.2.7* are chosen. DesignA makes continuous decisions regarding alternative repair methods. Decisions are announced via a Technical Order (TO) which is followed up when the Technical Directive (TA) is published.

### 3.2.13 Choice of Activities for Temporary Repairs and War Damage Repair

---

The objective of temporary repair and war damage repair is to provide temporary help for operational damage or combat damage to the technical system, this is when time or resources for verified repair methods are lacking and to facilitate the resolution of an ongoing assignment.

**Temporary repairs** are usually applied only during international efforts, and the repairs must be acceptable from a system safety point of view.

**Battle damage repairs** are carried out only during war or warlike conditions. The primary objective of the repairs is to make the technical system usable after battle damage as quickly as possible.

Instructions for these types of actions are dealt with only in *H SystSäk E Part 1, section 5.11.3*.

### 3.2.14 Choice of Activities for Communication Systems

---

When communication systems are used to control devices which, in the event of a failure of communication or information transfer, can result in accidental events or dangerous conditions, the communication system should be considered as a component of the technical system and treated equally with other components in accordance with, for example, *section 3.2.7*.

### 3.2.15 Choice of Activities for Expert Systems

---

When expert systems are used in technical systems that may cause hazardous events or dangerous conditions, the expert system should be regarded as a component of the technical system and treated equally with other components in accordance with *section 3.2.7*. See also *H SystSäk E Part 1, section 5.10.7*.

### 3.2.16 Choice of Activities for Training Materials

---

For a device designed to simulate the functions of certain weapons/management systems, it is important to ensure that it adequately imitates the actual technical system. If not, errors and behaviour that affect safety may be developed. System safety work when procuring simulators should therefore focus on identifying such differences between the simulator and the actual system that can bring about risk-inducing operator deviations. In addition, other risks of accidents must be identified and dealt with in accordance with *section 3.2.7*.

The scope and depth of the system safety work must be adapted and may be concentrated on what the similarities are when using live weapons/management systems at the operator interface, the similarity of use, how each version is handled and the risk of incorrect learning. Normally, the SCA approval and CSSB cover all technical systems, such as weapons/management systems for the technical system, including related simulators at the school or training facility. System safety activities are selected in accordance with *section 3.2.7*.



# 4 H SYSTSÄK E AND MIL-STD-882C

## 4.1 GENERAL INTERPRETATION AND GUIDANCE FOR MIL-STD-882C

Instructions are provided below as to which parts of MIL-STD-882C are applicable.

FOREWORD: Not applicable to Swedish conditions, it is replaced by *H SystSäk E Part 1, chapter 1*.

1. SCOPE: Not applicable to Swedish conditions, it is replaced by *H SystSäk E Part 1, chapter 1*.
2. APPLICABLE DOCUMENTS: The standard states explicitly that it does not have any references. In H SystSäk E Part 2, each activity is self-explanatory.
3. Acronyms and DEFINITIONS: MIL-STD-882C acronyms can be found in Acronyms/abbreviations. The definitions are applicable with the following additions and adjustments:
  - 3.2.2 Contractor: “DOD” corresponds to the Ministry of Defence, “MA”, see 3.2.8 below.
  - 3.2.4 Hazard: Corresponding to hazardous event or hazardous condition.
  - 3.2.6 Hazard severity: See *H SystSäk E Part 1, chapter 1 and 4*.
  - 3.2.8 Managing Activity: Corresponding to the Armed Forces (FM) and DesignA – responsible for the procurement of technical systems or a supplier (sub-supplier) that requests activities from sub-suppliers.
  - 3.2.9 Mishap: Corresponding to an ACCIDENT.
  - 3.2.10 Non-developmental item, b: “United States” corresponds to Sweden.
  - 3.2.21 System Safety Working Group: “MA”, 3.2.8. See activities for SSWG *section 5.8 and H SystSäk E Part 1, section 7.4 and section 6.8*.

3.2.24 System Safety Program: See activity for SSP, *section 5.1*.

3.2.25 System Safety Program Plan: See activity for SSP, *section 5.5*.

4. GENERAL REQUIREMENTS: Not applicable to Swedish conditions, it is replaced by *H SystSäk E Part 1*.

5. DETAILED REQUIREMENTS: Not applicable to Swedish conditions, it is replaced by *H SystSäk E Part 1*.

6. NOTES: Not applicable to Swedish conditions, it is replaced by *H SystSäk E Part 1*, *H VAS-E*, *H FordonSäk*, *RML*, *RMS* etc.

CONCLUDING MATERIAL: Not applicable to Swedish conditions.

TASKS: This part is generally applicable with the addition that even the unique Swedish activities, in accordance with *chapter 1*, should be taken into consideration. These have separate activity numbers that are not included in MIL-STD-882C.

APPENDIX A. GUIDELINES FOR THE IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS: Not applicable to Swedish conditions, replaced by *section 3.2*, each activity is described in *chapter 1* and *H SystSäk E Part 1*. (However, part of appendix A may have been used for the development of FURTHER INFORMATION for a certain activity in the handbook.)

APPENDIX B. SYSTEM SAFETY PROGRAM ACTIVITIES RELATED TO THE LIFE CYCLE PHASE: Not applicable to Swedish conditions, it is replaced by *section 3.2*, each activity is described in *chapter 1* and *H SystSäk E Part 1*.

APPENDIX C. SUPPLEMENTARY REQUIREMENTS: Not applicable to Swedish conditions, it is replaced by *chapter 1* and each activity is described in *chapter 1*.

APPENDIX D. DATA REQUIREMENTS FOR MIL-STD-882: Not applicable to Swedish conditions, it is replaced by *section H SystSäkE part 1* and each activity is described in *chapter 1*.



## 4.2 GENERAL DESCRIPTION OF THE ACTIVITIES IN H SYSTSÄK E

The section describes a number of system safety activities. These are used in appropriate parts and whenever applicable. *Table 4:1*, below, provides an indication as to when the activities are applicable.

When planning an operation for technical systems a System Safety Management Plan (SSMP) is produced (according to SSP, see *section 5.1*) and the System Safety Program Plan (SSPP, see *section 5.5*) for the document in question, the activities that are deemed as being relevant are chosen.

The unique Swedish activities are identified by the letter “S” followed by a two-digit number.

An “*italicized*” activity is included in MIL-STD-882C but is not used in H SystSäkE.

The Functional Hazard Assessment (FHA) activities *5.20* and Safety Critical Functions (SCF) *5.11* are not found in MIL-STD-882C, or in the previous edition of H SystSäk E, but are generally applicable safety activities which are included in both civilian and military standards. Therefore, they have been included in this edition of H SystSäkE.

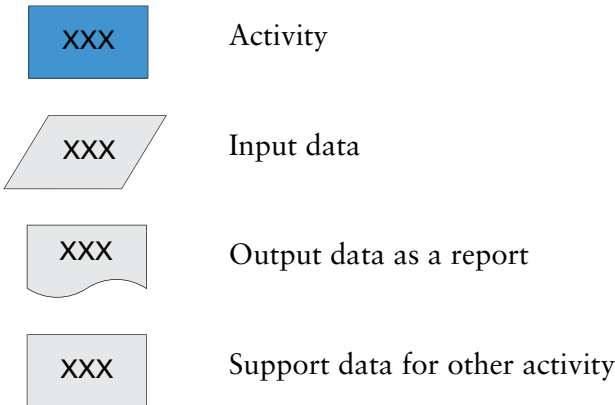
For unique Swedish activities the set-up is as follows:

- **PURPOSE**, a brief description of what the activity aims to do.
- **ACTIVITY DESCRIPTION**, a description of how the activity should be carried out.
- **INPUT DATA**, indicating which input data is needed to conduct the activity.
- **OUTPUT DATA**, indicates what is generated when the activity is carried out, such as the resulting report.

For the handbook's other activities, see MIL-STD-882C, with deviations described in each section below. The following sections are included:

- **PURPOSE**, this section contains a brief general description of the activity.
- **DEVIATIONS**, describes any deviations in relation to MIL-STD-882C.
- **COMPARABLE ACTIVITIES/DOCUMENTS**, reference to comparable activities in other standards that can be used, for example, in international cooperation.
- **FURTHER INFORMATION**, provides further guidance when carrying out the activity, often taken from MIL-STD-882C Appendix A.
- **INPUT DATA**, indicating which input data is needed to conduct the activity.
- **OUTPUT DATA**, indicates what is generated when the activity is carried out, such as the resulting report.

For each activity there is a picture that gives an overview of the input and output data for each activity. For each activity listed:



Blue indicates activity.

Grey indicates safety-related activity or report.

Yellow indicates condition.

Green indicates information not detailed in H SystSäkE.

## 4.3 OVERVIEW OF ALL SYSTEM SAFETY ACTIVITIES

Table 4:1 Activities

Task	Title	Phase					
		0	I	II	III	IV	V
101	System Safety Program (SSP)	G	G	G	G	G	G
S10	System Safety Evaluation (SSE)	S	S	N/A	N/A	N/A	N/A
S11	System Safety Requirements in TTEM	N/A	G	G	GC	N/A	N/A
S12	Requirements for Tender Enquiry (RFP)	N/A	G	G	GC	N/A	N/A
102	System Safety Program Plan (SSPP)	N/A	N/A	G	G	S	G
103	Integration/Management of Subcontractors (IMSC)	N/A	N/A	S	S	S	S
104	System Safety Program Review / Audits (SSPR)	N/A	S	G	G	S	S
105	System Safety Working Group (SSWG) Support	S	G	G	G	G	G
106	Hazard Tracking and Risk Resolution (HTRR)	S	G	G	G	G	S
107	System Safety Progress Summary (SSPS)	N/A	N/A	G	G	S	S
S13	Safety Critical Functions (SCF)	N/A	S	G	G	GC	N/A
201	Preliminary Hazard List (PHL)	S	G	G	S	N/A	N/A
202	Preliminary Hazard Analysis (PHA)	N/A	S	G	GC	GC	N/A
203	Safety Requirements/Criteria Analysis (SRCA)	N/A	S	G	GC	GC	N/A
204	Subsystem Hazard Analysis (SSHA)	N/A	S	G	GC	GC	N/A
205	System Hazard Analysis (SHA)	N/A	S	G	GC	GC	N/A
206	Operating and Support Hazard Analysis (O&SHA)	N/A	S	G	GC	GC	N/A
207	Health Hazard Assessment (HHA)	N/A	S	G	GC	GC	G
S21	Risk Analysis of External Environment (EHA)	N/A	S	G	GC	GC	G
S22	Functional Hazard Assessment (FHA)	N/A	S	G	GC	GC	N/A
301	Safety Assessment Report (SAR)	N/A	N/A	G	GC	S	N/A
302	<i>Test and Evaluation Safety</i>	N/A	N/A	N/A	N/A	N/A	N/A

Task	Title	Phase					
		0	I	II	III	IV	V
303	Safety Review (SR)	N/A	S	G	G	GC	N/A
401	Safety Verification (SV)	N/A	S	G	S	S	N/A
S41	Safety Instructions (SI)	N/A	S	G	G	GC	G
S42	System Safety Statement (SCA)	N/A	S	G	GC	GC	N/A
S43	Fault Reporting System (FRACAS)	S	S	G	G	G	S
403	<i>Explosive Hazard Classification (EHC) and Characteristics Data</i>	N/A	N/A	N/A	N/A	N/A	N/A
404	<i>Explosive Ordnance Disposal (EOD) Source Data</i>	N/A	N/A	N/A	N/A	N/A	N/A
S51	System Safety Approval System (SS)	N/A	N/A	S	G	S	N/A
S52	Test and Safety Regulations (TSR)	N/A	N/A	N/A	G	G	N/A
S53	Central System Safety Decision (CSSB)	N/A	N/A	S	G	S	N/A
S61	Risk Analysis for the Decommissioning of Systems (RADS)	N/A	N/A	N/A	N/A	N/A	G

### Explanations:

#### PROGRAM PHASE

- 0 Concept exploration
- I Demonstration/validation/technology development
- II Engineering/manufacturing, development
- III Production/deployment
- IV Operations and support
- V Decommissioning/disposal

#### APPLICABILITY CODES

- S Selectively Applicable
- G Generally Applicable
- GC General Applicable to Design Change Only
- N/A Not Applicable

# 5 DESCRIPTION OF ACTIVITIES

## 5.1 SYSTEM SAFETY PROGRAM (SSP) – TASK 101

### 5.1.1 Purpose

---

This activity is applied by the Armed Forces and DesignA when determining requirements and for planning purposes. Planned system safety activities are documented in a System Safety Management Plan (SSMP). The concept of a SSMP is not included in MIL-STD-882C, but in a later preliminary version of the standard. The concept is therefore considered appropriate to use in *H SystSäk E*. Both the Armed Forces and DesignA should regulate each System Safety Program in a plan. The SSMP document is that plan.

The SSMP will specify the Armed Forces’/DesignA’s SSP during the technical system’s entire service life. The plan should also indicate which activities are mandatory and what is otherwise required of suppliers before tendering.

The supplier must describe the planned SSP in the System Safety Program Plan (SSPP) 5.5.

### 5.1.2 Deviations

---

101.2.1: References to “Section 4” are replaced by *H SystSäk E Part 1*.

101.3.1 b: References to “Section 4” are replaced by *H SystSäk E Part 1*.

### 5.1.3 Comparable Activities/Documents

---

Safety operations in the UK are also referred to as Safety Cases. A similar plan is the Safety Management Plan. (JSP520 [33], JSP430 [38], JSP533 [29] and JSP454 [34]).

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 101, System Safety Program. This differs slightly and could be applied as an alternative.

### 5.1.4 Further Information

---

This activity is mandatory for all technical systems. However, the technical system's potential accident risks must be taken into account when the activities are selected for implementation, see *section 3.2.1*.

The task of defining system requirements are also included, these can come from *H SystSäk E Part 1* and *chapter 2* and *3* of *part 2* or from other sources.

Fault reporting and follow-up systems for incidents and accidents should be identified/established at an early stage.

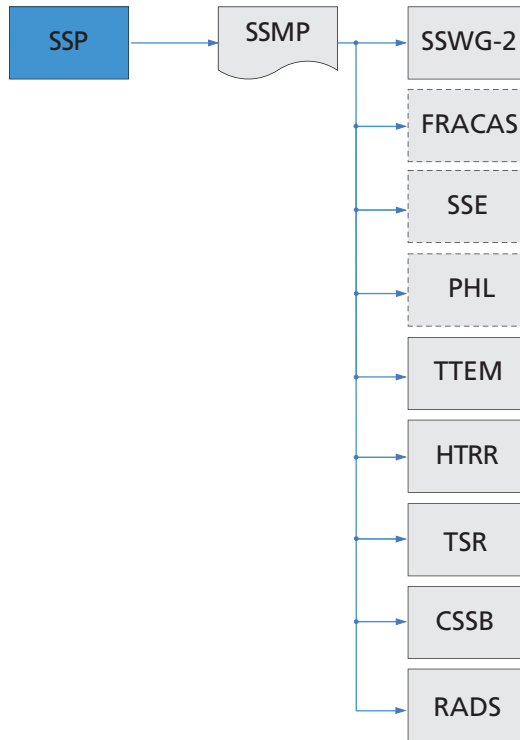
### 5.1.5 Input Data

---

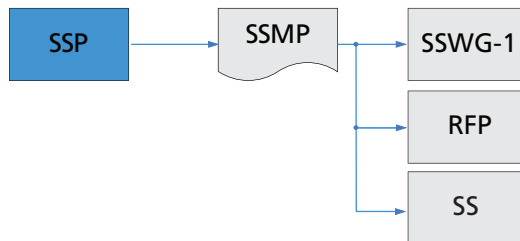
Support data for system safety requirements and activities, see *H SystSäkE part 1* and *chapter 2* and *3* of *part 2*.

### 5.1.6 Output Data

A SSMP defines planned activities. Templates/examples of a SSMP are on H SystSäk CDR.



*Figure 5:1 System Safety Program (SSP) for the Armed Forces*



*Figure 5:2 System Safety Program (SSP) for Design A*

## 5.2 SYSTEM SAFETY EVALUATION (SSE) – S10

### 5.2.1 Purpose

---

This activity is mainly used by the Armed Forces to provide tools to prioritize and rank system alternatives from a systems safety perspective. Implementation of studies and the preparation of system specification criteria are carried out in accordance with *H SystSäk E Part 1, section 6.4, Studies*.

### 5.2.2 Activity Description

---

A SSE relates to the various concepts/system specification criteria required in order to identify, analyse and evaluate possible system safety problems in terms of general factors, this is to provide decision data to prioritize concepts in the Armed Forces' continued educational activities.

Examples of activities for a SSE:

- To make a list of hazardous technical systems, subsystems, products, components, chemical substances, situations etc. A Preliminary Hazard List (PHL 5.12) is a good tool to identify hazards/hazardous conditions.
- To identify possible injury/damage to people, property or the external environment on the basis of the above. PHL 5.12 can be used for this. To give priority to the concept that contains the minimum number of hazards/hazardous conditions with the least potential impact on people, property or the external environment.
- To identify the general factors that should be assessed in terms of:
  - **Unknown technology** – based on the technical system's safety-vulnerable parts of the known existing technology, or is there a need for extensive technological development?
  - **Safety measures** – will the technical system require employees to use personal protective equipment or extensive safety precautions (such as in high-risk areas) during use?



- **Environmental impact** – what sort of environmental impact can be expected in the short and long term during both the use and the decommissioning of the materiel? (The environmental impact for normal emissions for all materiel handling is generally taken care of in the ordinary environmental work. If the environmental impact is not taken into consideration in this work, this should be done under system safety activities.)
- Analyse and evaluate the results from a system safety point of view. The total system safety evaluation (SSE - system safety, economy, efficiency, procurement lead time) must also take into account system safety aspects.
- Evaluate and document the results.

*Table 5:1* provides examples as to how an assessment can be made without weighting the constituent factors. The various concepts (A, B and C) are based on known techniques which can be assessed to require different types of safety measures. Depending on the choice of materials and the manner of propulsion, the various concepts have a greater or lesser impact on the external environment. The SSE shows that concept C is the best concept.

Table 5:1 Valuation Matrix

Concept	New, unknown technology	Requirements for safety instructions	Environmental impact	Summary and rating
A	Scope (3)	None (0)	Small (1)	Average (4)
B	Small (1)	Normal (1)	Large (3)	Worst (5)
C	None (0)	Extended (2)	Small (1)	Best (3)

### 5.2.3 Input Data

---

A description of the concept and possible PHL 5.12.

### 5.2.4 Output Data

---

The resulting report should clearly indicate the system safety priorities of the various concepts. Consideration must be taken to other evaluation criteria, such as efficiency, acquisition time and finances. An overall assessment takes place outside of the activity described here. A report from the SSE will form the basis of TTEM 5.3. There is no template for the report.

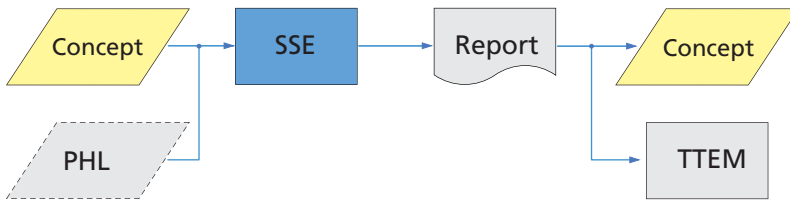


Figure 5:3 System Safety Evaluation (SSE)

## 5.3 SYSTEM SAFETY REQUIREMENTS IN TTEM – S11

### 5.3.1 Purpose

---

This activity is mainly used by the Armed Forces to identify and determine the system safety requirements to be included in TTEM. The requirements aim to ensure that technical systems are sufficiently safe when used as intended throughout their service life. The appropriate parts of the handbook should be used for the development of goals for training materials (with requirements according to TEMU, UTEMU, PTEMU).

### 5.3.2 Activity Description

---

There are two types of requirements which the Armed Forces makes on DesignA:

- Operational requirements, requirements regarding a particular operation and operational accomplishment (written in the document, customer order (KB)).
- Technical requirements, relating to the current technical system (written in the TTEM document).

Grounds for identifying the needs of and to formulate system safety requirements in TTEM in the KB are described in *H SystSäk E Part 1, section 6.5*. The grounds for special considerations in the preparation of requirements are also detailed.

### 5.3.3 Input Data

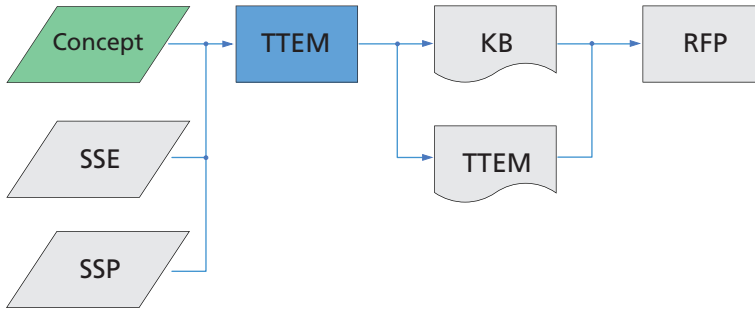
---

System specification criteria from DesignA and the Armed Forces' governing documents provide input data for TTEM.

### 5.3.4 Output Data

---

TTEM are used later as input data for the Request for Proposal (RFP) 5.4.



*Figure 5:4 System Safety Requirements in TTEM*

Examples of requirements to take into consideration regarding a KB/TTEM can be found on H SystSäk CDR.

## 5.4 DETERMINING REQUIREMENTS FOR TENDER ENQUIRY (RFP) – S12

### 5.4.1 Purpose

---

This activity is mainly used by DesignA to transform the system safety requirements which the Armed Forces has specified in the KB (and respectively in TTEM) as requirements that may be included in the RFP or for the production of internal requirements in DesignA, for example, a review of existing technical systems.

### 5.4.2 Activity Description

---

DesignA's system safety requirements for technical systems are specified in the RFP. The requirements are divided into technical requirements and operational requirements.

The Armed Forces' system safety requirements in terms of a KB and TTEM are cleared of conflicting requirements and formulated so that they are measurable (for example, with reference to *chapter 2, Materiel Requirements*, for general requirements). Durability requirements for ammunition in abnormal environments are formulated in accordance with H VAS-E [24] or the applicable standard.

The Armed Forces' may need system safety requirements for an entire technical system broken down to a technical subsystem level where different suppliers of technical subsystems may share the overall system safety requirements.

In addition to the materiel-linked safety requirements, as specified in the RFP, demands are to be made on system safety activities, in accordance with *chapter 3, System Safety Activities*. In response to a tender enquiry, a supplier will indicate which activities are proposed to be included in the system safety work and report these in the SSPP 5.5). How the supplier's response to the requirements should be worded is described in the SSPP 5.5 and Safety Requirements/Criteria Analysis (SRCA 5.14).

*Construction-influencing requirements are:*

The following examples of requirements act as a guide with regard to the requirements DesignA may need to establish in order to satisfy the Armed Forces' requirements (in TTEM and a KB). The requirements are not designed to be to be pasted in:

Operation-oriented requirements:

- Maximum time for the safety inspection for daily and special inspections.
- Maximum limitations for use, such as the largest acceptable safety distance and the longest acceptable time for training on safety precautions.

*Design requirements:*

- Certain materials and substances may not be used in the construction or during operation.
- Some design solutions may not be used in the technical system, see also H VAS-E [24], H FordonSäk [21] and *chapter 6*.
- Some design principles and design solutions are applicable to specific safety-critical systems and functions, such as fail-safe functionality, built-in test, redundancies, modularization, robust design, special components, programming languages, see *chapter 2* and *6*.

Requirements for decommissioning (see the RADS 5.34):

- development of the Recycling Manual [15]
- modular design to facilitate the reutilization of technical sub-systems.

System safety requirements:

The following **examples of requirements** are indicative of DesignA's requirements for potential suppliers. After consideration, requirements are chosen which act as a guide for the procurement in question, these requirements are then included in the tender request.

Requirements of the supplier's SSP (are included in the RFP):

- The supplier will develop a system safety plan in accordance with H SystSäk E and include it in the tender, in its preliminary design. The following activities will be included: SCA, SCF, RADS, xx, yy and zz. DesignA makes demands on the activities that the supplier must realize (and therefore these should be included in the supplier's SSPP). See *section 3.2, Selection of Activities (Tailoring)*.
- The supplier must implement additional system safety activities for the technical system, compared to what has been required for the SSPP, the results from these must be submitted to DesignA.
- The supplier must have their own safety management system which, in a traceable manner, demonstrates how system safety activities are led, followed up, agreed and documented and how this safety management system is monitored, evaluated and supplemented. A description of the safety management system must be enclosed with the tender.
- The supplier must have a special system safety organization with identified roles, responsibilities, authorities, rules, routines and working methods. This must be reported in the tender along with requirements regarding the expertise of each role.
- The supplier will continuously maintain detailed knowledge of the legal provisions (regulations etc.) that affect the design of the company's products, as well as their intended use, when they are being used by the Armed Forces. In the tender, the supplier must show how this can be ensured for the procurement in question.
- In the quotation which is submitted to DesignA, the supplier must report the name and position/role of the person who has the task of deciding the supplier's SCA (this person must be an authorized signatory or person who is directly managed by the supplier).

- The supplier must promptly notify DesignA of the existence of a non-tolerable accident risk (red risk) for which the supplier cannot identify requisite risk reduction.

An accident risk with lasting consequences for the external environment should be regarded as not tolerable.

- The supplier must deliver the SCA with the safety assessment report (SAR). Delivery must take place xx weeks before delivery of the technical system. The system compliance assessment will, in addition to the content in the example in *appendix 1*, also include xx, yy, zz.

The system compliance assessment will also be issued for the following subsystems (for example, included ammunition).

- The supplier must deliver complete risk documentation, including a Risk Log, risk decision for each accident risk, documentation for instructions, references, manuals etc., which describes how any identified accident risks should be avoided and any relevant restrictions (refers to restrictions in the technical system used to temporarily deal with certain accident risks). Delivery will take place in conjunction with the SCA. The documents are drawn up by the Armed Forces' supplied model (forms), examples of templates and how to fill in the forms can be found on H SystSäk CDR. If the provider wishes to apply a model that he/she has developed, this must be agreed with DesignA, a minimum of the data indicated on the Armed Forces' documents must be included.
- The supplier must deliver documentation for the training required from a system safety point of view. Delivery should take place in conjunction with the SCA.
- The supplier must deliver orders and instructions for use and maintenance (including support for SäkI). Delivery should take place in conjunction with the SCA.
- In designing the current technical system's deviation handling procedures, the Armed Forces' deviation handling system xx should be used.



- The technical system's documentation should be written in Swedish or English.

*In the development of this requirement, see H SystSäk E Part 1, section 5.10.4, and incorporate the appropriate options for the current parts of the documentation.*

- A special audit (quality control) should be implemented by subsystem yyy/product zzz and should be reported with a special review report.

*In the development of this requirement see H SystSäk E Part 1, section 5.12, and specify the current system parts/products.*

- **Military exemption** (See H SystSäk E Part 1, section 1.2 and 2.4.1).

In the tender, the supplier must provide a full account that the technical systems are in accordance with Swedish law/regulations applicable to the technical system in question and that they include some kind of exemption for military equipment/military use/activity. If the law/regulations provides threshold values for civil operations (or the equivalent) the supplier must request complimentary information during the bidding period relating to the Armed Forces' requirements for current threshold values so that the tender will be based on the right prerequisites.

- The supplier must declare the rules, such as laws and regulations, that have influenced the technical system's design along with the constitutional requirements that must be met by the Armed Forces during operations, maintenance and decommissioning.
- The technical system's specific injury/accident risks for an individual must not exceed the tolerable risk level according to the attached risk matrix for personal injury.
- The technical system's specific damage/accident risk for financial losses must not exceed the tolerable risk level according to the attached risk matrix for financial damage.

## 5 Description of Activities

- The supplier must implement ruggedized operations (environmentally engineered operations) as described in The Swedish Environmental Engineering Society (SSES) Handbook on Environmental Technology [37].
- The supplier must provide the technical system with the following safety/protective devices: XXX, YYY, ZZZ.  
*(This may, for example, consist of a specific type of firefighting equipment, additional evacuation functions or protection against radiation.)*

### 5.4.3 Input Data

---

Documentation for formulating the system safety requirements in the RFP is the TTEM 5.3.

### 5.4.4 Output Data

---

The tender enquiry and input data for the SSPP 5.5 and the SRCA 5.14.

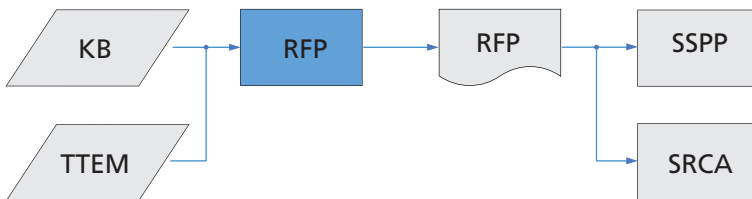


Figure 5:5 Determining Requirements for the Request for Proposal (RFP)

#### 5.4.5 As Low As Reasonably Practicable (ALARP)

---

In cases where the acquisition is planned in collaboration with another nation which applies the As Low As Reasonably Practicable (ALARP) methodology, some guidelines in the form of points of view regarding the implications of ALARP are available here. It should first be noted that the ALARP methodology involves the generation of documentation that is well suited for system operations in accordance with H SystSäk E.

The concept of ALARP was introduced by the UK Health and Safety Executive (HSE). The term refers to the cost of certain risk reduction being identified.

In the event that the risk-related gain is considered higher than the cost of certain risk-reducing measures, the risk-reducing measures should be introduced in accordance with British law.

However, if the cost is higher than the risk-related gains, the risk of an accident occurring is considered to be ALARP.

When a technical system complies with generally accepted design standards, it is often considered that ALARP has been achieved.

The methodology used in H SystSäk E has a similar meaning. However, there is a slight difference in the risk and how it is handled. ALARP and the system safety methodology is based on the risk of a specific accident occurring. However, a check must be carried out as to whether the estimated risk of an accident occurring in the ALARP model accounts for all the four risk elements from any accident risks, from an H SystSäk E perspective, or the “worst credible case” or “most credible case”. In the latter case, the missing risk elements for each individual accident risk must be identified (in terms of size) so that the system safety methodology can be fully applied.

## 5.5 SYSTEM SAFETY PROGRAM PLAN (SSPP) – TASK 102

### 5.5.1 Purpose

---

---

This activity, which defines the planned system safety activities, mainly applies to the supplier. Where DesignA is a unifying system, this task also applies for DesignA, which in these cases is the supplier of a technical system consisting of integrated subsystems.

### 5.5.2 Deviations

---

---

102.2.4 b: Reference should also be made to the described risk management process in *H SystSäk E Part 1*.

### 5.5.3 Comparable Activities/Documents

---

---

An equivalent plan is the System Safety Management Plan (SSMP), (Def-Stan 00-56 [42]).

The civilian standard GEIA-STD-0010 [27] has an equivalent activity, Task 102, System Safety Program Plan (SSPP). This activity has a more detailed description of all risk assessments (102.2.5), but does not differ with respect to the object and purpose and can therefore be applied as an alternative.

### 5.5.4 Further Information

---

---

A SSPP is used to evaluate a potential supplier's understanding and prioritization of system safety activities required for the development of technical systems.

For technical systems in which DesignA is responsible for the system, the SSPP will be established and its activities carried out by DesignA.

To support the identification of those activities that should be included in the SSPP, guidance is provided in *section 3.2, Selection of Activities (Tailoring)*.

### 5.5.5 Input Data

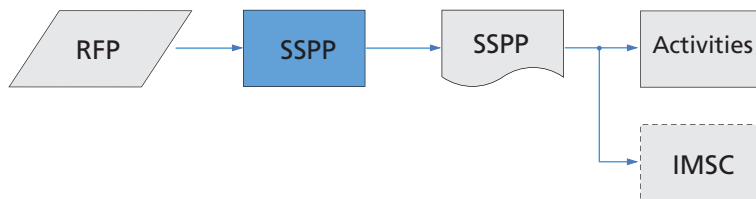
---

A RFP 5.4 forms the basis for the development of the SSPP. A RFP includes requirements for the delivery of a SSPP with activities and a time and delivery schedule.

### 5.5.6 Output Data

---

Output data from the SSPP activity is the SSPP document. The SSPP document provides information on all the system safety activities that are to be conducted.



*Figure 5:6 System Safety Program Plan (SSPP)*

Examples of a SSPP are on H SystSäk CDR.

## **5.6 INTEGRATION/MANAGEMENT OF SUBCONTRACTORS (IMSC) – TASK 103**

### **5.6.1 Purpose**

---

---

This activity relates to the ordering of parts for integration in a technical system or the use of subcontractors in the system work. When DesignA is acting in the capacity of holding the system together, this activity also applies for DesignA. The full name of the activity is “Integration/Management of Associated Contractors, Subcontractors and Architect and Engineering Firms” (IMSC). Please note that the acronym IMSC is not used in MIL-STD-882C.

### **5.6.2 Deviations**

---

---

103.2.1 (8): Reference should be made to the requirements in the Handbooks: the Handbook on Arms and Ammunition Safety [24] and the Handbook on Vehicle Safety [21].

### **5.6.3 Comparable Activities/Documents**

---

---

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 103, IMSC. This differs slightly and could be applied as an alternative.

### **5.6.4 Further Information**

---

---

In larger projects, several subcontractors are usually hired. If this occurs via a main contractor, the contractor is responsible for ensuring that the SSPP 5.5 also includes the subcontractors' SSPP.

### 5.6.5 Input Data

---

The SSPP 5.5 provides the basis for the activities to be implemented. Defined safety-critical parts and functions also govern the activities of subcontractors, see the SCF 5.11. The governing of subcontractors primarily takes place through the use of a Statement of Work (SOW), operational assignments or via requirements in the initial order.

### 5.6.6 Output Data

---

The output data generated (analyses etc.) are normally incorporated into the main subcontractor's safety documentation. For development projects to be performed by a subcontractor, a separate SSPP 5.5 must be requested. For complete technical subsystems, a SAR 5.21 should be requested. The document that guides the subcontractors is usually a SOW.

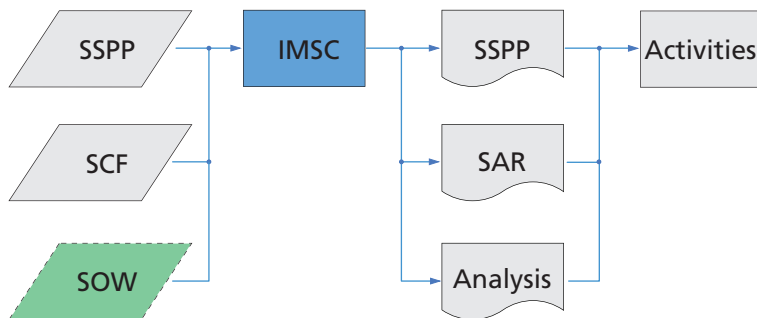


Figure 5:7 Integration/Management of Subcontractors (IMSC)

## 5.7 SYSTEM SAFETY PROGRAM REVIEWS/AUDITS (SSPR) – TASK 104

### 5.7.1 Purpose

---

---

The activity relates to both internal company audits and the supplier's involvement in customer audits. This activity relates mainly to the supplier. Please note that the specific acronym SSPR is not used in MIL-STD-882C.

### 5.7.2 Deviations

---

---

103. 2.3: Reference should be made to the requirements in the Handbooks: Weapons and Ammunition Safety Manual [24] and Handbook on Vehicle Safety [21].

### 5.7.3 Comparable Activities/Documents

---

---

This review is aimed primarily at fulfilling the requirements in the SSPP 5.5. Audits of the technical system and its hardware and software are not covered by this activity. This may be regulated by the standards used during development and manufacturing.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 104, SSPR. This differs marginally and could be applied as an alternative.

### 5.7.4 Further Information

---

---

Frequency and scope of audits performed by the client that requires the participation of the supplier is specifically regulated in the order.

Results from the review are documented in an assessment report and an accompanying action list detailing the shortcomings that have been identified.

Reviews to be carried out of DesignA's advisory groups are also covered by this activity, see H VAS E [24].



### 5.7.5 Input Data

---

A SSPP 5.5, with system safety documents generated by the implemented system safety activities, mainly Risk Log (see Hazard Tracking and Risk Resolution (HTRR) 5.9, provides an input for the review.

For reviews of Design A's advisory groups, the scope is regulated by requisite documentation in H VAS E [24].

### 5.7.6 Output Data

---

The output data are records of a security screening with a possible updated Risk Log (see the HTRR 5.9). From DesignA's advisory groups, special audit records are generated.

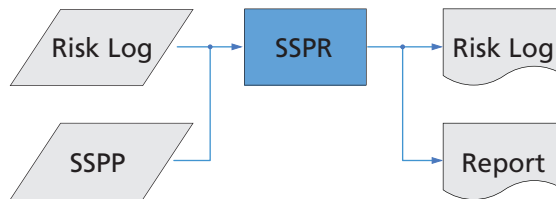


Figure 5:8 System Safety Program Reviews/Audits (SSPR)

## 5.8 SYSTEM SAFETY WORKING GROUP (SSWG) – TASK 105

### 5.8.1 Purpose

---

In *H SystSäkE Part 1*, two different designs for the SSWG are defined and described. The full name of the activity is the System Safety Group/System Safety Working Group Support (SSWG).

SSWG-1: Is appointed by DesignA as support for the project and is involved during development and procurement. The Armed Forces, DesignA and the supplier may participate.

SSWG-2: Is appointed by the Owner Representative (ÄF) as a part of the responsibility for the technical system when in operation. SSWG-2 is involved throughout the technical system's entire life but mainly focuses on system maintenance and the decommissioning phases. The Armed Forces, DesignA and the supplier may participate in the group.

### 5.8.2 Deviations

---

105.1: "Service regulations" are usually not applicable to Swedish conditions, this is regulated by the Armed Forces/DesignA.

### 5.8.3 Comparable Activities/Documents

---

An equivalent group is Safety Panel (JSP520 [33], JSP454 [34] and Def-Stan 00-56 [42]).

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 105, System Safety Group/System Safety Working Group Support. This differs marginally and could be applied as an alternative. GEIA-STD-0010 requires that the supplier is responsible for the meeting agenda and meeting minutes (105.3.d).

#### 5.8.4 Further Information

---

Frequency and scope of the supplier's participation in SSWG-1 and SSWG-2 must be specifically regulated in the order.

#### 5.8.5 Input Data

---

Regulation of the frequency of meetings and the agenda can be made in the SSMP, see the SSP 5.1 and the SSPP 5.5. An agenda for the meeting should be distributed prior to the meeting taking place. Risk Log (see the HTRR 5.9) and misreporting (see the FRACAS 5.28) is often used as input data for the meetings.

5.8.6 Output Data

---

For meeting notes and information for the Risk Log, or equivalent, see the HTRR 5.9.

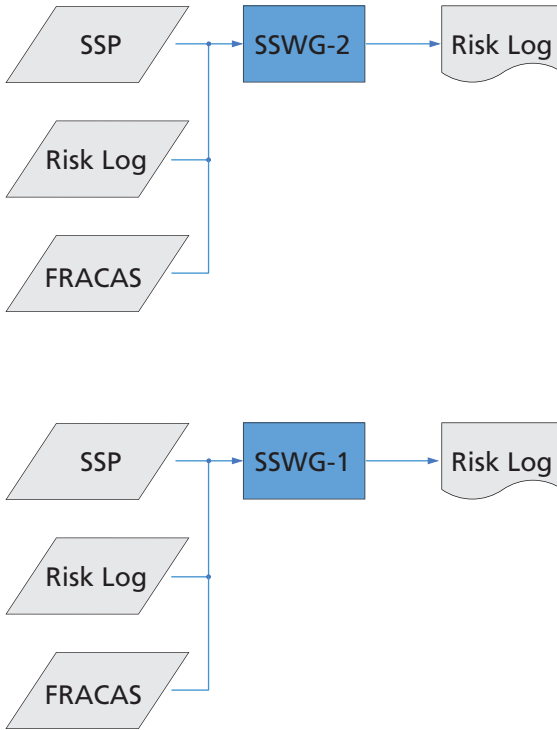


Figure 5:9 System Safety Working Group (SSWG)

## 5.9 HAZARD TRACKING AND RISK RESOLUTION (HTRR) – TASK 106

### 5.9.1 Purpose

---

The activity relates to the establishment of a risk management process with documentation of identified accident risks in a Risk Log (Hazard Log) where other administration and the closing of risks is also documented. For existing technical systems, the risk monitoring process of the Armed Forces is to be established and run. The acronym HTRR is not used in MIL-STD-882C.

### 5.9.2 Deviations

---

–

### 5.9.3 Comparable Activities/Documents

---

In the UK, the Hazard Log is the equivalent of a Risk Log. The format of this is strictly regulated and information is kept in a database named Cassandra, (Def-Stan 00-56 [42]).

The civil standard GEIA-STD-0010 [26] has a similar activity, Task 106, HTRR. This differs marginally and could be applied as an alternative. GEIA-STD-0010 specifies that all accident risks must be recorded, not only residual risk of accidents (106.2.1.d). Note that regardless of the standard used, the Risk Log for the technical system, according to H SystSäk E, must always cover all identified risks of accidents.

### 5.9.4 Further Information

---

The Risk Log is a “database” with information about identified accident risks. This should be maintained throughout the entire life of the technical system. The Risk Log is usually initiated by the Armed Forces when studies are carried out, then taken over by the supplier for development and manufacturing, and is

returned on delivery of the technical system to the Armed Forces for maintenance and decommissioning phases. Closure of the risk of accident takes place in accordance with the SSPP 5.5. Normally, the Risk Log is reported in the SSPR 5.7 and System Safety Progress Summary (SSPS) 5.10.

### 5.9.5 Input Data

---

The SSMP (see the SSP 5.1) and the SSPP 5.5 initiate and define the implementation of a Risk Log. Accident risks from analyses (PHL 5.12, PHA 5.13, SRCA 5.14, FHA 5.20, SHA 5.16, SSHA 5.15 and FRACAS 5.28) are used as input data for the Risk Log (Hazard Log).

### 5.9.6 Output Data

---

Risk Log (Hazard Log) can be used for Safety Verification (SV 5.24) and for the development of SAR 5.21. Reporting the Risk Log can be made at the SSPR 5.7, SSWG 5.8 and SSPS 5.10.

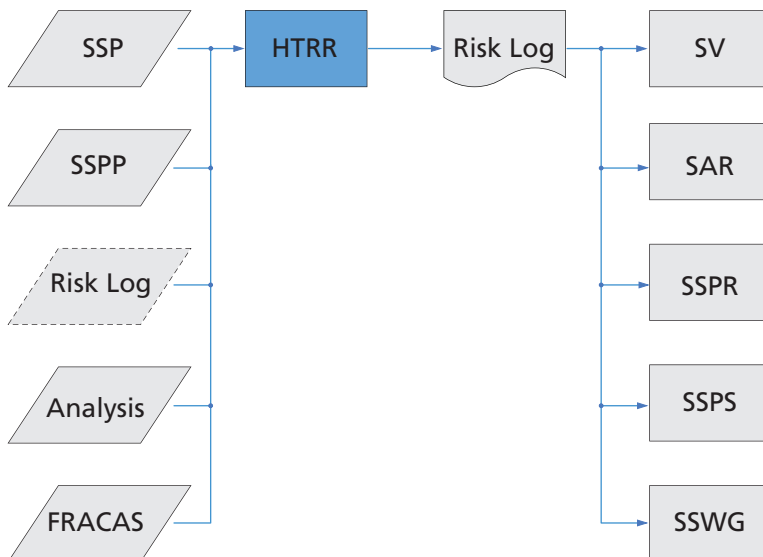


Figure 5:10 Hazard Tracking and Risk Resolution (HTRR)

## **5.10 SYSTEM SAFETY PROGRESS SUMMARY (SSPS) – TASK 107**

### **5.10.1 Purpose**

---

---

The activity relates mainly to the supplier's report of the state of the SSP and system safety activities. This activity is closely linked to the SSWG 5.8.

The acronym SSPS is not used in MIL-STD-882C.

### **5.10.2 Deviations**

---

---

–

### **5.10.3 Comparable Activities/Documents**

---

---

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 107, SSPS. This differs marginally and could be applied as an alternative.

### **5.10.4 Further Information**

---

---

The periodicity of reporting must be specified in the Delivery Plan or the SSPP 5.5.

### **5.10.5 Input Data**

---

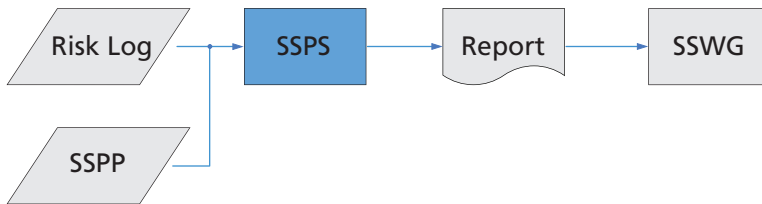
---

The SSPP 5.5 and activities that are carried out during the last period. Accident risks with input data from the Risk Log (see the HTRR 5.9) are reported.

### 5.10.6 Output Data

---

Status report on safety (System Safety Progress Report).



*Figure 5:11 System Safety Progress Summary (SSPS)*



## 5.11 SAFETY CRITICAL FUNCTIONS (SCF) – S13

### 5.11.1 Purpose

---

As a part of the quality schedule for a technical system, the supplier must identify, establish, document and maintain procedures, development processes, work instructions and processes for all production operations etc., used in the development and manufacture of components that can be characterized as critical for safety. By specifying criticality classes in the development and product descriptive documents, the conditions are created to guide the resources in the development and manufacturing processes, along with inspection where they are needed most. The corresponding activity is the civilian standard GEIA-STD-0010 Task 209 [26]. This activity is not described in the previous edition of H SystSäk E but is internationally applied, so the English designation is used. Critical properties (CI) can be found in *chapter 2, Materiel Requirements*.

### 5.11.2 Activity Description

---

#### *Definition of Critical Characteristics*

---

Safety-critical and safety-related components are those which have characteristics (tolerance, hardness, surface quality, resilience of software etc.) that may result in a hazardous event if there is a shortcoming or parts which in itself can provide a hazardous event if they are lacking in an installation.

The **safety-critical** characteristics/features are those that directly (for example, a single fault) affect the safety of the technical system.

The **safety-related** properties/details are those that affect safety (for example in the event of a double fault or an error of a higher order) within the technical system.

These critical and safety-related characteristics are divided into two groups: those that in the event of property shortcomings can give rise to a CRITICAL ERROR (which can result in an accident – DAMAGE CLASS 1) and those that may cause a MAJOR FAULT (which can result in an accident with maximum DAMAGE CLASS 2).

The critical components/attributes are identified during the risk analysis by examining the deviations'/shortcomings' contribution to the hazardous event for the technical system. For each component/feature, the likelihood or failure rate of a fault occurring is noted, and the consequences are noted in the technical system. If the lack of the specified property has a sufficient influence on the hazard event, the properties/components must be classified on the drawing or in the specification.

For hardware or hardware-related elements, the CI are classified in accordance with, for example, SS 2222 [40] (Swedish Standard). For software and associated electronics, the criticality must be expressed in accordance with the instructions in *chapter 6* and H ProgSäke [18].

### *Definition of Criticality in Complex Systems*

---

Information in this section is primarily taken from the aeronautical field, where there are defined methods of dealing with systematic faults in complex systems.

The primary sources of information are SAE ARP4754 (Certification Considerations for Highly Integrated or Complex Aircraft Systems) [4], RTCA/DO-178B (Software Considerations in Airborne Systems and Equipment Certification) [39] and RTCA/DO-254 (Design Assurance Guidance for Airborne Electronics Hardware) [6].

For delimited components, their criticality can be determined by analysing how they can contribute to the occurrence of accident hazards and the consequences of the risk. ARP4754 [4] and RTCA/DO-178B [39] contain information as to how components can be classified based on the presence of the monitoring function and redundancy.

All the above-referenced documents use a scale from A–E for the classification of components, where A signifies the most-critical components and E the least-critical components.

All components in a system can be classified based on criticality, but only those components that are considered complex need to undergo a development methodology that is differentiated based on criticality.

A component is considered complex when the audit, analysis and testing carried out as a natural part of the component's development is not necessarily considered to validate its full behaviour. Examples of such components include software and various types of programmed circuits. Non-complex components are considered equivalent to criticality class A when verification has been carried out which insures its functionality and features.

The methodology prescribed by the above-referenced documents can be summarized as follows:

- Define and reach agreement with the customer/agencies as to which methodology is to be used for categorising criticality. ARP4754 [4], DO-178B [39] and DO-254 [6] can be used as a starting point, but IEC 61508 (functional safety of electrical/electronic/programmable electronic safety-related systems) [16] can also be used.
- Identify all the complex components of the system.
- Analyse how the components can help to identify accident risks.
- Classify the components as per the agreed methodology.
- Come to an agreement as to which development activities (audit, analysis, test etc.) should be implemented for the various criticality levels. Even here this information can be retrieved from ARP4754 [4], DO-178B [39], DO-254 [6] and IEC 61508 [16].
- Develop systems and constituent components as per the agreed methodology.
- Report results of development (identified deficiencies etc.) and any deviation from the agreed methodology.

Verify that the developments have actually been implemented as per the agreed methodology via independent quality audits.

Assuming that the development has been conducted in accordance with agreed practices, independent evidence exists to prove this and to show that product deficiencies have been identified, then systematic product deficiencies/errors can be regarded as having been dealt with.

Operational experience can be used as an alternative or supplement to a defined development methodology, provided that:

- The operational profile during the operating time corresponds to the intended operating profile of the new system.
- The operating time is considered sufficient with regard to the system's/component's criticality.
- An effective FRACAS is available for the current operating period.
- Any product faults can be accepted.
- Any changes to the product during the duration of operation have been identified and are found not to affect the system/components in such a way that the operating time comes into question.

### Identification of Critical Properties

CI are identified through analyses (PHL 5.12, PHA 5.13, SRCA 5.14, FHA 5.20, SHA 5.16 and SSHA 5.15). CI can be identified in many ways (or in combination):

- The Fault Tree Analysis (FTA) – if a single property contributes to the critical hazard event of sufficient magnitude it is safety critical. It is appropriate to set the level in the SSPP 5.5. The method used for these calculations is Minimal Cut Set (MCS).
- With Fault Modes Effects and Criticality Analysis (FMECA) – if a single property has a large enough occurrence probability or failure rate the potential hazard event is critical. The level is set in the SSPP 5.5.

- Based on experience/engineering assessments, if a single property is judged to significantly affect safety or is regulated through the appropriate standards. For software, see *chapter 6*.

#### *List of Critical Properties (CIL/SIL)*

---

The supplier will, if so required in the order documents, provide DesignA with a list of known critical properties. The list should also indicate the production and inspection records relating to the relevant property or part. For software, the methodology used in the development of the software should be indicated.

#### *Development of the Software*

---

The properties that are critical must be identified and guide the choice of the methods used for the production and verification of related software. See *chapter 6*.

#### *Production Management/Control of Processes*

---

The processes used to manage/control CI must be specified in the production documentation and quality plans or equivalent.

For the processes used, it should be possible for the operator to verify that they have been carried out correctly.

In cases where a subcontractor is used, equivalent requirements must be imposed on him/her, see the IMSC 5.6.

#### *Control Equipment*

---

The equipment used for the inspection of CI must be identified and described.

#### *Change Management*

---

A deviation/modification of a critical property should not be carried out by the supplier without the approval of DesignA. How this process is carried out is regulated in the Configuration Plan or equivalent. See the Safety Review (SR 5.23).

### 5.11.3 Input Data

---

The basis for SCF is all of the completed analyses PHL 5.12, PHA 5.13, SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19, FHA 5.20 and requirements in accordance with SRCA 5.14.

### 5.11.4 Output Data

---

Critical Item List (CIL) and Safety Integrity Level (SIL).

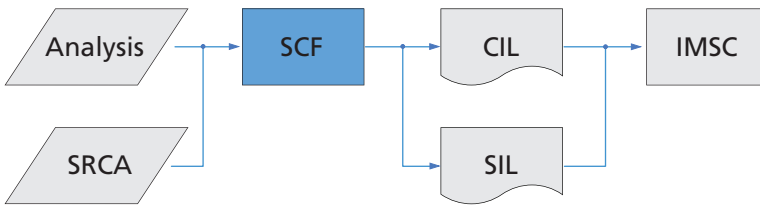


Figure 5:12 Safety Critical Functions (SCF)

## 5.12 PRELIMINARY HAZARD LIST (PHL) – TASK 201

### 5.12.1 Purpose

---

---

The activity refers to the early identification of potential accident risks. This activity is closely linked to the HTRR 5.9 with Risk Log (Hazard Log).

### 5.12.2 Deviations

---

---

–

### 5.12.3 Comparable Activities/Documents

---

---

For software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 201, PHL. This differs marginally and could be applied as an alternative. GEIA-STD-0010 has a more detailed description of the type of data that can be included in a PHL (201.2.4).

### 5.12.4 Further Information

---

---

A PHL may be required as part of a bid. A PHL is usually followed by further in-depth analyses such as the PHA 5.13, SRCA 5.14, FHA 5.20, SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18 and EHA 5.19.

There are a large number of useful charts available to identify potential accident risks, recommended charts include: US WSESRB Hazard Analysis Guide List [43] and UK Hazard Identification Checklist (Def-Stan 00-56 [5]).

### 5.12.5 Input Data

---

A concept or a design description is needed to implement a PHL. Amendments to the concept according to the SR 5.23 are followed up in a PHL.

### 5.12.6 Output Data

---

A PHL and input data to the Risk Log (Hazard Log) according to the HTRR 5.9.

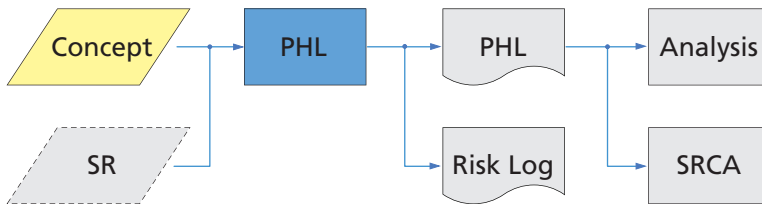


Figure 5:13 Preliminary Hazard List (PHL)

A Risk Log is available as an Excel file on H SystSäk CDR.



## 5.13 PRELIMINARY HAZARD ANALYSIS (PHA) – TASK 202

### 5.13.1 Purpose

---

The activity refers to the early identification of potential hazardous events and makes a preliminary system safety evaluation. This activity is closely linked to the HTRR 5.9 with a Risk Log (Hazard Log).

### 5.13.2 Deviations

---

–

### 5.13.3 Comparable Activities/Documents

---

For software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 202, Preliminary Hazard Analysis (PHA). This differs marginally and could be applied as an alternative. GEIA-STD-0010 has a more detailed description of the type of data that can be included in a PHA (202.2.2) and requirements for the reporting of accidents instead of hazardous events (202.3.1.b). If GEIA-STD-0010 is used decommissioning will also be required in accordance with (202.2.2.3 b(2)).

### 5.13.4 Further Information

---

A PHA is usually an initial analysis similar to the PHL 5.12, which is updated afterwards and extended through more detailed analyses. The results of a PHA can be used when defining requirements.

A PHA should include:

- experience data
- a list of known hazardous events
- measures taken to eliminate/minimize hazardous events
- requirements as a result of identified hazardous events
- recommended measures to take in order to eliminate/minimize hazardous events.

The documentation required includes the concept and design descriptions, flow charts and information about the operational profile.

The format of a PHA may vary from purely descriptive documents to a matrix format.

### 5.13.5 Input Data

---

A concept or a design description, flow chart, operating profile and often a PHL 5.12 is needed in order to implement a PHA. Changes to the design are reported in accordance with the SR 5.23 and are followed up in the PHA.

### 5.13.6 Output Data

---

A PHA and input data to the Risk Log (Hazard Log) according to the HTRR 5.9.

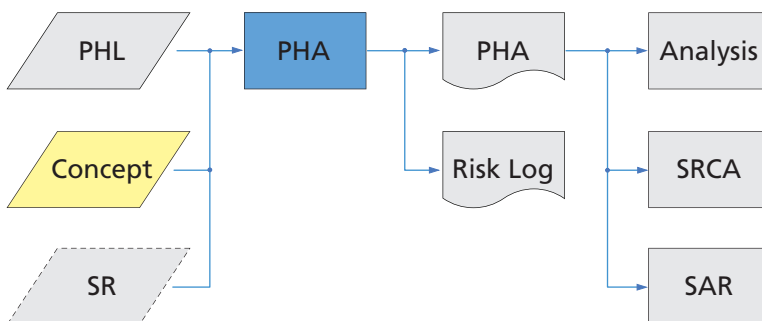


Figure 5:14 Preliminary Hazard Analysis (PHA)

## 5.14 SAFETY REQUIREMENTS/CRITERIA ANALYSIS (SRCA) – TASK 203

### 5.14.1 Purpose

---

The activity is designed to identify safety requirements related to the hazardous events or hazardous conditions identified in the PHL 5.12/PHA 5.13 and FHA 5.20 and also identify other safety-related requirements, for example legal, customer requirements (RFP 5.4), standards and more.

### 5.14.2 Deviations

---

203.2.2: This also includes the RFP 5.4, H VAS-E [24], H FordonSäk [21] and *chapter 6* for software.

203.2.2.e: “Appendix A” has been replaced with *chapter 6*.

### 5.14.3 Comparable Activities/Documents

---

For software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 203, Safety Requirements/Criteria Analysis. This differs marginally and could be applied as an alternative.

GEIA-STD-0010 has a more detailed description as to which data can be included in a SRCA (203.2.5). If GEIA-STD-0010 is used the word “federal” may be deleted under 203.2.5.1.1.

### 5.14.4 Further Information

---

The supplier must identify critical elements and functions in a technical system as early as possible. The intention is that, based on this, the requirements must be defined that prevent these critical parts from malfunctioning, see activity S13, Safety Critical Functions (SCF 5.11). A SRCA may be documented in accordance with DI-SAFT-80101B, System Safety Hazard Analysis Report [8].

### 5.14.5 Input Data

---

In order to carry out a SRCA, PHL 5.12/PHA 5.13 or FHA 5.20, requirements from the RFP 5.4 are required along with relevant legislation and regulations.

### 5.14.6 Output Data

---

Documentation for requirements specifications (SSS, SI, IRS), identification of critical software (SCCSC) and documentation for a Risk Log (see the HTRR 5.9) and CIL (see the SCF 5.11). SV 5.24 is closely linked to the SRCA.

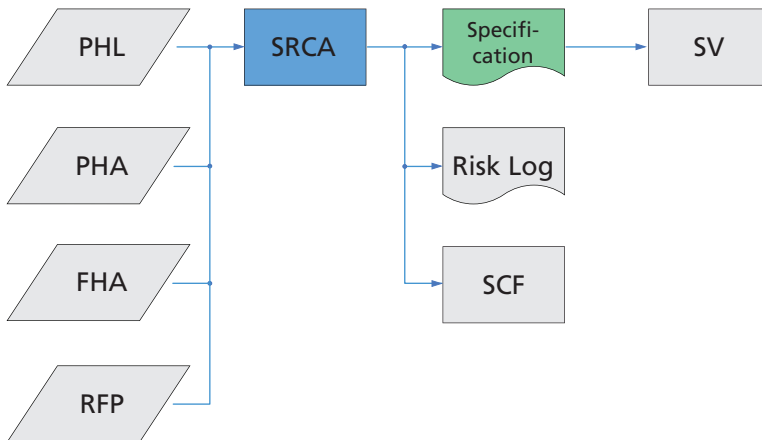


Figure 5:15 Safety Requirements/Criteria Analysis (SRCA)

## 5.15 SUBSYSTEM HAZARD ANALYSIS (SSHA) – TASK 204

### 5.15.1 Purpose

---

The activity is designed to identify potential additional hazardous events after the initial risk identification and also to verify compliance with safety requirements for the technical subsystems.

### 5.15.2 Deviations

---

204.2.3: The specified standards, DOD-STD-2167, DOD-STD-2168 and MIL-STD-1679 R, are replaced by the instructions in *chapter 6*.

204.3.1 c, d, e: These can also be defined in the SSPP 5.5.

### 5.15.3 Comparable Activities/Documents

---

For software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 204, Subsystem Hazard Analysis (SSHA). This differs marginally and could be applied as an alternative.

GEIA-STD-0010 has a more detailed description of what data can be included in a SSHA (204.2.5). If GEIA-STD-0010 is used, decommissioning is additional (204.2.5.3 b (2)).

GEIA-STD-0010 specifies that any accident risks must be recorded, not just the residual risk of accidents (204.3.b).

Note that regardless of the standard used, the Risk Log for the technical system, according to H SystSäk E, must always cover all identified risks of accidents.

### 5.15.4 Further Information

---

This activity is carried out if the technical system consists of a number of technical subsystems or components. Accident risks that may be associated with failure modes or operational management should be analysed. In addition, risk-reducing measures should be identified. A SSHA may be documented in accordance with DI-SAFT-80101B, System Safety Hazard Analysis Report [8]. See *chapter 8* for examples of analysis methods.

### 5.15.5 Input Data

---

A concept or a design description, flow chart, operating profile and often a PHA 5.13 or FHA 5.20 are needed in order to implement a SSHA.

### 5.15.6 Output Data

---

A SSHA and support documentation for a SHA 5.16, SCF 5.11 and Risk Log (see HTRR 5.9).

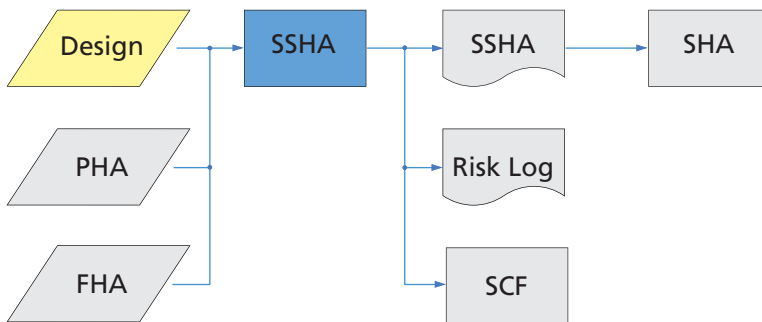


Figure 5:16 Subsystem Hazard Analysis (SSHA)

## 5.16 SYSTEM HAZARD ANALYSIS (SHA) – TASK 205

### 5.16.1 Purpose

---

The activity is designed to identify potential additional hazardous events, depending on the interaction between the technical sub-systems, and also to verify compliance with the safety requirements for the technical system.

### 5.16.2 Deviations

---

205.2.1 (e) The word “reasonable” should be construed as the use that COULD REASONABLY BE EXPECTED to be consistent with product liability law [35].

205.2.3: The specified standards, DOD-STD-2167, DOD-STD-2168 and MIL-STD-1679, are replaced by the instructions in *chapter 6*.

205.3.1 d: These can also be defined in a SSPP.

### 5.16.3 Comparable Activities/Documents

---

For an SHA focusing on software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 205, SHA. This differs marginally and could be applied as an alternative. GEIA-STD-0010 has a more detailed description of what data can be included in a SHA (205.2.5). If GEIA-STD-0010 is used, decommissioning is additional (205.2.5.3 b (2)). GEIA-STD-0010 specifies that any accident risks must be recorded, not just the residual risk associated with accidents (205.3.b).

Note that regardless of the standard used, the Risk Log for the technical system, according to H SystSäk E, must always cover all identified risks of accidents.

### 5.16.4 Further Information

---

A SHA is implemented when the technical system's design has been determined. It focuses on the interaction between the different technical subsystems and takes the system aspects into consideration. In addition, collaboration with other technical systems must be considered. Analysis techniques similar to the SSHA 5.15 can be used. See *chapter 8* for examples of analysis methods.

The following are given special consideration:

- the technical subsystem's interaction with other technical subsystems
- compliance with defined safety requirements
- combinations of independent and dependent errors
- whether the technical system degenerates during normal use
- whether changes in the technical system can affect system safety.

A SHA may be documented in accordance with DI-SAFT-80101B, System Safety Hazard Analysis Report [8].

### 5.16.5 Input Data

---

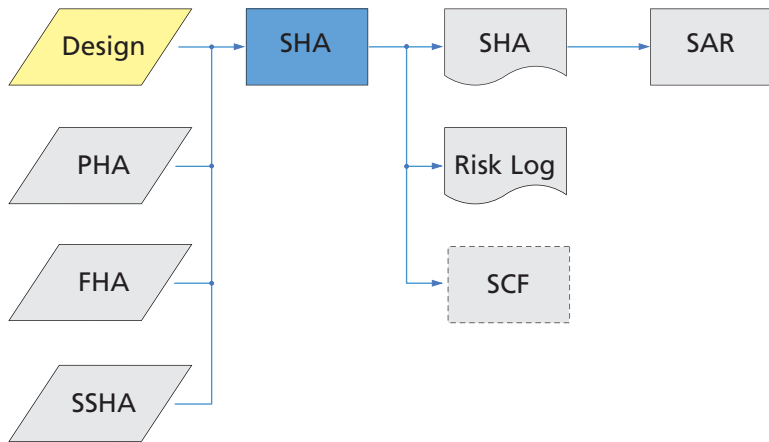
A system and design description, operating profile and often a PHA 5.13, FHA 5.20 and SSHA 5.15 may be required in order to implement a SHA.



### 5.16.6 Output Data

---

A SHA supports documentation for a SCF 5.11 and input data for a Risk Log (see the HTRR 5.9).



*Figure 5:17 System Hazard Analysis (SHA)*

## 5.17 OPERATING AND SUPPORT HAZARD ANALYSIS (O&SHA) – TASK 206

### 5.17.1 Purpose

---

The activity is intended to analyse the technical system in terms of accident risks from a user's perspective and to evaluate the regulations and instructions.

### 5.17.2 Deviations

---

206.2.2: The supplier's production-related operations are not subject to Swedish conditions as these are regulated by the Work Environment Act (AML) [2]. However, production to be carried out by the Armed Forces' personnel is covered by the paragraph.

206.3.1 c: This may also be defined in the SSPP 5.5.

### 5.17.3 Comparable Activities/Documents

---

For decommissioning, see also RADS 5.34.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 206, Operating and System Hazard Analysis. This differs marginally and could be applied as an alternative.

GEIA-STD-0010 has a more detailed description as to which data can be included in an O&SHA (206.2.5). If GEIA-STD-0010 is used, decommissioning may have to be considered (206.2.5.3 b (2)). GEIA-STD-0010 specifies that any accident risks must be recorded, not just the residual risk associated with accidents (206.3.b).

Note that regardless of the standard used, the Risk Log for the technical system, according to H SystSäk E, must always cover all identified accident risks.

#### 5.17.4 Further Information

---

FMV's HMI handbook for technical officers provides further information [14].

An O&SHA may include the use and management of the technical system, for instance, testing, maintenance, modifications, training and installation.

User phases which should also be considered include emergency phases, such as emergency evacuation and rescue operations.

An O&SHA may be documented in accordance with DI-SAFT-80101B, System Safety Hazard Analysis Report [8].

See *chapter 8* for examples of analysis methods.

#### 5.17.5 Input Data

---

A system description, operations profile and usually a PHA 5.13, SHA 5.16, SSHA 5.15 and HMI reports are required to implement an O&SHA. For investigation and analysis of usage instructions, a draft form is required as a minimum.

5.17.6 Output Data

---

O&SHA and the input data for the Risk Log (see HTRR 5.9) and SI 5.25 and TSR 5.32 are generated.

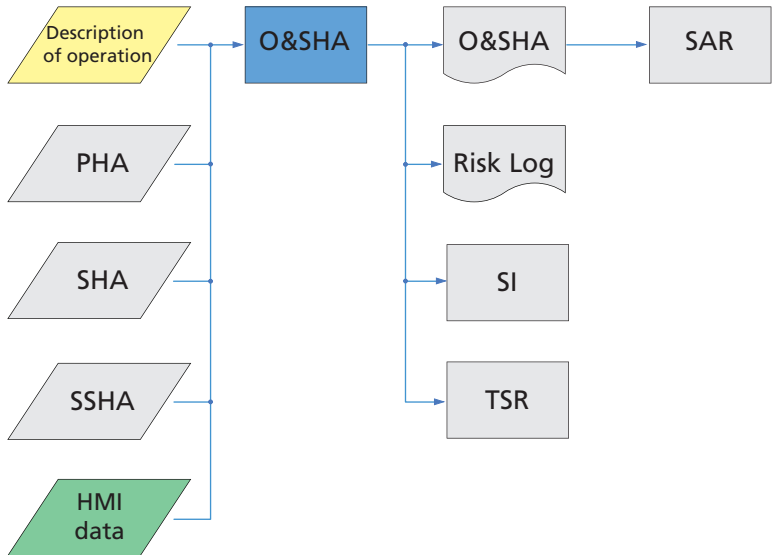


Figure 5:18 Operating and Support Hazard Analysis (O&SHA)

## 5.18 HEALTH HAZARD ASSESSMENT (HHA) – TASK 207

### 5.18.1 Purpose

---

The activity is designed to identify health-related risks and to evaluate hazardous materials and substances. The support documentation should provide information for the systematic environmental work which must be conducted by the employer in the organization that will use the technical system.

### 5.18.2 Deviations

---

207.2: The effects on the external environment are dealt with in the activity EHA 5.19.

207.2.2: Supplier production-related operations are not subject to Swedish conditions as these are regulated by the AML [2]. However, production related to the technical system, to be carried out by the Armed Forces' personnel, is covered by the paragraph.

207.3.1 d: This may also be defined in SSPP 5.5.

### 5.18.3 Comparable Activities/Documents

---

For decommissioning, see also RADS 5.34. Applicable requirements are specified in the Swedish Working Environment Authority's (AV's) instructions, Swedish environmental legislation and other relevant agency/authority regulations. In the UK, Operating and Health Hazard Analysis (OHHA) and Control of Substances Hazardous to Health (COSHH) are applied.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 207, Health Hazard Assessment. This differs marginally and could be applied as an alternative. GEIA-STD-0010 has a more detailed description as to which data can be included in a HHA (206.2.3) but lacks the instructions as to what the review should cover which is specified in MIL-STD-882C paragraph 207.2.2. GEIA-STD-0010 specifies that all risks must be registered, not just residual risks (206.3.b).

Note that regardless of the standard used, the Risk Log for the technical system, according to H SystSäk E, must always cover all identified risks of accidents.

A response to MIL-STD-882C paragraph (207.2.3.4.2) is that for each chemical product there should be a Safety Data Sheet (SDB) available. The SDB's format is governed by the European Council's regulation [13] (REACH).

### 5.18.4 Further Information

---

Through an inventory of hazardous substances and other hazards/hazardous conditions for which users may be exposed during the technical life of the system, a good basis for further examination is created. Analysis and assessment should be made in accordance with the regulations as stipulated by the Chemicals Inspectorate and the Work Environment Authority.

The following factors should be considered in the assessment:

- the amount of hazardous materials or hazardous exposure (extent of)
- the emissions during planned use
- the emissions in the event of a hazardous event
- the hazardous waste from the technical system
- how hazardous materials are disposed of
- the required protective equipment needed when using the technical system
- indicators for the release of hazardous substances
- the number of exposed people
- possible protective measures.

The following factors should be considered during the evaluation:

- permitted limit values, both for short- and long-term exposure
- chronic health effects
- carcinogenic materials
- contact allergy risk
- fire propensity.

A HHA may be documented in accordance with DI-SAFT-80106A, Health Hazard Assessment Report (HHAR) [12].

See *chapter 8* for examples of analysis methods.

### 5.18.5 Input Data

---

A system description, operations profile and usually a PHA 5.13, SHA 5.16, SSHA 5.15, O&SHA 5.17, HMI and material information (material list/material declaration) are required to implement a HHA.

### 5.18.6 Output Data

---

A HHA, SDBs and the support documentation for a Risk Log (HTRR 5.9).

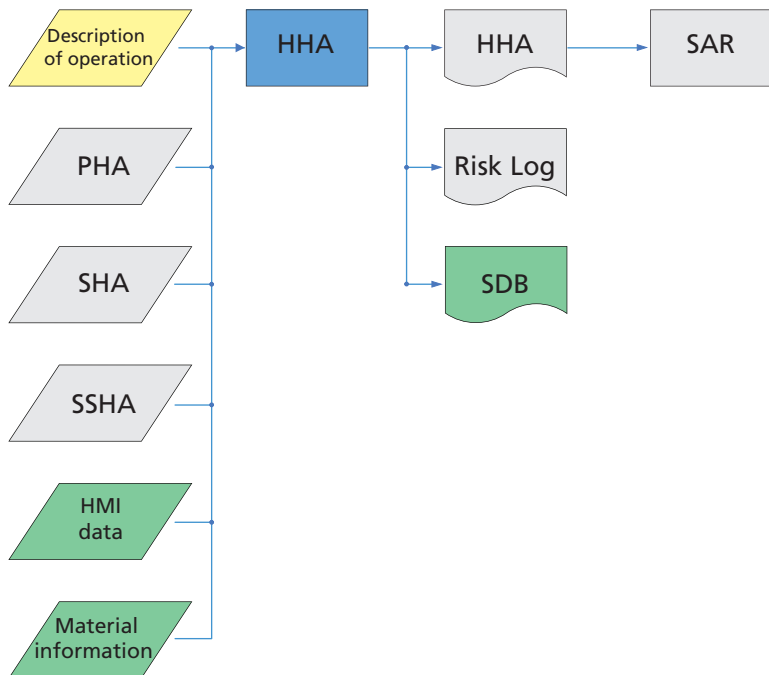


Figure 5:19 Health Hazard Assessment (HHA)

## 5.19 RISK ANALYSIS FOR EXTERNAL ENVIRONMENT (EHA) – S21

### 5.19.1 Purpose

---

The purpose of the risk analysis for the external environment (EHA - Environmental Hazard) is to evaluate potential accidents, due to hazards/hazardous conditions, which can occur during the management of the technical system. The management ranges from the first time the technical system is put into use to its destruction or decommissioning. The environmental impact for normal emissions (not accident related) for all handling is generally taken care of in the ordinary environmental work. When the impact on the environment is not taken into account, the equivalent environmental work should be carried out within the framework of the EHA activity. The activity is carried out by the supplier.

### 5.19.2 Activity Description

---

This activity deals with hazardous events that can lead to the release of emissions into the immediate environment.

The input data for this analysis is the Operation and Support Hazard Analysis (O&SHA 5.17, PHL 5.12, PHA 5.13, Subsystem Hazard Analysis (SSHA 5.15), System Hazard Analysis (SHA 5.16), experience from, for example, fault reports (FRACAS 5.28 and material information (material list/material declaration). For the EHA analysis, the event tree and fault frequency analysis are recommended, see *chapter 8*.

#### *Risk Analysis for External Environment (EHA)*

---

The first step in the environmentally oriented analysis (EHA) is to identify substances that are potentially hazardous to the external environment. Based on the input data, the amount of damage that may result from a hazardous event is calculated. Subsequently, an assessment of the likelihood of a hazardous event occurring is carried out in order to estimate the risk of an accident in accordance



with *H SystSäk E Part 1*. The final step is to eliminate or reduce the risk in order to comply with this requirement. This can be achieved through reconstruction, the introduction of protective contrivances or through the introduction of operating instructions. Even emissions caused by emergency situations, such as fire, must be taken into consideration.

Consideration is also given to the following factors:

- The technical system's design/condition at each phase of its service life.
- Peripheral equipment that is used and its impact on the technical system.
- Expected operating environment and constraints.
- Abnormal environments to which the technical system may be subjected.

The analysis should:

- report that legal requirements are met
- report that requirements in the order are fulfilled
- identify the accident risks that must be reduced in accordance with the requirements in the order.

The analysis should identify:

- Activities that may cause hazardous situations, when they occur and what measures are required to minimize risk during these activities/time periods.
- Hazardous materials/substances that are found in the technical system, or that may be produced, for example, in the event of fire, enemy attack etc.
- Necessary amendments to the design of hardware/software/documentation, auxiliary appliances, tools or maintenance equipment/test equipment designed to eliminate or control the risk of accidents occurring.
- Requirements for safety devices and safety equipment to protect the external environment when hazardous events occur.

- Warnings, instructions, signs, precautionary measures and, in particular, procedures in the event of, for example, a fire.
- Requirements for safety training and requirements for special authorities to take action/competence of personnel.

The analysis will document system safety ratings of the measures that are relevant to all phases during the technical system's service life. See *chapter 8* for examples of analysis methods.

### *Activities Relating to Environmental Impact for Normal (Planned) Emissions*

---

For emissions formed during normal (planned) use, destruction or decommissioning, hazardous materials/substances should be identified. See RADS 5.34. This can be done through the development of material information and that the material is analysed in terms of prevailing legislation. Emissions during use and decommissioning are calculated or measured. Comparisons are then made with the law and the requirements in the order.

Concessions and other operations subject to authorisation are dealt with outside of H SystSäk E. However, documentation from the EHA activity can also be used for this.

On analysis and review, the following factors may be taken into consideration:

- The technical system's design/condition during each phase of its service life.
- Peripheral equipment/tools that are used and their impact on the technical system.
- Expected operating environment and constraints.

The analysis should:

- demonstrate that legal requirements are met
- demonstrate that requirements in the order are fulfilled
- identify those hazardous substances that may be replaced by less hazardous substances.

The results of the analysis should be documented.

The picture below outlines the principles which make it easier to understand the impact on the external environment. The ordinary system safety work begins with one of the Armed Forces-defined activities (documented in a SSMP according to the SSP 5.1) with the determining requirements in TTEM 5.3. DesignA transforms the requirements from TTEM 5.3 to a RFP 5.4. The supplier defines the activities planned in SSPP 5.5 and examines both the health and environmental impact of the technical system (during operation and decommissioning) in terms of the laws and regulations. This forms the basis of the safety analyses. Risks that have been identified and dealt with are documented in the Risk Log and the results of the safety work are documented in a SAR 5.21. The SCA 5.27, which is based on the SAR 5.21, forms the basis of the Safety Statement (SS 5.31) and the Central Safety Compliance Decision (CSSB 5.33). In order to implement complete system safety work, support documentation is required from environmental operations in the form of material information, a recycling manual and SDBs [13].

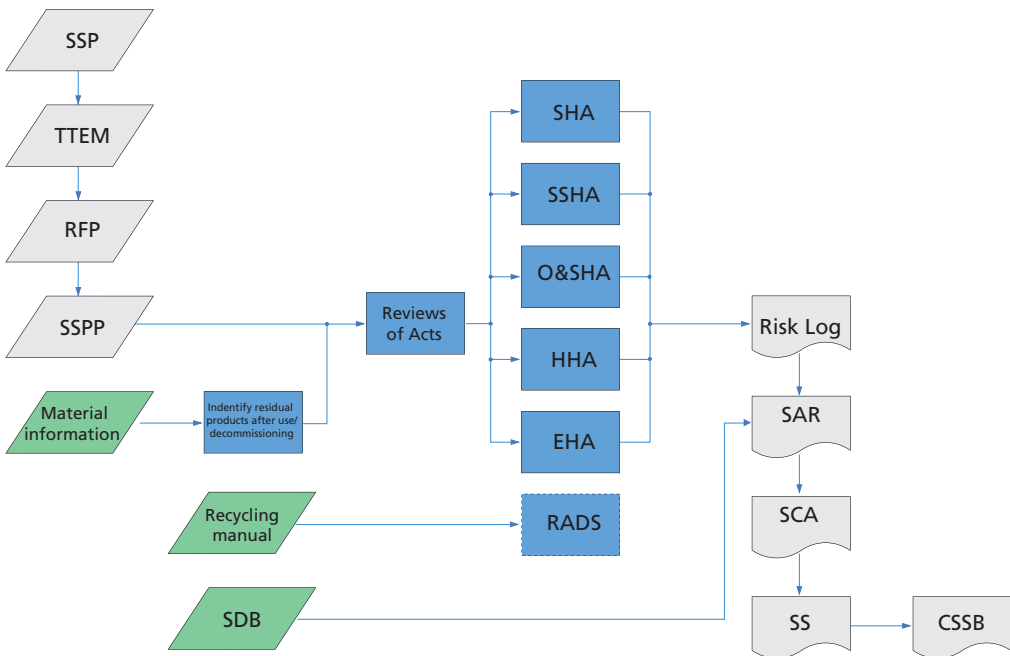


Figure 5:20 Environment-Related Activities

### 5.19.3 Input Data

---

A system description, operations profile and usually a PHA 5.13, SHA 5.16, SSHA 5.15, O&SHA 5.17, FRACAS 5.28, HMI documentation [14] and material information (material list/material declaration) are required to implement a HHA.

### 5.19.4 Output Data

---

A risk analysis of the external environment (EHA) and the support documentation for a Risk Log (HTRR 5.9).

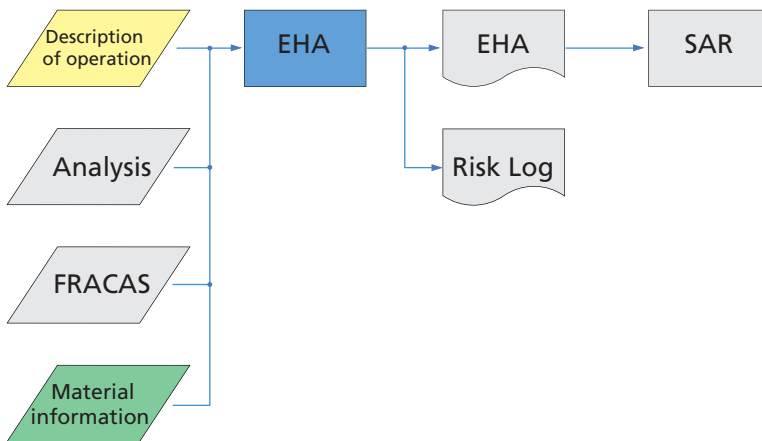


Figure 5:21 Risk Analysis of External Environment (EHA)

## 5.20 FUNCTIONAL HAZARD ASSESSMENT (FHA) – S22

### 5.20.1 Purpose

---

To provide an early identification of functionally related accident risks for individual systems or systems as part of the system of systems. A FHA is used to identify and classify the system functions (from a criticality point of view) and to identify functional defects. The classification is used to identify SCF 5.11. This provides the possibility of distributing criticalities in a system architecture, both functionally and physically, to the various elements which make up the technical system, such as hardware, software or the HMI parts. For a definition of safety-critical and safety-related functions/components, see SCF 5.11.

By applying FHA early on during a procurement/development process it is possible to identify the elements/components to be analysed further in the continued analysis activities and to identify safety-critical software which can be dealt with in accordance with *chapter 6*.

The corresponding activity is the civilian standard GEIA-STD-0010 Task 208 [26]. Note that for aviation products, which require approval from Transportstyrelsen, FHA based on Luftfartverket's regulations should be used. For aircraft and related equipment there is a guide in *section 5.20.5*.

This activity is not described in the previous edition of H SystSäke but is internationally applied, so the English name is used. The activity is carried out mainly by the supplier.

### 5.20.2 Activity Description

---

The supplier will implement and document a FHA in order to provide a risk assessment of a concept or system.

Based on available data, which also includes material from the fault reports (FRACAS 5.28) for similar systems, the identified functions are analysed (including input data, output data, interactions with other systems) to distribute the identified malfunctions to the subsystems affected, as well as to evaluate the severity of these malfunctions.

As part of the efforts made to address potential malfunctions, safety requirements must be identified in the requirement specifications, see SRCA 5.14. In addition, constructive measures are identified which can eliminate or reduce the risk of accidents to the required risk level.

In order to implement a FHA, the following points must be identified and taken into account:

- The hardware components are identified (the physical composition of the technical system with its subsystems down to the major components).
- The critical interaction/synergy between the physical subsystems. Both physical and functional interactions must be considered.
- A functional description of the interaction between subsystems and components is implemented.
- A listing of the risks of accidents, loss of function and malfunctions. As with a fault modes and effects analysis (FMEA), likely effects and associated effects must be identified and taken into consideration.
- An evaluation all the identified risks of accident. The evaluation should only be made with regard to the effect/consequence. No numerical evaluation of probabilities should be made at this early stage of analysis operations. Consequences are defined according to SSPP 5.5.
- Identify safety-critical features/properties (both CIL and SIL) according to the 5.11.

- Evaluate whether the identified features can be included in the design or not.
- List all identified safety requirements to be included in the specifications, see SRCA 5.14. If requirements are fulfilled, this will lead to a reduced occurrence probability for hazardous events which is reflected in the subsequent analyses (PHA 5.13, SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18 and EHA 5.19).

### 5.20.3 Input Data

---

A concept and system description, operating profile and usually experiences from failure report procedure in FRACAS 5.28.

### 5.20.4 Output Data

---

A FHA report represents the output data from the activity. This should include:

- A simpler system description, mainly descriptive, of the physical components and functions identified.
- Results of a FHA:
  - a breakdown of the technical system (including system of systems) in the functions and how these are realized through physical devices. The format of the Work Breakdown Structure (WBS) can be used
  - a listing of all the system functions
  - a listing of all the safety-critical functions
  - a description of how the safety-critical functions relate to the software architecture, including, for example, criticality levels
  - a listing of all the identified safety requirements.

## 5 Description of Activities

- A FHA can also generate:
  - a list of the accident risks for a PHL 5.12/PHA 5.13
  - an input to FMEA or FMECA
  - a method to verify fault scenarios, see SAE ARP 4761 [36] and *section 5.20.5*
  - an identification of the current construction status for safety-critical interactions in the technical system.

Furthermore, import data are provided for the Risk Log in accordance with HTRR 5.9 and SRCA 5.14.

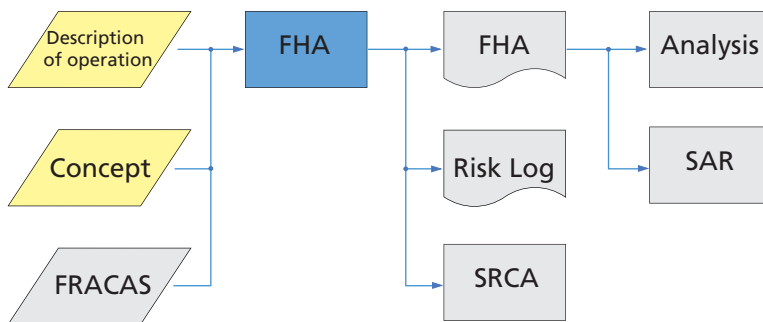


Figure 5:22 Functional Hazard Assessment (FHA)

### 5.20.5 FHA for Civil Airborne Systems

---

This section describes the activity FHA for civil airborne systems and the description is based on the civilian standard SAE ARP4761 (Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment) [36].

### 5.20.6 Purpose

---

FHA is defined as a systematic evaluation of functions on complete aircraft and subsystems for the identification of error events that these functions can cause. The identified error events are classified according to their effects (worst consequence/accident outcome).



FHA is carried out early in both full flight and at the subsystem level and is a first step in the early identification of safety-critical functions and related system safety requirements. In this way, FHA provides a basis to build robust and fault tolerant craft/subsystems.

FHA will focus on the function in order to be, as far as possible, independent of the realization of the function.

### 5.20.7 Activity Description

---

The methodology prescribed in SAE ARP4761 [36] is the same for both complete aircraft and subsystems and can be summarized as follows:

- Identify all functions of the aircraft/subsystem.
- Identify and describe the functions' various error events. Take into account both single faults and multiple faults in the normal and degraded/deviating conditions and environments. In the event that combination errors of functions are more serious than the ingoing functions, the combination error will be analysed and entered as a new unique malfunction in FHA at the complete aircraft level.
- Evaluate the effect (worst consequence/accident outcome) of all error events which a function can cause by analysing possible/probable damage/injury to the complete aircraft, crew and passengers.

From experience it has been proven to be beneficial to also consider possible risk-reducing measures during the analysis in order to eliminate or control the error events that are critical to safety.

- Define and allocate system safety requirements (criticality/development assurance level (DAL), redundancy, independent error probabilities) based on the results from the FHA of the design.
- Identify the verification method in order to evaluate whether requirements have been fulfilled in terms of the defined system safety demands.

FHA, at the complete aircraft level, is a qualitative evaluation of an aircraft's functions that have been defined at the beginning of an aircraft's development.

**Note:** In order to carry out a FHA at complete aircraft level requires a sound knowledge and experience from similar aircraft with similar functions and it is therefore recommended that you seek consultation with specialists in relevant fields.

FHA at the subsystem level is a qualitative evaluation of the functions of a subsystem in the aircraft.

**Note:** The objective of the FHA at subsystem level is to identify and analyse faults in the hardware or software components that are supposed to form part of the new or modified subsystem.

### 5.20.8 Input Data

---

Input data to a FHA at complete aircraft level includes:

- a list of all the functions at complete aircraft level
- aircraft requirements and customer requirements.

Input data to a FHA at the subsystem level includes:

- a list of functions at the subsystem level to take into consideration
- FHA at complete aircraft level or the next higher subsystem level
- a functional diagram showing the external interfaces
- defined design requirements and design decisions and the reasons for the decisions.

### 5.20.9 Output Data

---

The following information should be documented:

- a description of the operating phases
- a list of the features that have been analysed in FHA
- the degraded/abnormal conditions and habitats identified during the analysis
- a description of the consequences of error events
- a classification of the effect of each error event
- the identified accident risks for documenting in the Risk Log
- the references to material that confirms and justifies the analysis in FHA
- the authentication methods for defined system safety requirements.

## 5.21 SAFETY ASSESSMENT REPORT (SAR) – TASK 301

### 5.21.1 Purpose

---

The activity intends to evaluate and summarize the risks associated with the technical system before testing or use. For Swedish conditions, this is usually the basis for a SCA 5.27 which must be provided.

### 5.21.2 Deviations

---

301.2.d (5): “Material Safety Data Sheet” replaced by SDB according to the European Council Regulation (REACH) [13].

301.3.1 c: Who should sign the SAR may be regulated in SSPP 5.5. The signing of the SCA 5.27, is normally carried out by an authorized signatory of the supplier or the person specially appointed to do so. The signing of the SAR can therefore be at a lower level.

### 5.21.3 Comparable Activities/Documents

---

The UK uses a similar Safety Case Report (Def-Stan 00-56 [42]).

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 301, SAR. This differs marginally and could be applied as an alternative.

### 5.21.4 Further Information

---

The use of SAR is to report on residual risks with the technical system in use and to estimate the related numerical risk. SAR can also be used as a source of information on the acquisition of fully developed systems.

A SAR may be documented in accordance with DI-SAFT-80102B, SAR [9].

### 5.21.5 Input Data

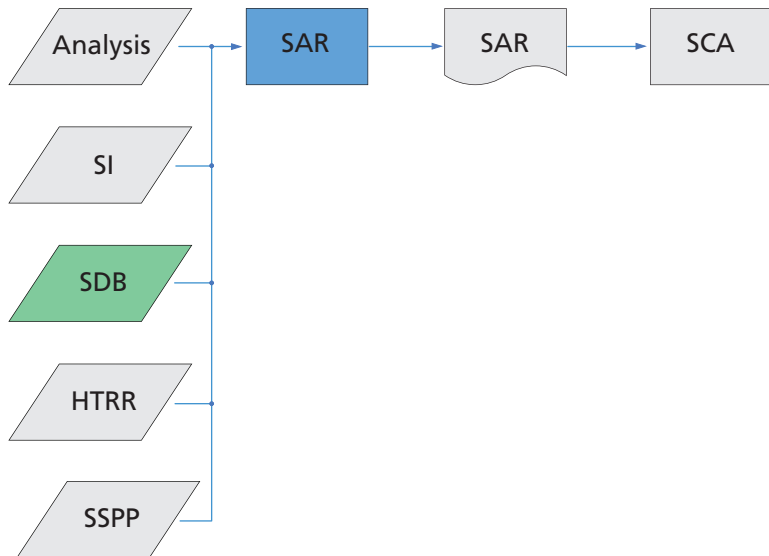
---

As support documentation for a SAR, all relevant safety documentation is gathered. Main documents come from the completed analyses 5.12, PHA 5.13, SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19, FHA 5.20 and Related Risk Log (Hazard Log), (see HTRR 5.9), and Safety Instructions (SI) in accordance with SI 5.25 and SDBs. The various support documentation for a SAR can be incorporated in a SAR or referred to from a SAR.

### 5.21.6 Output Data

---

A SAR, which forms the basis for the SCA 5.27.



*Figure 5:23 Safety Assessment Report (SAR)*

## 5.22 TEST AND EVALUATION SAFETY – TASK 302

Not applicable to Swedish conditions. Replaced by requirements from the testing authorities/bodies.

## 5.23 SAFETY REVIEW (SR) – TASK 303

### 5.23.1 Purpose

---

The full name of the activity is “Safety Review of Engineering Change Proposals, Specification Change Notices; Software Problem Reports and Request for Waiver Deviation” (ECP/SCN/SPR/PTR/STR). This title has been shortened to Safety Review (SR).

The activity is designed to evaluate changes and deviations from a safety perspective.

### 5.23.2 Deviations

---

303.3.1 b, c, d: This can also be adjusted in the Configuration Management Plan (CM Plan) or SSPP 5.5.

### 5.23.3 Comparable Activities/Documents

---

For software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has a similar activity, Task 303, Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Request for Deviation Waiver. This differs marginally and could be applied as an alternative.

### 5.23.4 Further Information

---

Any amendment must be reviewed to ensure new risks do not arise when the amendment is introduced. The classification of changes must be defined in the configuration plan or equivalent (safety-related changes are often class I).

An amendment proposal may be documented according to DI-SAFT-80103A, Engineering Change Proposal [10] and a deviation in accordance with DI-SAFT-80104A, Waiver or Deviation System Safety Report [11].

### 5.23.5 Input Data

---

A basis for the amendments are fault reports (FRACAS 5.28) or results of analysis such as a SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19 and related Risk Log (Hazard Log), see HTRR 5.9.

### 5.23.6 Output Data

---

The reports constitute amendment proposals and deviation reports (ECP/SCN/SPR/PTR/STR).

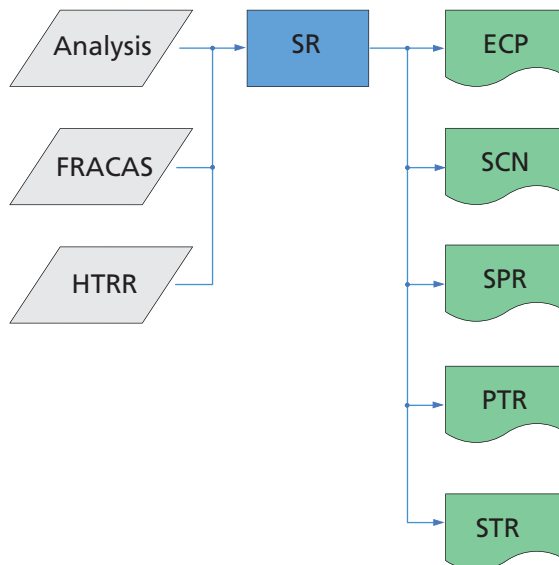


Figure 5:24 Safety Review (SR)

## 5.24 SAFETY VERIFICATION (SV) – TASK 401

### 5.24.1 Purpose

---

The activity intends to define and implement the verification (testing, analysis, review and demonstrations) that is needed to be able to verify the safety.

### 5.24.2 Deviations

---

401.2.a: “Catastrophic hazards” is replaced for Swedish conditions with HAZARDOUS EVENTS OR HAZARDOUS CONDITIONS MAY CAUSE INJURY CLASS 1. “Marginal and Negligible hazards” are replaced by OTHER HAZARDOUS EVENTS OR HAZARDOUS CONDITIONS.

### 5.24.3 Comparable Activities/Documents

---

For software, see *chapter 6*.

The civilian standard GEIA-STD-0010 [26] has an equivalent activity, Task 401, SV. This differs marginally and could be applied as an alternative. GEIA-STD-0010 has a more detailed description of the type of data that can be included in a SV (401.2.2).

### 5.24.4 Further Information

---

Many of the safety requirements must be verified through analysis and simulations, testing only is often inadequate. If there are design changes, a new verification must take place. Testing often acts as a support to the performed analysis. Completed tests can be documented in accordance with DI-SAFT-80102B, SAR [9] or in separate test reports.



### 5.24.5 Input Data

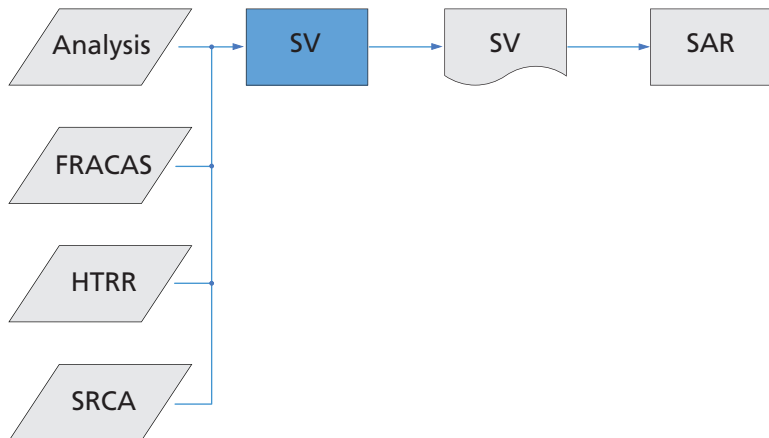
---

Support documentation for safety verification are analyses such as SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19 and EHA-related Risk Log (Hazard Log) HTRR 5.9 and SRCA 5.14.

### 5.24.6 Output Data

---

Report from the verification of safety requirements provides a basis for the overall validation of the technical system and input data to SAR 5.21.



*Figure 5:25 Safety Verification (SV)*

## 5.25 SAFETY INSTRUCTIONS (SI) – S41

### 5.25.1 Purpose

---

To provide a complement to structural measures taken to prevent the incorrect use of the technical system. Basic requirements for the establishment of these are the analyses (SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, and EHA 5.19) in which the technical system's design and the expected use have been analysed. The activity is often carried out by the supplier.

### 5.25.2 Activity Description

---

It is often impossible to design systems that are safe, irrespective of how they are handled. In order to improve safety, the use of certain SI needs to be stated. When these are incorporated in the instructions in the manuals and other safety-related information they are best broken down into the different handling phases that are relevant to the technical system.

The examples listed here are some points to consider for the various handling phases:

- Storage:
  - minimum and maximum storage temperature
  - maximum and minimum humidity
  - maximum temperature change rate during storage
  - maximum service life with the above climate
  - maximum stacking height
  - maximum electromagnetic irradiation.
- Transport
  - maximum acceleration or permissible transport modes
  - allowed transport packaging
  - maximum transport times
  - requirements for special transportation to secure the load.

- Handling
  - packaging requirements when handling
  - maximum time for storage when first opened
  - requirements for special handling procedures
  - for software, see *chapter 6*.
- Use
  - restrictions regarding use
  - maximum and minimum temperature
  - maximum and minimum humidity
  - risk areas for blasts (splinters), sound pressure, heat, electromagnetic irradiation, crushing etc.
- Decommissioning
  - limitations in the disposal methods
  - requirements for the handling of waste products.

### 5.25.3 Input Data

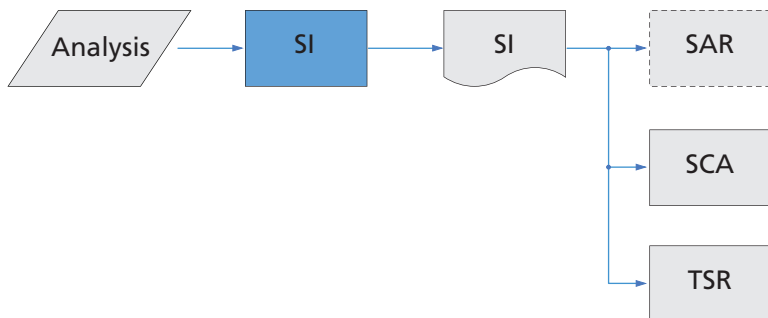
---

Support documentation for the SI are the analyses such as SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18 and EHA 5.19.

### 5.25.4 Output Data

---

SI as the basis for SCA 5.27 and TSR 5.32.



*Figure 5:26 Safety Instructions (SI)*

## 5.26 SAFETY COMPLIANCE ASSESSMENT – TASK 402

This activity is governed entirely by the SCA – S42 5.27.

## 5.27 SAFETY COMPLIANCE ASSESSMENT (SCA) – S42

### 5.27.1 Purpose

---

To report the supplier's position on the technical safety of the system. The SCA is also included in the support documentation upon which DesignA provides a SS 5.31. The SCA may be an activity made at the end of the order. In the SCA a review should also be made of the existing legislation to ensure it is met.

The summarised support documentation is usually documented in a SAR 5.21).

### 5.27.2 Activity Description

---

The SCA is a summary of the system safety work that has been carried out, a review of current legislation, a response from the developing supplier that the technical system's safety is acceptable for use, assuming the specified safety precautions are followed (SI 5.25).

For testing/trial at Armed Forces' facilities and with the Armed Forces' personnel, health and safety legislation applies, which explains why the activity is not addressed under the SCA activity.

SCA is based on the activities that were agreed in the SSPP, in which the analyses (SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19, FHA 5.20 and those parts of RADS 5.34 that have been implemented), SI 5.25, experiences from fault reports (FRACAS 5.28) and the evaluation of the SV 5.24 are of major importance. The results of these are shown in a SAR 5.21.

As a basis for the SCA all the safety activities carried out during the development of the technical system are found. These activities are documented as and when they are implemented. In the SCA, reference is made to these documents or a summary is made of the activities, which is included in the report.

In principle, the SCA can include the following:

- A report of the safety criteria and requirements used in the development of the technical system, including how risks have been identified, classified and treated, so they can be eliminated or reduced in order to obtain a tolerable safety level.
- Identification and statement that current legislation is complied with.
- Analyses and tests performed to identify risk of accidents and their causes.
- A statement of the measures that have been taken to eliminate or minimize the causes of the risk of accidents. Any points of view from the SSWG 5.8 with regard to the adequacy of the measures.
- A presentation of residual risk and the measures required to achieve tolerable safety, for example SI and personnel training.
- A report of the tests and analyses, with prerequisites, which form the basis for the verification of the safety requirements.
- A report of each hazardous event or hazardous condition that may occur under normal use as unusual and abnormal conditions, together with recommendations and regulations that provide tolerable safety.
- Report on the environmental and health hazardous substances/materials found in the technical system which humans or the environment may be exposed to in the event of hazardous events or hazardous conditions during use, maintenance or decommissioning. Reporting of risks to human health, property or the external environment, together with regulations, warnings and procedures to prevent injury/damage from occurring.
- For chemical products, current SDBs [13] should be available.

- In the SCA there must always be an unequivocal statement from the supplier which, in light of the above-reported measures, indicates that the technical system is safe under the conditions given.
- For the technical system's software elements verification must be reported which, at an increasing level of detail, shows that the software safety requirements for the suppliers' personnel, process, product and production environment are met. A requirements list is a good basis for the SCA. From this it is clear to what extent the requirements have been verified, the reasons for incomplete verification and, for requirements that have not been met, proposals for action in the event of an incomplete coverage of requirements etc. Examples of the latter may be product/process improvements, training and SI.

The SCA must be signed by a supplier's authorized signatory or someone delegated by them. Whoever signs the SCA can be regulated in the SSPP 5.5.

### 5.27.3 Input Data

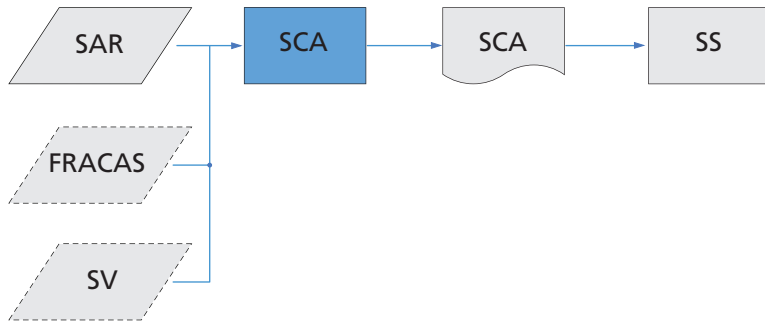
---

The basis for the SCA is the SAR 5.21 and may also be FRACAS 5.28 and SV 5.24.

#### 5.27.4 Output Data

---

The SCA forms the basis for the SS 5.31. For examples of the SCA see *appendix 1*.



*Figure 5:27 Safety Compliance Assessment (SCA)*

See examples of SCA in *appendix 1*. The example is available as a file on H SystSäkE CDR.

## 5.28 FAILURE REPORTING, ANALYSIS AND CORRECTIVE ACTION SYSTEM (FRACAS) – S43

### 5.28.1 Purpose

---

To restore safety-related information to those responsible, to improve the technical system's system safety.

The FRACAS should be available from the first test/handling until the technical system has been discontinued. This information can be used for both the actual technical system and for similar technical systems which, for example, use the same subsystem(s). The support for failure follow-up forms a part of the basis for the SAR 5.21 and the SCA 5.21. Even the analyses (SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19 and FHA 5.20) are highly dependent on the information being returned, partly to gain experience and partly to analyse the impact of any changes that may arise from the failure report procedure. The failure report is monitored by the work groups SSWG-1 and SSWG-2 – the work groups can also propose corrective measures. The activity is carried out by the Armed Forces, DesignA and the supplier.

### 5.28.2 Activity Description

---

This is used primarily by the Armed Forces' existing FRACAS. If this is not available a special FRACAS must be established. It is good if many interested parties are satisfied with one and the same reporting system, for example, interested parties interested in both safety and maintenance can use the same data. The purpose of this activity is to ensure that a – preferably standardized – reporting system is established and is kept alive for the lifetime of the technical system.

The reporting system will provide all interested parties with information, regardless of what phase the technical system is in. Therefore, a responsible authority (the Armed Forces, DesignA or the supplier) is appointed to operate and manage the information and how it is reported. During development and procurement, when



suppliers are responsible for the reporting system, work groups for system safety (SSWG-1/SSWG-2) should be provided with the relevant information.

Since the “human factor” today is usually a significant factor in all types of incidents and accidents, it is important to report all incidents where people have directly or indirectly influenced the course of events.

Certain basic conditions must be established and are required before the FRACAS is designed:

- A person responsible for establishing and maintaining the FRACAS.
- Reporting channels during different phases of the technical life of the system, including feedback to the authors of the report.
- A person conducting the analysis and decision-making is to implement corrective action in the technical system.
- The content of the report documentation and format for reporting.
- How the information is intended to be made stable for future systems.

Some basic information must always appear in the FRACAS:

- the technical system’s identity
- the configuration of the technical system and its components
- operational and user conditions when the fault arises
- the fault’s/incident’s nature and scope
- details as to who drew attention to the fault/incident, in order to procure supplementary information. Anonymous reports do not provide this opportunity.

All existing reporting must be used and supplemented so that it can be evaluated from a system safety standpoint. To make this possible, regular and existing reporting, as far as possible, is required in order to be able to provide answers to the following additional questions:

- Was the person injured or was there a risk of injury?
- Was any materiel/property damaged or was there a risk of such? This also relates to the technical system itself.
- Was the external environment damaged or was there a risk of environmental damage?

After the fault has been reported an analysis must be carried out in which the cause of the fault is traced to a physical or operative condition. An investigation should be carried out as to whether the fault can also occur in other systems other than the system the fault report relates to.

The cause of the fault should be verified to ensure that the correct cause of failure has been identified. Corrective action should be decided and implemented. After possible modification of the technical system, particulars of the technical system configuration must be changed.

In the event that fault reports are submitted without action, when the case is completed, any action should be noted on or in connection with the fault report or the special action report.

### 5.28.3 The resulting report

---

Fault reports and action reports that provide input data for the Risk Log (see HTRR 5.9).

Support documentation from the fault follow-up forms a part of the basis for the SAR 5.21 and the SCA 5.27. The analyses (SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19 and FHA 5.20) are also dependent on this report.

#### 5.28.4 Input Data

---

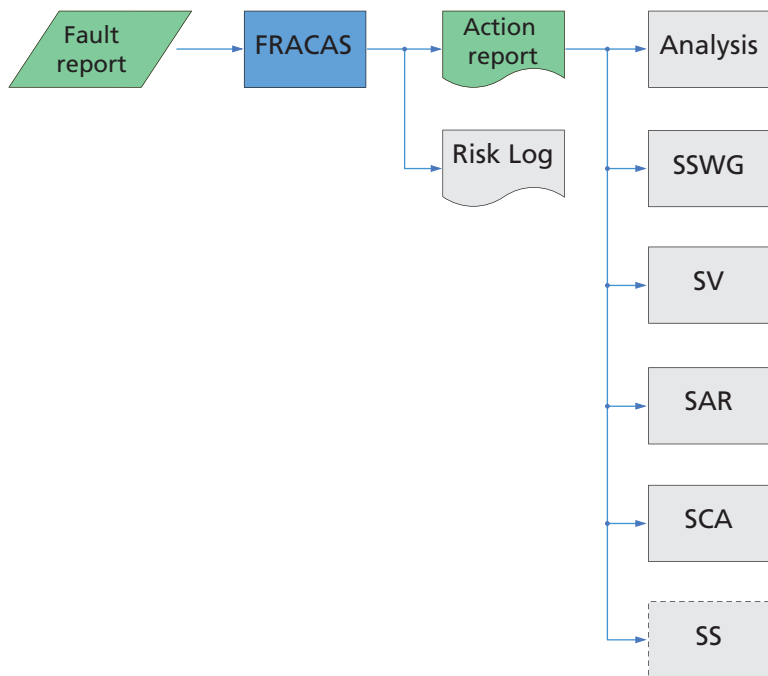
Support documentation for FRACAS includes fault reports and deviation reports of various kinds.

#### 5.28.5 Output Data

---

Action reports provide input data for the Risk Log (see HTRR 5.9).

Support documentation from the fault follow-up forms a part of the basis for the SAR 5.21 and the SCA 5.27. The analyses SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19 and FHA 5.20 are also dependent on this report.



*Figure 5:28 Failure Reporting, Analysis and Corrective Action System (FRACAS)*

### **5.29 EXPLOSIVE HAZARD CLASSIFICATION AND CHARACTERISTICS – TASK 403**

This activity is governed entirely by the H VAS-E [24].

### **5.30 EXPLOSIVE ORDNANCE DISPOSAL SOURCE DATA – TASK 404**

This activity is governed entirely by the H VAS-E [24].

### **5.31 SAFETY STATEMENT (SS) – S51**

#### **5.31.1 Purpose**

---

The purpose of this activity is to formally approve the system safety of developed or procured systems. The SS is a formal decision from DesignA. The decision means that the Armed Forces' established system safety requirements, including requirements relating to risk of injury, are satisfied and that the applicable laws and regulations and other applicable provisions have been complied with.

The SS may require safety precautions to be observed.

The SS for the Sea Trials Command (PTK) is called a Safety Certificate.

Input data for this activity is carried out by DesignA in the form of systems safety and audit work and the supplier's SCA 5.27.

The SS is submitted by DesignA to the Armed Forces as the basis for a CSSB 5.33.

### 5.31.2 Activity Description

---

As part of the development and procurement procedures, the safety of the technical system is continuously examined during the SS 5.7. The number of SRs is regulated in the SS 5.5. Consultation may be made with DesignA's advisory group for system safety (this can be organised as and when required). The supplier's SCA 5.27 is examined when it is presented.

Based on these overall audits and DesignA's own safety activities, a decision regarding the SS can be taken. The SS means that DesignA approves the technical system from a systems safety point of view.

DesignA's safety activities, which form the basis for decisions about the SS, consist of:

- a review of the supplier's system safety activities
- a review of analysis reports
- a review of a Risk Log
- a review of the supplier's SCA 5.27
- ensuring that the support documentation for the handling instructions is available
- ensuring that documentation for safety regulations (SI 5.25) is available
- verification that it has identified what needs to be followed up and how existing reporting systems should be applied
- where appropriate (for specific weapons), to ensure that there is a list as to which ammunition has been approved to be used with the weapon.

A completed examination, as described above, is to be documented in inspection reports. How to conduct the review is described in *H SystSäk E Part 1*.

The production of systems is usually a complicated process which takes a long time. The process often includes several successive field trials and materiel research before series-produced units can be presented to the Armed Forces.

It is the product leader at DesignA that is required have the requisite knowledge of the technical system's risks. Before each measure is taken with the technical system, with regard to testing and trial, it should describe the technical system's residual risks of their intended activities. The technical configuration of the system, the remaining risks, intended activity and any restrictions with regard to its intended activity are described in a SS for its intended activity. This SS will be transmitted to the person designated to carry out its intended activity.

Examples of occasions when the SSs are to be developed are:

- delivery to the Armed Forces of the completed technical system
- delivery to the Armed Forces of the technical system, reserved only for certain trials
- handover to the testing department of the technical system intended for a particular trial
- handover to the head of the PTK of the technical system which consists of a ship (before starting the test run period).

Here, the SS is the equivalent of the Safety Certificate.

Before a technical system is transferred to the Armed Forces (both finished as well as those intended for testing/trials), a SS must be available. However, it is sufficient that the system safety measures, as listed above, are limited to the activity and to the conditions under which the technical system in each individual case is intended to be used.

### *Safety Statement for Weapons and Ammunition*

---

Ammunition objects are a particularly hazardous technical system which, from a system safety point of view, should always be handled in two different ways:

- As ammunition which is often intended for a particular purpose or a particular weapon or other specified use (see, for example, the anti-tank mine, which is intended to be used independently or with particular orientation equipment). This means that the ammunition is safe enough for the intended use in the intended weapon and during the intended use if it is possible to be carried out independently.
- As a stand-alone transport and storage item. Objects always consist of packaging/transport and packaging materials used during storage with certain specified properties and contain a certain number of ammunition units. The requirements of the object is that the ammunition in its packaging must be sufficiently safe when exposed to the intended handling in the intended environment.

Both these aspects will be covered by the separate SS which DesignA will always provide for each ammunition unit.

### *Safety Statement for the Technical System Prior to Testing*

---

The SS is based on a safety analysis focusing on intended testing, a design review and a summary document for the technical system.

### *The Safety Certificate for the Technical System's Vessel Prior to Sea Trials*

---

New ships are built or major modifications to vessels are often conducted in small batches so that it is not reasonable to produce prototypes for testing. Some testing of subsystems can be done separately, but testing must be carried out on a series of vessels – testing is most extensive with the first ship in the series.

Ship testing is usually divided into three phases:

- engineering test trials, the shipbuilding yard's own controls/ tests
- delivery control, DesignA's inspection of the ship to ensure it meets the requirements of the order
- system tests, DesignA's verification that the ship complies with requirements in TTEM.

In all three testing phases, the Armed Forces provides a crew which is at the shipyard's and DesignA's disposal. To solve the task, special sea-test trials are arranged. For PTK, personnel with experience are taken from similar types of ships.

In order to provide personnel with the best possible knowledge of the new ship type, PTK is established before testing is scheduled to start. Meanwhile, at the construction yard, personnel serve principally as advisers to DesignA.

During the testing phases and at the same time as the actual testing, it is PTK's job to produce the documentation required which is not included in the DesignA's delivery.

When system testing has been completed, the ship is handed over from DesignA to the Armed Forces.

The testing of the vessel in accordance with this principle, i.e. during the PTK period, is managed directly by the organization responsible for design, which explains why the CSSB 5.33 and the BOA is not required. (These latter decisions are required only when the first ship is handed over from DesignA to the Armed Forces.)

However, prior to starting the PTK period, it is required that DesignA produces a Safety Certificate for the current technical systems (vessel).

In a special Safety Certificate for the PTK, DesignA – for each measure to be implemented with the technical system under the PTK – must at least specify:

- the technical system (the vessel's) configuration
- residual risks
- the necessary restrictions.



The system safety certificate will be forwarded to the manager of the PTK.

A prerequisite for issuing a Safety Certificate for the current technical system (vessel) prior to the PTK is that DesignA has consulted with the Military Safety Inspectorate. In addition, the vessel prior to use must have an approved seaworthiness inspection certificate from MFI (Marinens Fartygsinspektion – Navy Vessel Inspection). The inspection of seaworthiness is not a requirement to issue a Safety Certificate. MFI may request to see the Safety Certificate during the inspection for seaworthiness.

#### *System Safety Announcement*

---

In those instances where DesignA has been assigned to produce a SS for a specific technical system, but the technical system does not describe the specified risk requirements, a report is submitted in the form of a safety announcement.

#### 5.31.3 Input Data

---

Input to the activity SS is made up of:

- a SCA 5.27
- a SAR 5.21 with test data and analysis reports
- DesignA's inspection reports
- FRACAS 5.28 when applicable.

### 5.31.4 Output Data

---

Output data from the SS activity is made up of the document SS. Sometimes the SS may have certain limitations and, for example, cover only ammunition, specified testing of a certain technical system or cover the activities which, wholly or in part, are to take place under the form PTK. The SS is signed by DesignA's appointed Product Manager.

The document serves as the basis for CSSB 5.33. Examples of a SS and a Safety Certificate can be seen in *appendix 1*.

In cases where the technical system does not contain requirements with regard to risk, no SS is issued, but instead a report is submitted in the form of a system safety announcement.

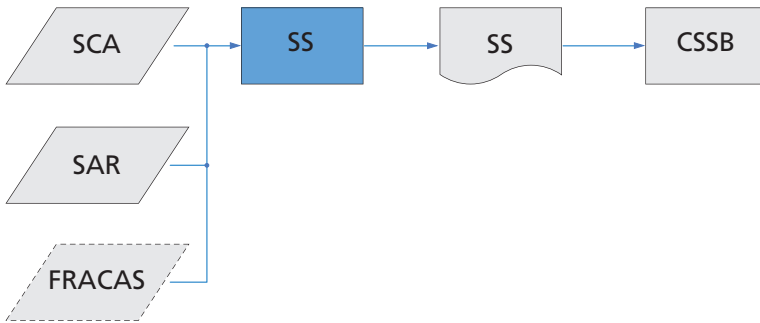


Figure 5:29 Safety Statement (SS)

Examples of SSs and Safety Certificates can be found in *appendix 1* and as files on H SystSäk CDR.

## 5.32 TRAINING SAFETY REGULATIONS (TSR)

### 5.32.1 Purpose

---

Identify and provide the instructions for the safe operation of technical systems. Input data for the activity is made up of the SS 5.31 from DesignA with input from safety regulations (SI 5.25). TSR is a prerequisite for the CSSB 5.33. User manuals and regulations for training are developed through the Production Manager at HKV with help from the Combat School (or equivalent) concerned or on DesignA's order.

### 5.32.2 Activity Description

---

#### *Manuals with Safety and Protective Instructions*

---

Safety and protective instructions must be established and communicated to the user(s) concerned prior to training or handling. Support documentation for the instructions is available in the safety regulations (SI 5.25).

Handling involves everything from production to end use and decommissioning (disposal). This includes the development, storage, transport, handling, use, operation, maintenance and decommissioning. Handling instructions must be continuously developed for the various phases under development all the way to the final regulations, which will form a part of SäKI [41] and other SI.

The individual responsible for the assignment at DesignA will be helpful in developing support documentation for user and safety instructions.

TSR should include provisions for:

- operation and maintenance
- training and other activities within the technical system
- storing and transporting hazardous materials during exercises
- inventory management and transport (for materiel routing, modification, UN missions etc.)
- dealing with accidents and incidents and conducting investigations as a result of an accident/incident.

TSR may be indicated by:

- instructions and pictures that follow the materiel and/or that are distributed to users in connection with initial and recurrent training
- materiel descriptions and instruction manuals which provide a complete description of the materiel – these are allocated to units and schools
- a repair manual
- an instruction film
- regulations for storage and transportation of hazardous materials during exercises.

Such instructions, which are essential for safety, will be incorporated into SäkI [41]. This publication is reprinted every year.

Where necessary, changes/additions are provided. Other publications, such as service branch regulations that apply when in battle, are updated as necessary. However there should, over time, always be a agreement between SäkI [41] and other corresponding Safety instructions.

The handling of the materiel is described by the appropriate regulations, instructions and descriptions. In some instances provisions are made to warn of such errors when being handled, which pose particular risks.

In SäkI [41] provisions for the exercise-related handling of materiel are not included even if they involve measures that are taken from a safety point of view.

The Safety instructions for weapons and ammunition etc. (SäKI [41]), are common to the Armed Forces. They consist of a common part, a part that is intended for managers and executives, and a number of parts for various types of weapons etc. The books contain both mandatory regulations and guidance. The expression SäKI [41] is used as a generic term for the entire series. The provisions in SäKI [41] apply for training during peacetime, during emergency conditions and for training during a war when the training is not preparation for combat.

### *Regulations for Transport and Storage*

---

In combination with a CSSB 5.33 of an item of supply or a system which contains explosives, MSB determines a classification code (ADR [1]) and a storage code (F-code in accordance with IFTEX [19]).

### *Training*

---

The intention is to train the user so that he/she can safely and correctly manage the technical system (follow the published user manuals with safety and protective instructions).

The developing supplier presents a proposal for training. This is demonstrated by safety regulations (SI 5.25) and any training plans.

In connection with field trials, training regulations are worked out, determined and handed over to a service branch centre (or equivalent).

### 5.32.3 Input Data

---

Input data for this activity is made up of SI 5.25.

### 5.32.4 Output Data

---

User manuals and instructions, such as Säkl [41], BVKF [20] and IFTEX [19], make up the main output data. The documentation forms the basis for CSSBs 5.33.

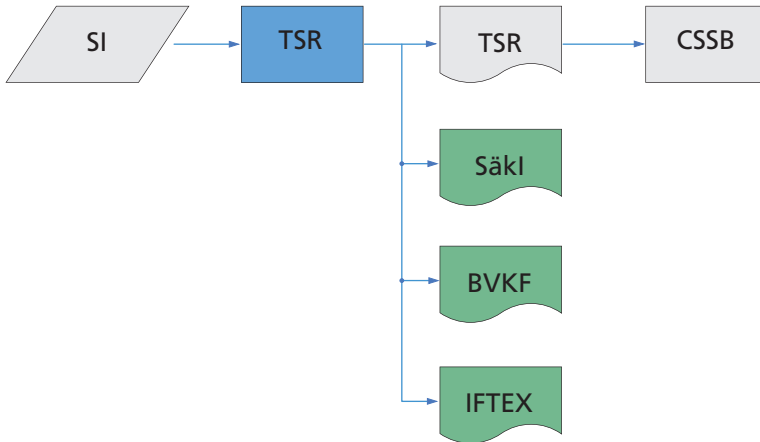


Figure 5:30 Training Safety Regulations (TSR)

## 5.33 CENTRAL SAFETY COMPLIANCE DECISION (CSSB) – S53

### 5.33.1 Purpose

---

The CSSB is the Armed Forces' decision that the technical system is safe to use from a system safety point of view. The CSSB means that the technical system, from a system safety point of view, is ready for a BOA in respect of issued instructions and regulations relating to system safety. The BOA is a decision which relates to the suitability of the system from various safety aspects. The BOA is regulated outside the area of system safety.

The CSSB is valid for a system for a particular version/design. If the version or the design changes, a new CSSB must be taken.

The decision is based on the SS 5.31 from DesignA and that user handbooks and training safety regulations (TSR 5.32) have been developed.

### 5.33.2 Activity Description

---

The Armed Forces verifies that the required system safety activity for the technical system has been implemented.

The CSSB is based on the following steps being taken:

- Verification that the system safety requirements that have been established for the system have been met.
- DesignA's SS for the system has been received for the requested parts.
- Instructions for handling, safety and maintenance have been decided and distributed.
- Regulations for reporting accidents and incidents have been decided and distributed.
- The workgroup for system safety has been formed and details regarding this have been decided.

The production of the technical system is usually a complicated process which takes a long time. The process often includes several successive field trials before series-produced units can be obtained. Prior to each field trial (series of tests) on specific “trial editions” (pilot units) of the system, a decision (CSSB) is taken regarding use. However, it is sufficient that the documentation in the example above is limited to the activity and the conditions under which the systems in each individual case are intended to be used.

### 5.33.3 Input Data

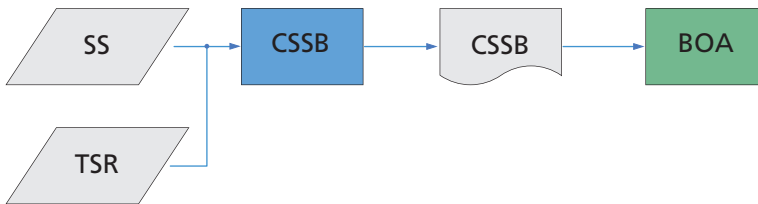
---

Input data to this activity is the SS 5.31 and SI in accordance with (TSR 5.32).

### 5.33.4 Output Data

---

The CSSB examples can be found in *appendix 1*. The approval forms the basis for the BOA.



*Figure 5:31 Central Safety Compliance Decision (CSSB)*

Examples of CSSBs are available in *appendix 1* and as a file on H SystSäkE CDR.



## **5.34 RISK ASSESSMENT PRIOR TO DISPOSAL OF SYSTEM (RADS)**

### **5.34.1 Purpose**

---

To implement the risk analysis that takes place before disposal, the support documentation produced during the technical system's development, during the ordinary safety work, must be updated. Parts of RADS operations should be carried out during regular analysis activities during the development of the system when accident risks, health and environment-related risks are identified. These risks may also be relevant to decommissioning (disposal), this is why decommissioning must always be treated as part of the service life of the technical system and must be taken into account during development and production. Good configuration management throughout the entire technical life of the system is necessary so that all changes, with possibly new risks, can be identified during the decommissioning phase. The Armed Forces is responsible for the activity.

### **5.34.2 Activity Description**

---

#### *Supporting Documentation*

---

Risk analysis prior to decommissioning should always be carried out for a technical system.

The documentation from the analysis must, in a systematic way, describe the materials, substances or components that form part of the system and can be assumed to be hazardous to people or the external environment. In addition, one or more possible ways to dispose of/destroy the technical system should be described. Every possible disposal method must be analysed/investigated with regard to safety.

For the technical system/the product – the following items are reported:

- possible destruction/disposal methods
- the risks associated with the disposal/decommissioning process.

For each potential hazard/hazardous substance the following are reported:

- health hazards
- environmental hazards.

These characteristics must be weighed against the prescribed limits or other approved requirements.

The possibility of reusing materials or substances should be reported with a proposal as to how they can be used again. For substances which, as a result of their characteristics, cannot be reused, recycled, have energy extracted or destroyed, it is important to specify how these can be taken care of (in terms of terminal storage).

Risks due to stored energy, for example in the form of pressurized vessels, tension springs, reactive substances and energy in electrical components, should be reported. Safe methods to eliminate these risks during dismantling or destruction should be specified.

### Analyses and Activities

For systems developed in accordance with *H SystSäkE* methodology, disposal analyses are presented in accordance with RADS. For simpler systems, normal analysis operations (PHA 5.13, SHA 5.16, SSHA 5.15, O&SHA 5.17, HHA 5.18, EHA 5.19 and FHA 5.20) may also deal with the disposal, so no separate RADS is required.

For the disposal of older systems, developed without the support of system safety activities and where support documentation is missing or incomplete, analyses must always be carried out in accordance with RADS where appropriate.

Material/substance identification:

- list all components in the technical system
- list all materials, including surface treatments, for each component
- compare substances with the Chemicals Inspectorate's PRIO-guide [27].

Analysis of disposal/destruction methods:

- describe the disposal process
- describe each step of the process
- state any restrictions/warnings for the various steps in the process
- analyse the risks in each step, for example in accordance with the UK Ordnance Board P115 [7]
- adjust the process in order to minimize any risks
- demonstrate that the process can be carried out as described
- document the final process with its analysis results.

The UK Ordnance Board P115 [7] indicates that each step should be analysed in terms of risk of accident, health and environmental impact.

### *Configuration Control*

---

The person responsible for system documentation following delivery from the supplier, usually the person responsible for materiel systems at DesignA, will also be responsible for updating the changes to the configuration in order to perform a final risk analysis prior to final disposal. Mandatory requirements of great importance for the safe disposal of the technical system should be documented in the reporting system. This should be linked to a F designation (M number).

### *Sale*

---

If residual products or systems are to be sold in connection with disposal, special inspections are required.

If scrap is produced, a certificate must be presented which states that the scrap is free from remains of explosive materials and that it does not contain flammable materials or gases. This requirement applies to all military scrap delivered to the Armed Forces or DesignA, whether it has contained explosives or not. Scrap is also declared in respect of any environmentally hazardous substances (hazardous waste) that may be included in the scrap.

For completely or partly usable systems, any defects or hazards/hazardous conditions must be documented in writing and this documentation must accompany the item which is for sale. In some cases the dangerous or prohibited substance/part must be removed before sale.

The Armed Forces' detailed rules for the sale and other disposal, together with rules for management, planning and implementation of such measures, are described in H Förnavv [22].

#### 5.34.3 Input Data

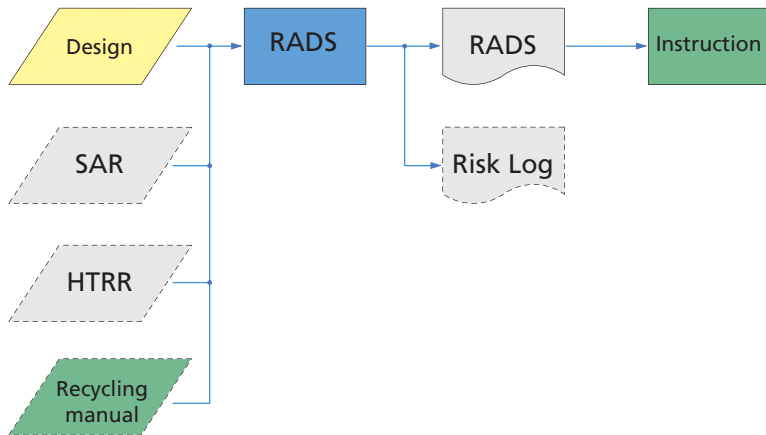
---

Input data for this activity forms a design description and, if possible, even SAR 5.21 and a Risk Log in accordance with HTRR 5.9. For environmentally related activities, there may be a Recycling manual [15], this may form support documentation for RADS.

#### 5.34.4 Output Data

---

Disposal instruction and a risk analysis report prior to disposal. Identified risks can be documented in the Risk Log in accordance with HTRR 5.9.



*Figure 5:32 Risk Assessment at the Disposal of System (RADS)*



# 6 SOFTWARE SAFETY

## 6.1 GENERAL

Program Software Safety applies the principles and activities, as defined for system safety work, on the technical system's software elements. Various procedures, activities and methods are used to incorporate system safety properties in the general system architecture and further down into the software architecture and implementation. How this occurs will be described in the System Safety Program Plan (SSPP 5.5). These processes are dependent on the characteristics which a realization in software entails, which is not only confined to the software as a product, but also the parts involved in its development, operation and maintenance and the processes they make use of. The grounds for the development of software are described in H ProgSäkE [18].

## 6.2 SOFTWARE FEATURES

A software product is represented by its overall documentation with regard to the requirements, architecture/design, interfaces, implementation, analysis results, change descriptions or fault databases.

A realization in the software may display design features not found for components realized using other techniques, such as:

- An abstract, conceptual description of complex relationships without physical limitations.
- Discontinuous behaviour: a small change in one of the conditions for which the component is designed, could lead the execution into other branches of the execution tree with radically different behaviour as a result.
- The properties displayed are controlled by the context in which the software is adapted to and used with (the system, environment, user profile).
- Systematic faults (logical mistakes) dominate over random faults.

- Relevant estimation of failure rates is not possible before the deployment of the software with very low fault probabilities (high Safety Integrity Levels).
- Safety threats directly initiated by the software can originate from the software product (faults with the specifications/design or its implementation), its production processes, production tool or a member of staff's actions. For example, a supplier can be re-used a code under changed conditions or an end user may operate outside of the intended area of use, or the system may have been used in violation of the specifications and instructions.
- Hidden security threats in the technical system's interface can accidentally be activated when the software interacts with other components (software, hardware, operators), even if each individual component has demonstrated safe behaviour.

These peculiarities affect the ways that software safety can be satisfied in that:

- A realization where parts of a higher criticality cannot be isolated from those of lower or no criticality as a whole are critical to its highest degree.
- The software design must be based on a safety philosophy for the entire technical system as it is intended to be used.
- Software that is considered to be safe in a particular context may not be safe in another.
- Reuse of software, which was not designed for reuse, is precarious and requires special safety checks and measures. This also applies to the reuse of very closely related systems or in an unchanged system with different operating conditions.
- A definitive assessment of the software features must be based on the software as an integral part of the technical system in the environment and the use it is intended for.
- Risk reduction for software focuses primarily on redesign (rather than the addition of protective features).



- Risk reduction in the form of redundancy can only be based on diversity, non-identical copies.
- Software parts for which requirements are made in order to obtain a very low failure rate (high Safety Integrity Levels) usually require a redesign so that the higher failure rate may be permitted for the software component with the possibility that, prior to operational use, requirements can be verified by using statistically reliable estimates.

A conscious, safety-oriented system design based on general design principles is necessary to overcome these peculiarities.

Among the more significant include:

- **Simplicity, determinism and verifiability** are prioritized in the design of the top system level and down to the software level. These features are necessary in order to conduct different risk assessments: simplicity, in order to carry out an assessment in a practical manner, determinism, in order to assess the technical system's behaviour based on the given conditions, and verifiability, in order to determine that the specific system characteristics have been realized.
- **Security-oriented architectures** are defined with strategies as to how system security must be maintained. For system of systems, a hierarchy of architectures is required, which cooperate in order to satisfy the system security as seen from the top level. For identified system security threats it is determined at what levels and which (sub)systems these should be received with. For remaining safety threats, which could not be eliminated or reduced in accordance with the requirements through redesign, the design is supplemented with special safety mechanisms.
- **Criticality partitioned software** is created to ensure that critical software components can be affected directly or indirectly by a component with lower or no criticality.
- **Diversity** is considered as the first alternative for risk reduction, particularly for the software, where requirements regarding low-frequency fault probabilities are made.

- **Unnecessary and redundant functionality** is eliminated or deactivated in the safety critical code in order to prevent unintentional execution. This means that dead code is cleaned out, that functionality intended for a certain system mode or a certain system configuration is prevented from being executed in another mode/configuration and that functionality that has not been demanded is screened (relevant for example for reusable software).

Early efforts, which aim to incorporate these features in the technical system at the highest level and the lower parts of the realization units, are required for the best effect in terms of the invested security work. Monitoring how these properties are later detailed and realized is to be carried out at supplier audits as well as at the System Safety Working Group (SSWG 5.8) follow-ups, see *section 6.4*.

### 6.3 SAFETY REQUIREMENTS FOR SOFTWARE

Software, which can produce a hazardous event occurring, or whose function is to prevent this, is safety critical, see Safety Critical Functions (SCF 5.11). Typical examples would be software for controlling, monitoring, protection and communications relating to a safety critical activity, equipment or information.

The general requirements, which may be made for this type of software, not only refer to software products in its various stages, but also personal qualifications and the processes that are applied to a software system during its lifetime. These requirements relate to both the Armed Forces as clients and end users as well as the ordering party, DesignA and the supplier. A summary of the requirements, which may be relevant for newly developed and reused software in safety-critical systems, can be found in H ProgSäkE [18]. These are graded based on the software's criticality and there are often several varieties provided. A selection of the requirements, which apply to the safety-critical software elements in the current system, are therefore necessary. This is governed by the criticality of the individual parts and the relevance of the requirement.

An excluded requirement requires justifications, which are subject to review if conditions change. Only where independence can be shown between the separate parts is it possible that requirements for different criticality can apply in the same system. The selection of requirements will therefore distinguish between criticality-separated parts. Support for documentation of the selected requirements and the monitoring of the degree to which these requirements are met can take the form of a number of cross-reference lists.

The requirements of H ProgSäkE [18] are divided into two categories: basic requirements and general safety requirements. Software safety requirements relating to a particular component, function or (sub)system are not included, but instructions on how these can be derived are included. These specific requirements are therefore additional to the requirements listed in the H ProgSäkE [18]. The resulting amount of requirements will determine subsequent activities in Safety Verification (SV 5.24) and the Safety Compliance Assessment (SCA 5.27), see *section 6.4*.

The process of developing a more complete set of software safety is repetitive and takes place at the same time as the traditional breakdown of requirements and specification of the technical system in the underlying software components. This requirement specification, a sub-activity under the Safety Requirements/Criteria Analysis (SRCA 5.14), is based on analyses conducted under the Preliminary Hazard List (PHL 5.12), Preliminary Hazard Analysis (PHA 5.13), System Hazard Analysis (SHA 5.16), Subsystem Hazard Analysis (SSHA 5.15), Functional Hazard Assessment (FHA 5.20) and Operating and Support Hazard Analysis (O&SHA 5.17). Hazardous events with their causes, which are identified in these analyses, are reformulated to system specific safety requirements and safety-oriented restrictions of the software architecture.

Reuse of the technical system's safety-critical software elements can be facilitated by a step-by-step derivation of the system-specific safety requirements. The analyses focus on first identifying the safety requirements common to the domain, in order to subsequently add the domain-specific safety requirements, and finish with those that are system specific.

Domain common safety requirements consist of requirements which relate to an individual software function/component/system without regard to its context (for example a weapons systems for aviation, the navy, the army), while domain-specific requirements relate to a particular application domain (such as a weapons system for the navy).

### 6.4 VERIFICATION OF SOFTWARE

The purpose of the SV (5.24) is to ensure that the technical system's safety requirements are met. These represent a subset of other requirements. SV (5.24), with respect to software, is therefore integrated with the verification process. This is required for all types of software and is continuously performed during the construction and integration with other system components. For safety-critical software verification it means that both basic requirements and system safety requirements must be verified, see *section 2.1*.

Verification may consist of review/monitoring and various analyses (static/dynamic/system safety oriented). Procedures and tools that support this activity are part of the traditional software development environment. Support during the review of constituent products and activities of the safety-critical software can be done with the help of checklists which focus on software safety. When monitoring safety requirements compliance, cross-reference lists have been developed, linking requirements with the current status of the verification mode and evidence of completed verifications. This specification provides a good picture of the software's safety operations and safety situation, which makes it useful as a basis for the supplier's System Safety Progress Summary (SSP 5.10) report.

For verification of software developed in accordance with any other safety-oriented handbook or standard, a representation is first carried out of its demands for a more comprehensive number of requirements in H ProgSäkE [18] before an evaluation can be carried out as to whether the software fulfils its requirements.

# 7

## CHECKLIST FOR MATERIEL REQUIREMENTS AND ACTIVITIES

The following checklist is used for the development of the requirements for Request for Proposal (RFP), the implementation of project follow-ups and the reports of the audit groups (SSPR 5.7); the checklist is also used by the advisory groups and the System Safety Working Group (SSWG 5.8). A complete description of requirements can be found in *chapter 2* and *section 3.1*.

Requirement no	Designation	Applicability			Comments
		Yes	No	N/A <sup>a</sup>	
<b>Materiel requirements</b>					
0.21.001	Minimum safety instructions				
0.21.002	Single fault				
0.21.003	Common causes				
0.21.004	Resistance to abnormal environments				
0.21.005	Properties which can lead to critical errors are defined in the product documentation				
0.21.006	Properties which can lead to major faults are defined in the product documentation				
0.21.007	The programme's basic quality standards/requirements				
0.21.008	A selection of general software safety requirements				
0.21.009	Avoid using exemptions				
0.21.010	Joining methods				
0.21.011	Identification of plastic materials				
0.22.001	General inspection of properties that can lead to a critical error				

## 7 Checklist for Materiel Requirements and Activities

Requirement no	Designation	Applicability			Comments
		Yes	No	N/A <sup>a</sup>	
0.22.002	General inspection of properties that can lead to a major fault				
0.22.003	General inspection of properties that can lead to a critical error				
0.22.004	General inspection of properties that can lead to a major fault				
0.22.005	The calibration of control equipment				
0.22.006	The segregation of defective units				
0.23.001	Maintenance for safety enforcement				
0.23.002	Safety following maintenance				
0.24.001	Reuse and recycling rate				
<b>Activities</b>					
0.31.001	System Safety Program (SSP)				
0.31.002	System Safety Evaluation (SSE)				
0.31.003	Safety Requirements in TTEM				
0.31.004	Request for Proposal (RFP)				
0.31.005	System Safety Program Plan (SSPP)				
0.31.006	Integration/Management of Associate Contractors, Subcontractors and Architect and Engineering Firms (IMSC)				
0.31.007	System Safety Program Reviews (SSPR)				
0.31.008	System Safety Working Group (SSWG)				
0.31.009	Hazard Tracking and Risk Resolution (HTRR)				
0.31.010	System Safety Progress Summary (SSPS)				

Requirement no	Designation	Applicability			Comments
		Yes	No	N/A <sup>a</sup>	
<b>0.31.011</b>	<b>Safety Critical Functions (SCF)</b>				
0.31.012	Preliminary Hazard List (PHL)				
0.31.013	Preliminary Hazard Analysis (PHA)				
0.31.014	Safety Requirements/Criteria Analysis (SRCA)				
0.31.015	Subsystem Hazard Analysis (SSHA)				
0.31.016	System Hazard Analysis (SHA)				
0.31.017	Operating and Support Hazard Analysis (O&SHA)				
0.31.018	Health Hazard Assessment (HHA)				
0.31.019	Environmental Hazard (EHA)				
0.31.020	Functional Hazard Assessment (FHA)				
0.31.021	Safety Assessment Report (SAR)				
0.31.022	Safety Review (SR)				
0.31.023	Safety Verification (SV)				
0.31.024	Safety Instructions (SI)				
<b>0.31.025</b>	<b>Safety Compliance Assessment (SCA)</b>				
0.31.026	Failure Reporting, Analysis and Corrective Action – (FRA-CAS)				
<b>0.31.027</b>	<b>Safety Statement (SS)</b>				
0.31.028	Test and Safety Regulations (TSR)				
<b>0.31.029</b>	<b>Central Safety Compliance Decision (CSSB)</b>				
<b>0.31.030</b>	<b>Risk Assessment at the Disposal of Systems (RADS)</b>				

a. N/A = Not applicable





# 8

## SYSTEM SAFETY ANALYSIS

### 8.1 PRINCIPLES FOR SYSTEM SAFETY ANALYSES

A safety analysis (also known as hazard analysis) is a systematic procedure, which analytically examines how and to what degree for example, an integration error, component failure or improper handling can produce to in terms of hazardous events in a system.

There are a large number of analytical techniques aimed at different applications such as design solutions, operational management and production processes. Each method has limitations which means that in many cases, it is appropriate to combine several methods to obtain a good result.

The picture below shows what a complete safety analysis covers (shown in yellow in the picture), and how these activities interact.

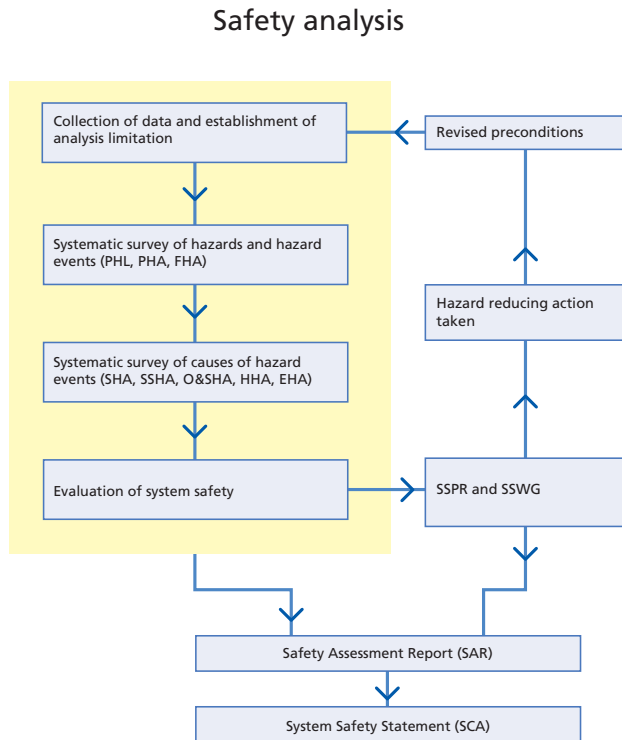


Figure 8:1 Safety Analysis

Within this general model, safety analyses can look quite different depending on:

- Choice of analytical method, the choice is mainly determined by the system's design and function, and the purpose of the analysis. Whether the evaluation is qualitative or quantitative.
- How detailed the technical documentation is at the time of the analysis.
- What level in the system (sub-assemblies, components, software blocks, etc.) the analysis covers.
- Which phase, design or manufacture, the analysis covers.
- What the formal part of the analysis (symbols and forms) looks like.

Four commonly used methods of analysis are described clearly below. For more detailed descriptions, refer to the literature within the area.

Accident risks/hazardous events identified during for example PHL, PHA and FHA are analysed to ascertain the root causes that may contribute to them arising. The activities SHA, SSHA, O&SHA, HHA and EHA often use one or some of the following methods of analysis FMECA, FTA, ETA and HAZOP.

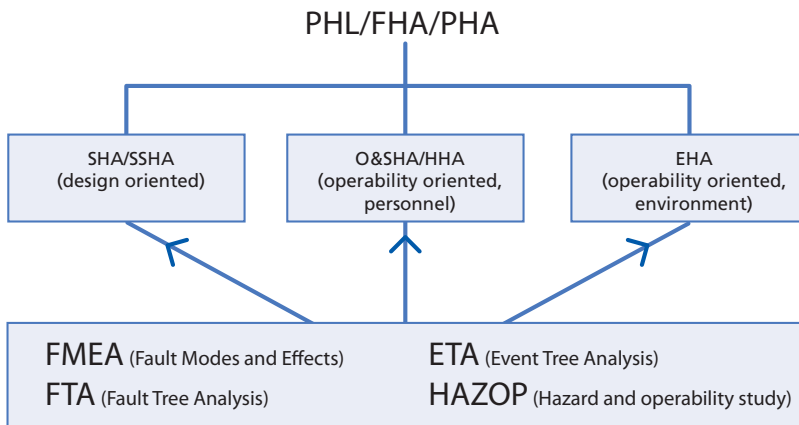


Figure 8:2 Linking of Activity to the Method

## 8.2 FAULT TREE ANALYSIS (FTA)

The Fault Tree Analysis, FTA, is a method of analysis in which a potential hazardous event is examined in stages in order to determine which subordinate events, or combinations thereof, can cause a hazardous event. This is deductive (top down).

FTA takes a look at one hazardous event at a time and demonstrates first of all what the immediate underlying events, or combinations thereof, that lead to the hazardous event. These events may include malfunctioning components, improper handling or specific environmental conditions. The underlying events and their causes are broken down further in the same way and the analysis continues down to a level of detail that is suitable for risk mitigation. The lowest level of the analysis consists of basic faults in simple components or similar.

A fault tree therefore describes how faults in various parts of the system can interact and lead to a hazardous event. To make the method systematic and graphic, a logical schematic is used with standardised symbols.

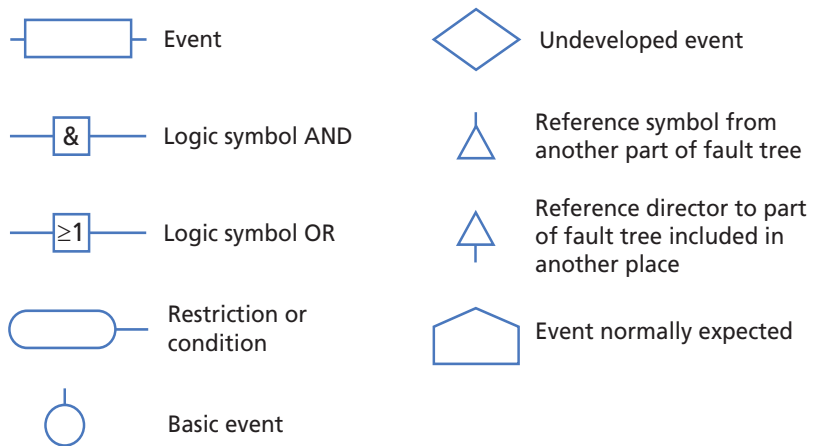


Figure 8:3 Fault Tree Symbols

- Suitability:** FTA is an excellent tool and becomes easily understandable when a hazardous event requires two or more faults/events (independent of each other) to occur. It can therefore manage situations with redundancies.
- Disadvantages:** The breakdown of the subordinate events makes great demands on accuracy and knowledge of the system for the person conducting the analysis. It is easy to overlook one-time events and incorrect procedures that can cause or contribute to hazardous events. The fault tree analysis is a static approach. For this reason, FTA cannot be used uncritically in operationally “dynamic” systems with for example, changing operating modes, stand-by situations (such as passive redundancies) or deterministic elements (such as periodic maintenance). Some tricks have to be resorted to in order for the calculations to be accurate.

### 8.2.1 Qualitative Fault Tree Analyses

---

The fault tree produces basic events which specify the root causes of the identified hazardous event. They are made up of planned events, conditions or basic faults. To eliminate the hazardous event, measures must be taken with the impacting events. The type of measures that must be taken depends on how clearly they influence the hazardous event (depending on the tree structure) and how often they might occur.

Normally such simple faults, which alone could lead to a hazardous event, are not tolerated; i.e. those which can be eliminated through design changes.

In order to minimize manufacturing-related shortcomings, various measures are taken with basic faults. The measures taken depend on how often these faults can be expected to occur and to what degree they contribute to the hazardous event (how many &-conditions that exist between the basic event and the hazardous event, or how many entries there are in &-gates).

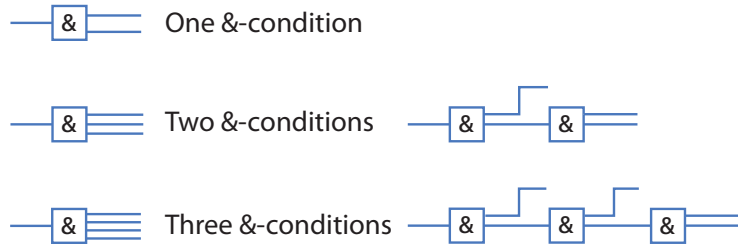


Figure 8:4 The amount of & conditions

Examples of how the number of & conditions are developed is presented in the picture below.

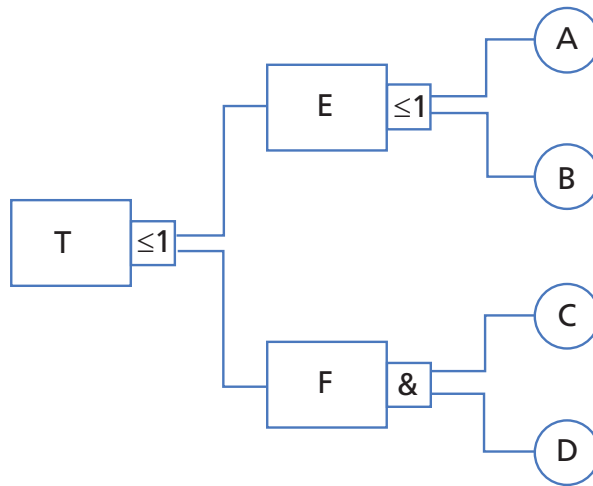


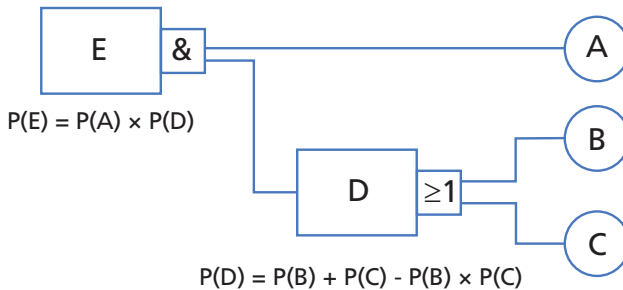
Figure 8:5 Fault Tree with Different Amounts of & Conditions

Basic event A has no & conditions for the hazardous event T while the basic event C has one & condition for a hazardous event T.

### 8.2.2 Qualitative Fault Tree Analyses

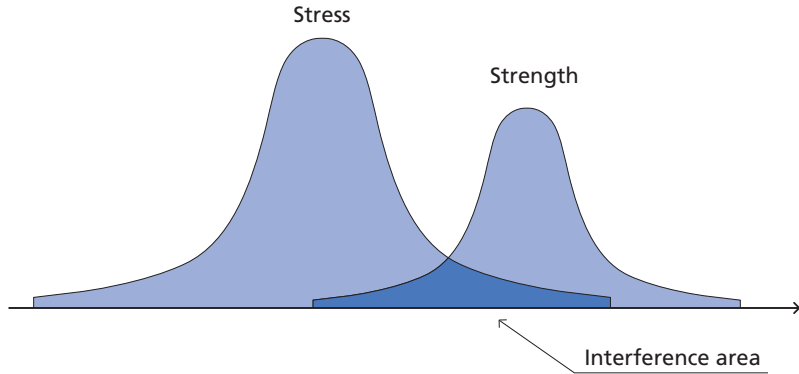
Since the safety requirements are quantitative, verification is carried out by showing that the likelihood of a hazardous event or accident occurring does not exceed the specified requirements. One difficulty may be to obtain relevant input values for the calculations. It is therefore inappropriate to draw too far-reaching conclusions regarding the materiel's safety or to compare different systems, since the conditions for the calculations can be very different.

The calculations can be done in accordance with the following basic examples. Note that this simplified calculation assumes independence between the different basic events.



*Figure 8:6 Calculations of Fault Tree Probabilities*

To obtain the probabilities of each basic event, normally experience values (database) are used or for materials-related design flaws, the STRESS-STRAIN method may be used. This method means that you must calculate the probability that the strength of the design exceeds the stress produced by environmental factors. The picture below illustrates how the probability, which corresponds to the interference surface, is dependent on the distribution of stress-strength.

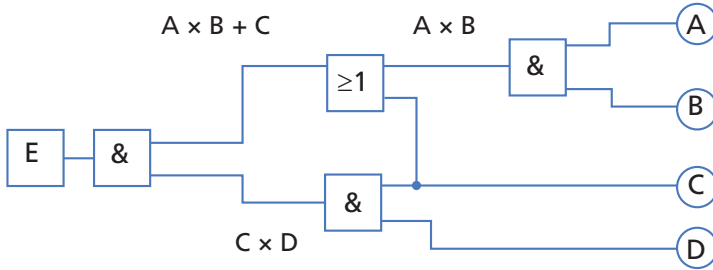


*Figure 8:7 The Stress-Strain Interference Surface*

As the probabilities cannot be calculated for the basic events, a so-called sensitivity analysis may be performed. Equal probability is applied for the different basic events and the likelihood of a hazardous event can be calculated. The probabilities are then changed for each of the different basic events and the hazardous event probability is recalculated. In this way, the basic events that provide the greatest contribution to the hazardous event can be distinguished. The method is most suitable for large fault trees, where transparency is low.

Another method is to use Boolean algebra, where each basic event is given a specific designation, such as a letter of the alphabet. After reduction of the expression for the hazardous event, you can identify which basic events that mostly affect the probability of a hazardous event.

Calculations with numerical values should not occur until reduction of the final expression has occurred. Such reductions are virtually impossible to do by hand for large fault trees.



$E = (A \times B + C) \times (C \times D)$  which is reduced to  $E = C \times D$

Figure 8:8 Example of Solution with Boolean Algebra

In this example, the standard IEC symbols have been used. Different solutions on a fault tree structure can arise naturally.

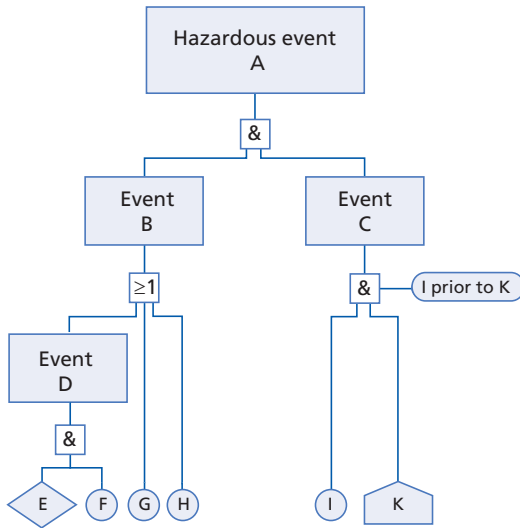


Figure 8:9 Example of Fault Tree Analysis

The fault tree expresses the causal link: A occurs if both B and C occurs. B occurs if at least one of the events D, G or H occur. D occurs if both E and F occur. C occurs if both I and K occur where I must occur before K. The event E can be further subdivided. The event K is always expected to occur.



### 8.3 FAULT MODES AND EFFECTS ANALYSIS (FMEA)

With FMEA the analysis work is carried out inductively (from the bottom upwards), in principle, in the reverse order of a fault tree analysis. It is based on components or subsystems for which every failure mode is analysed in terms of the impact it would have on the system.

Depending on how far the detailed design of the analysed system has come, the failure modes of functions or components can be taken into consideration. For each failure mode, the cause and the effect is specified. From all possible fault effects, any hazardous events may then be identified and measures taken to reduce the risk.

The fault effects analysis may well be carried out in preliminary form and at an appropriate level of detail in the early stages of the design work so that risk-reducing measures can quickly be taken.

The analysis is carried out with the help of a form where different columns specify the current component and/or function, including possible failure modes, the probable cause of failure, the fault's effect both at a detailed level and for the entire system, and also the probability that the fault will occur.

**Advantages:** The fault modes and effect analysis is particularly appropriate for the study of the potential failure modes, each of which can cause a hazardous event. The method is systematic and comprehensive and the results are clear and easy to understand.

**Disadvantages:** The method requires the review of a large number of components and failure modes, which are not directly related to safety. The analysis will therefore be extensive and time consuming for complex systems. Furthermore, it is difficult to detect with the method the effects of a combination of multiple simultaneous faults.

### 8.3.1 Qualitative Fault Modes and Effects Analyses

---

Analogous to qualitative fault trees, a risk matrix can be used to evaluate different failure modes. In the fault modes and effects analysis, a column for severity is introduced, also referred to as criticality. The analytical method is described as FMECA (Fault Modes, Effects and Criticality Analysis).

### 8.3.2 Qualitative Fault Modes and Effects Analyses

---

In order to more easily examine the results of an FMEA it may be of value to carry out the following: an assessment or estimation of the occurrence of a failure mode, and a gradation of the impact of the failure mode on the system. This provides greater opportunities to compare different design solutions from a safety standpoint.

The FMECA form can therefore be extended with three columns. One column where the fault frequency is specified on a scale from A to E, for example where A corresponds to the highest fault frequency. A second column specifying the failure mode's effect on a scale from I to IV, where I is equal to the highest severity (injury class). The third column calculates the fault mode's Risk Priority Number (RPN).

There are several different methods to calculate the RPN. Within one and the same area of operation, it is appropriate that the same method is used. The most common method is multiplication. Calculation of the RPN is carried out by multiplying the scale values for the failure rate (A=1, B=2, and so on) and the severity (I=1, II=2 and so on) with each other. The RPN will produce a relative, numerical value as to how critical a certain failure mode is compared to other failure modes. In this way, different failure modes are ranked and actions can be prioritized.

The fault modes and effects analysis is carried out using the form with columns, where the conditions and the results are entered. The form may vary depending on the purpose of the analysis and the degree of detail, an example is given below.

Item no/ Denomination	Fault mode	Cause	Phase	Fault effect Locally	Fault effect Sub-system	Fault effect System	Fault detection	Cons.	Freq.	RPN	Comments
1. Mounting body	Play between mounting body and breech casing	Carrier not tightened. To much play	4	Negligible move- ment between mounting body and breech casing	Increased wear of joint	Reduced availability	Gun crew during service	IV	C	12	Maintenance interval reduced Not safety critical
	Breech casing joint constrict- ed	Carrier has to little play etc.	4	Difficult to elevate	Increased wear of joint	Reduced availability	Gun crew during service	IV	B	8	Maintenance interval reduced Not safety critical
2. Breech casing	Play constricted (see item 1)	Material defect	4	Movement be- tween mounting body and breech casing	Barrel loosens dispersion increases	Breakdown, firing outside in- tended firing area	Gun crew during firing	I	C	3	Calculation of strength properties, safety factors and failure rate
		Trunnion shears due material defect	4	Movement be- tween mounting body and breech casing	Barrel loosens dispersion increases	Breakdown, firing outside in- tended firing area	Gun crew during firing	II	D	8	
	Loosens	Barrel mounting constricted	4	Increases load on breech casing trunnion	Barrel loosens dispersion increases	Breakdown, firing outside in- tended firing area	Gun crew during firing	II	D	8	High kinetic forces
		Material defect, defective recoil buffer (see also item 5 Recoil buffer)	4	Increases load on recoil buffer trunnion	Barrel loosens dispersion increases	Breakdown, firing outside in- tended firing area	Gun crew during firing	II	E	10	
	Recuperator detaches	Material defect, defective recoil buffer (see also item 5 Recoil buffer)	4	No recuperation function	Barrel does not return to recuperated position	Firing stoppage	Gun crew during firing	IV	D	16	Not safety critical

Figure 8:10 Example of Fault Modes and Effects Analysis

Below is an example of the input data needed to create an FMECA. The product/system structure defines the parts and components the system consists of. Component data defines the type of component and its features. Furthermore, a component specification is used in order to identify the component's failure modes (and failure mode distribution) and a prediction of the probability of the failure mode occurring for the specified use in accordance with the system's operational profile.

The product structure (system description) constitutes the basis for the implementation of risk identification (PHL, PHA, FHA) in order to identify hazardous events at system level. These hazardous events are associated with the identified effects of the components' failure modes. Furthermore the consequences for the system effects (hazardous event) are specified, for example as an injury class..

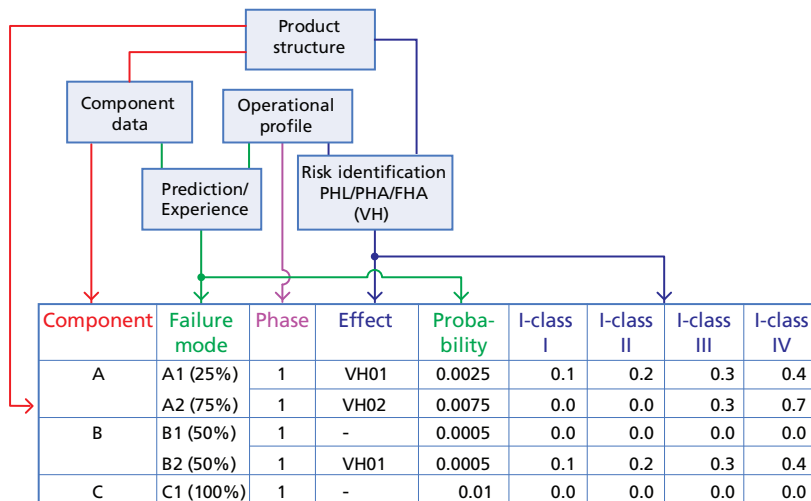


Figure 8:11 Examples of Basis for Fault Modes and Effects Analysis

### 8.4 EVENT TREE ANALYSIS (ETA)

This method, which may be qualitative or quantitative, is used to identify the effects of a given event. This method is often used to analyse systems that have protective and safety devices. Each event is assumed to result either in success or failure. Note that the probabilities in the tree are conditional probabilities, since a previous event must have occurred. In the same way as for ordinary fault trees, it poses the question, what happens if a sub-event occurs or does not. For a comprehensive analysis, all start events must be identified.

It facilitates the construction of an event tree if there is access to a functional description in the form of a block structure, a so-called functional safety schedule (Reliability Block Diagram).

The following examples show how the event tree technique can be applied to demonstrate what a grounding can produce in terms of end events. All sub-events operate in series, so a subsequent event is conditioned by the previous one having occurred. The occurrence probabilities have been noted with a yes/no answer.

It should be observed that all events are not described in the example, for instance, false alarms are not dealt with.

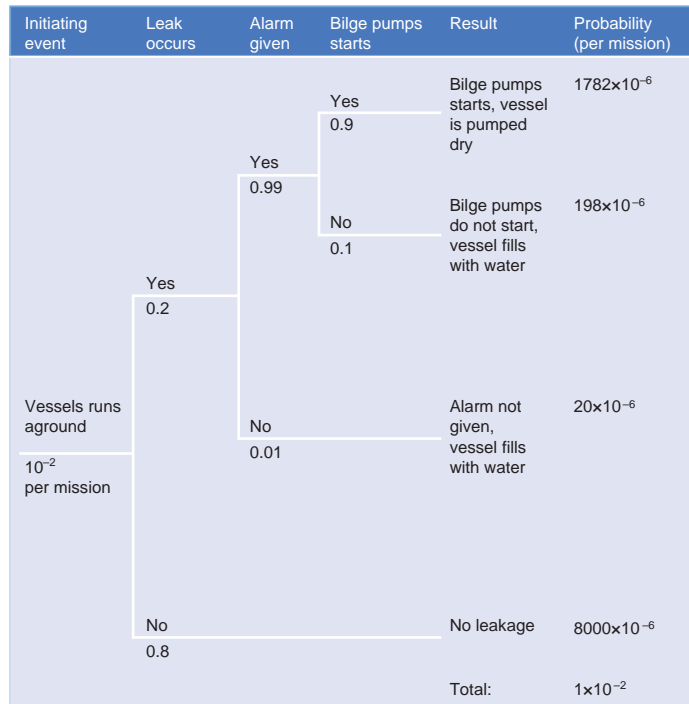


Figure 8:12 Example of Event Tree Analysis

## 8.5 HAZARD AND OPERABILITY (HAZOP) STUDY

This method is best suited for processes and operational processes. The method is closely related to FMEA, but the failure modes have been defined and made uniform from the beginning. The following fundamental steps are applied:

- Describe the process or the operational process, including the human involvement, as well as the intended function.
- Review every part of the process or the operational process systematically to determine how a deviation from the intended function can arise.
- Decide whether these variances could lead to accidents or incidents.

HAZOP is best done several times during the development phase so that the information can be fed back to the design manager responsible in stages, this is to achieve a more reliable (safer) system. Since HAZOP is a relatively simple analysis it can be performed early on in the design process.

The analysis includes the following steps:

1. Define the scope of the analysis, which sub processes or operational processes are to be included.
2. Gather a group of persons who can carry out the analysis together. Preferably the group should consist of both designers and users/operators who can assess the impact of a deviation from the intended function.
3. Gather all relevant documentation describing the process or the operational sequence (flow charts, drawings, user manuals, maintenance manuals and safety instructions).
4. Analyse each sub-process or operational process by applying the predefined guide words that lead to process-specific abnormalities (deviations), indicate possible cause, the consequence of the deviation, and the requisite action. The following provides a summary of the work process:
  - 4.1. Select a sub-process or operational process.
  - 4.2. Specify the intended function of the process.
  - 4.3. Apply the first guide word.

- 4.4. Determine which deviation that occurs.
- 4.5. Specify the possible cause.
- 4.6. Specify the consequence.
- 4.7. Specify the required action.
- 4.8. Repeat steps 4.3–4.7 until no new deviations can be determined.
- 4.9. Apply the next guide word.
- 4.10. Repeat steps 4.3–4.7 until no new deviations can be determined.
- 4.11. Repeat 4.9–4.10 until all the guide words have been exhausted.

The guide words must be determined for each process or operational process. The picture below shows some pre-defined guide words with their definitions.

Table 8:1 Guide Words Table

Guide word	Definition
None	no operation can be achieved
More	a quantitative increase in the output result
Less	a quantitative decrease in the output result
As well as	a qualitative increase
Part of	a qualitative decrease
Reverse	opposite effect
Other	something other than the intended function

The following is an example of a part of a HAZOP in which only the first guide word “none” has been applied.

Table 8:2 Example of HAZOP

Guide word:	Deviation	Possible cause	Consequence	Action
None	No assurance	1. Improper use	Risk of unintentional discharge	a) Prior to instruction in the manual b) Prior to a section of the training plan
		2. The block is missing	As 1	a) Change the design



## Appendix 1 Examples of Decision Documents

### Purpose

---

This appendix provides simple examples of the design of the Safety Compliance Assessment (SCA), 5.27, the system safety approval, 5.31, safety certificates, 5.31, and the central safety compliance decision (CSSB), 5.33. In the text below they are referred to collectively as “Decision Documents”.

The scope of a certain decision document, over and above what is reported in these examples, is required by the clients (The Armed Forces via a Customer Order (KB), DesignA via a Request for Proposal (RFP)).

Certain basic principles, as stipulated below, determine the formulation of a decision document – see the examples in the sections on *System compliance assessment – Safety certificate*.

The designation of a decision document is always “pure”, i.e. it is without epithet in the form of “temporary”, “preliminary”, “final”, “time limited” or suchlike. Instead, the heading of the decision document specifies the technical systems to which it relates. For example, “Safety Compliance Assessment (SCA) for Flamethrower 01, experimental design type E”.

Time limits are used only in exceptional cases where the technical system is considered to be a perishable good. The other limitations which each decision document must contain, with reference to the extent of the technical system and its utilization, are described in detail in the decision document itself.

The technical system in question is defined with regard to its scope and constituent parts/subsystems/any accessories (major/safety related) in order to clearly account for what has been included in system safety activities and in the decision document.

The technical system is identified by stating the name, designation, type number, marking, reference to technical documentation in which the technical system is described in detail, and likewise for incorporated subsystems and any safety-related accessories.

For utilization, the operational phases, methods of use and external conditions for which the technical system is intended are identified and, whenever applicable, the propellant, ammunition types etc., that are qualified to be used together with the technical system.

In the decision document, any interoperability is specified with other technical systems that have been qualified (for example, that a certain flamethrower is also permitted for use from a certain vehicle).

In those instances where DesignA has, for example, been assigned to a specific technical system to develop a Safety Statement (SS), but the technical system's accident risk does not meet the requirements, a report is submitted in the form of a **safety message** with (a) proposal(s) to the Armed Forces with regard to appropriate action to take.


The Sea Trials Command (PTK) under SS, 5.31, contains a decision document which is called a **safety certificate**. The certificate is issued by DesignA and it means that DesignA, after taking into consideration all the relevant circumstances, has found that the vessel that the PTK is to test has an acceptable level of safety. An example of a safety certificate is provided in the section *Safety Certificate*.

The distribution list for decision documents should generally include all the authorities affected by the decision. Among other things, the client that has ordered the assignment concerning the production of the decision document. Units and the System Safety Working Group (SSWG-2), 5.8, receive the system safety documentation as annexes to a Decision Regarding Use (BOA).

All these examples presented here are available as Word files on H SystSäke CDR.

# Safety Compliance Assessment

## An Example of a Supplier's Safety Compliance Assessment

 <p>PETTERSSON SMIDE AB Simpevarp</p>	<p>SAFETY COMPLIANCE ASSESSMENT 15-06-20XX</p>	<p>Ref. 102/-XX</p>
<p><b>Safety compliance assessment for VULKANUS flamethrower mod/01 with model number 700-953 (3 attachments)</b></p>		
<p><b>1 Identification of the technical system</b></p>		
<p><b>1.1 Designation</b> Designation: "Flamethrower VULKANUS". Model designation: "mod/01". Model number: "700-953".</p>		
○	<p><b>1.2 Scope</b> The technical system consists of a Fuel tank (article number 700-953-001), steel tubes with hose package (article number 700-953-002), and three different fuels (article number 700-953-003 - 005).</p>	
○	<p><b>1.3 Performance</b> The technical system's technical performance is described in the technical documentation including drawings. The designation of the technical documentation is "ggggggg-vvvv-01" and is included as annex 1. Differences, compared to the previous version (Flamethrower VULKANUS, trial edition, model number 600-01) the coil has been replaced with a newly designed coil with similar function but different internal way of working. This has produced greater reliability and the risk of accident has been reduced to a tolerable level of risk.</p>	
<p><b>1.4 Marking</b> Sign with information as stated in 1.1 is attached to the flamethrower fuel tank.</p>		
<p><b>1.5 Use</b> The technical system is intended to be used for all the operational phases and under all the external conditions that are reported in the description book with the designation "ggggggg-vvvv-02" which is included as annex 2 here.</p>		
○	<p><b>2 Supporting documentation</b></p>	
○	<p><b>2.1 SSPP and SAR</b> DesignA requirements for the supplier's implementation of the system safety activities are shown in the System Safety Plan 20XX-05-20 (Pettersson Smide AB ref. no. 101/-XX to which reference is made in DesignA's order). The results of the implemented system safety activities are documented in the System Safety Report (SAR), (Pettersson Smide AB ref. no. 101/-XX). Under 3 below there are summaries of the essential elements of the System Safety Report.</p>	
<p><b>2.2 Systems safety requirements</b> The system safety requirements applied in the system safety activities are comprised of:</p>		
<ul style="list-style-type: none"> <li>• The purchaser's requirements under section System Safety Requirements in the RFP and the corresponding section in our tender (Pettersson Smide AB ref. no. 151/-08.)</li> </ul>		

Pettersons Smide AB Simpevarp	SAFETY COMPLIANCE ASSESSMENT 15-06-20XX	Ref. 102/-XX
<ul style="list-style-type: none"><li>• Applicable Swedish laws and regulations from the National Chemicals Inspectorate, the Environmental Protection Agency and the Swedish Civil Contingencies Agency, all of which are listed in the SAR. SAR makes up annex 3 to this safety compliance assessment.</li></ul>		
<b>2.3 Classification of accident risks</b>		
In the classification of accident risks, methods in accordance with the Armed Forces' Handbook System Safety 2011 have been applied.		
<b>3 Implemented system safety activities</b>		
<b>3.1 Identification of accident risks through analysis and testing</b>		
○	For the identification of accident risks, a Risk Log has been developed, within which, identified hazards and hazardous conditions have been documented. A preliminary risk source analysis has been carried out. This has identified potential hazardous events which have been analyzed by means of fault trees and fault effect analyses. The results of all analyses and tests have been documented in the technical system's Risk Log.	
○	The sensitivity of the structure/design in terms of both normal environment and abnormal environments in accordance with the requirements specification have been tested through practical testing.	
Analysis and test results have been used continuously in the design work.		
In this respect, it has been possible to eliminate all single faults through redesign.		
It has not been possible to determine any common cause-fault.		
<b>3.2 Risk reduction measures</b>		
Numerous risk-reducing measures have been taken and incorporated into the design (see list in SAR).		
The most important measure is considered to be the introduction of composite fuel. The fuel (liquid) consists of two stable, relatively insensitive components which when mixed assume characteristics required of an efficient fuel, which means that it becomes highly sensitive to external stimuli, has a low flash point, etc. The two components are stored in separate containers on the flamethrower and are first mixed in the nozzle while being used (during firing).		
○	<b>3.3 Potential hazardous events, remaining risks</b>	
○	A list of possible hazardous events is produced through a preliminary analysis of risk sources and hazardous conditions and are reported in SAR. This list relates to type-approved Pettersson Forging AB products (according to type approval ref 121/-XX) and presents accident risks at the system level, during the interaction between sub-systems and above the system level through interaction between the technical system and the vehicles it can be mounted on.	
For each hazardous event or hazardous condition, the accident risks have been identified and the safety regulations required for the prevention of an accident, illness, disease, system loss or damage to the external environment have been specified. A list of the safety regulations that form part of SAR is described in annex 3 of this safety compliance assessment.		
<b>3.4 Hazardous substances/materials</b>		
All hazardous substances/materials have been identified through analysis according to applicable laws and regulations as well as the Armed Forces' special environmental conditions as per the requirements in the tender.		

Pettersons Smide AB  
Simpevarp

SAFETY COMPLIANCE ASSESSMENT  
15-06-20XX

Ref. 102/-XX

### 3.5 Safety regulations

Based on the risks listed in the Risk Log for Flamethrower VULKANUS, the following safety precautions that form a part of the risk-reducing measures have been compiled for the system. Each safety instruction specifies the measures the user must observe so that each accident risk should be kept to a tolerable risk level.

It is for the user to comply with these safety regulations and that before each use, thoroughly train each person who intends to use the flamethrower.

Safety regulations:

- When refuelling, the two fuel components must be kept apart and the filler caps must not be mixed up. The special mounting devices for the filler caps (chains) must not be broken.
- When in use (being fired), own troops must not stand within a semicircle in front and to the side of the shooter, where he/she is in the centre. The radius of the circle is 35 metres.
- Firing is not allowed when the wind blowing against the direction of fire exceeds 15 metres per second.

### 4 Safety compliance assessment

The VULKANUS flamethrower mod 2001 with model number 700-953 is designed to the best possible specifications. The development work has been supported by a comprehensive system safety activities in accordance with DesignA's established SSPP and whose results are reported in the above system safety report. A number of safety regulations have been specified for the flamethrower which are reported in the system safety report.

The VULKANUS flamethrower mod 2001 with model number 700-953 is as safe as can reasonably be expected under the following conditions:

- Safety regulations as stated in clause 3.5 above and the system safety report should be carefully observed.
- Personnel should be familiar with the handling of the flamethrower.
- Personnel should be trained in handling, safety regulations, care and first line maintenance of the flamethrower
- Personnel who participated in the test activities with the system, should be trained on the difference between the trial edition with model number 600-01 and the VULKANUS flamethrower mod 2001 with model number 700-953.

Sven Pettersson  
MD Petterssons Smide AB, Simpevarp

### Annexes

1. Technical documentation including drawings, with the designation "ggggggg-vvvv-01"
2. Description book with the designation "ggggggg-vvvv-02"
3. System Safety Report / SAR, Petterssons Smide AB, ref. 101/-XX

## Comments Regarding the System Safety Compliance Assessment

If no other demands have been made with regard to the time for the transfer of the SCA, 5.27, the focus should be on submitting the SCA as soon as possible. As and when the first series of items are produced, the SCA should be able to be submitted to DesignA.


Test materiel is usually dealt with in the same way as series produced materiel. However, the documentation cannot be as comprehensive nor can the possible areas of use or environments/ abnormal environments be as complete as those for series produced materiel.

The drawing up of the SCA for test materiel is more or less a dress rehearsal prior to the production of the SCA for series produced units, for example.

For complex or safety-critical systems, DesignA, as a result of its SSWG-1, 5.8, will check that the SSPP is followed up by the supplier during the development and design phases.

# System Safety Approval

## An Example of DesignA's Safety Statement

	UNCLASSIFIED	Date	FMV Documents designation	Version
		2010-04-09	ÅÅFMVXXXX-1	1.0
			Area/unit responsible	Classification no.
				Page
				1 (3)

Armed Forces/PROD

**Safety Statement for VULKANUS flamethrower mod 01 M2101-XXX (9 annexes)**

**1 Identification of the technical system**

**1.1 Name and model number**

The technical system is called "VULKANUS flamethrower".

The model number is "mod 01"

The technical system has type number "700-953"

Stock number: M2101-xxxxxx

Stock title: VULKANUS flamethrower mod 01.

**1.2 Scope of the technical system**

The technical system consists of a fuel tank (article number 700-953-001), steel tubes with hose package (article number 700-953-002), and three different fuels (article number 700-953-003 - 005).

**1.3 Technical design**

The technical system's technical performance is described in the technical documentation which includes drawings designated "vvvvvv-gggg-01" and which are included here as annex 1.

Divergence, compared with previous trial edition (VULKANUS flamethrower, trial edition, type number 600-101) involves the unit xxxx being replaced with a device with similar functionality but which internally has a quite different mode of operation. As a result of this, greater reliability is obtained, and the accident risk (personal injury) has been reduced to the specified requirements level.

**1.4 Marking**

Sign with information as stated in 1.1 is attached to the flamethrower's fuel tank.

**1.5 Use**

The technical system is intended to be used for all the operational phases and under all the external conditions that are reported in the description book with the designation "vvvvvv-gggg-02" which is included as annex 2.


FMV  
Försvarets materielverk  
115 88 Stockholm  
Street address: Banérgatan 62

Tel: 08-782 40 00  
Fax: 08-667 57 99

registrator@fmv.se  
www.fmv.se

CIN: 202100-0340

FMV Mall Upprättad basering Utlösare nr 11.0

	<b>UNCLASSIFIED</b>	Date	FMV Documents designation	Version
		2010-04-09	ÅÅFMVXXXX-1	1.0
			Area/unit responsible	Classification no.
				Page
				2 (3)

**2 Scope**

This safety statement includes the following part-approvals:

- a) The safety statement for the technical system VULKANUS flamethrower in accordance with annex 3.
- c) This safety statement for the VULKANUS flamethrower's installation on Combat vehicle 90 and light armoured vehicle in accordance with annex 5 and 6.

**3 Supporting documentation**

The supplier's system safety work as defined in the System Safety Plan has been continuously monitored and, where appropriate has been realigned by the Project Management's System Safety Group (SSWG-1).

The supplier's safety statement, including safety and Risk Log have been reviewed and found to correctly describe the safety work and residual accident risks.


**4 Safety regulations**

In order to ensure a tolerable level of risk, a number of safety regulations and restrictions are required. These are provided in the following documentation:

- Approved fuels listed in annex 4
- Support documentation for operating instructions in accordance with annex 7.
- Support documentation for the safety instructions in accordance with annex 8.
- Support documentation for instructions for stock storage in accordance with annex 9.

FMV/Mat Typensakhandling 10/10/10



	UNCLASSIFIED	Date	FMV Documents designation	Version
		2010-04-09	ÅÅFMVXXXX-1	1.0
			Area/unit responsible	Classification no.
				Page
				3 (3)

**5 Safety statement**

The safety work for the VULKANUS flamethrower has been completed. The intended outcome, i.e. that the residual accident risk is tolerable, has been achieved. In order for the level of risk to remain at this level, it is necessary that DesignA has issued documentation for handling and storage requirements which are carefully observed by FM.

The VULKANUS flamethrower is hereby approved from a safety point of view.

Swedish Defence Materiel Administration

Hans Hansson

Bengt Bengtsson

**Annexes**

1. Technical documentation including drawings – with the designation "vvvvvv-gggg-01"
2. Description book with the designation "vvvvvv-gggg-02"
3. The safety statement for the system VULKANUS flamethrower
4. Restrictions for approved fuels
5. This safety statement for the VUKANUS flamethrower's installation on Combat vehicle 90
6. This safety statement for the VUKANUS flamethrower's installation on light armoured vehicle 2008
7. Support documentation for operating instructions.
8. Support documentation for safety instructions.
9. Support documentation for instructions for stock storage.

FMV MBE (Operational handling) Version 1.0

### *Comments Regarding the Safety Statement*


**Time.** When can this take place? The supplier's SCA, 5.27, cannot be obtained before the prototype has been tested and is ready. Often, this is not before the series type test is ready.

What are the Armed Forces' requirements? Naturally, the Armed Forces wants DesignA's documentation as soon as possible. The Armed Forces must produce its documentation before the materiel can be used by the unit. The solution may involve *cooperation*, so that the supporting documentation is developed successively and is firmly established by the Armed Forces through preliminary documentation. In this way the Armed Forces is given the opportunity to begin its work on the development of the CSSB, see below under test materiel.

**Test materiel.** The production of systems is usually a complicated process which takes a long time. The process often includes several successive field trials before series-produced units can be presented to the Armed Forces. Prior to each submission of systems for field trials etc., to the Armed Forces, a decision is taken regarding system safety approval. However, it is sufficient that the number of annexes, compared to the example above, and their content are adapted to the activity and the conditions that are relevant for how the system, in each individual case, is intended to be used. This is defined accurately in the safety statement, 5.31.

## Central Safety Compliance Decision (CSSB)

### An Example of the Design of the Armed Forces' CSSB

	<b>SWEDISH ARMED FORCES</b> ARMED FORCES HEADQUARTERS	Date	Designation	Page 1 (3)
		2010-04-06	14 910:XXXXX	

<input type="radio"/>	Your reference	Your date	Your designation
<input type="radio"/>	Our reference Sven Svensson	Our previous date	Our previous designation

**MS 895 Central Safety Compliance Decision for the technical system the VULKANUS flamethrower, mod 01, M2101-xxxxxx**  
(3 annexes)

**1. Identification of the technical system**

**1.1. Name and model number**

The technical system is called "VULKANUS flamethrower".  
 The model number is "mod 01"  
 The technical system has type number "700-953"  
 Stock number: M2101-xxxxxx  
 Stock title: VULKANUS flamethrower mod 01.

**1.2. Scope of the technical system**

The technical system consists of a Fuel tank (article number 700-953-001), steel tubes with hose package (article number 700-953-002), and three different fuels (article number 700-953-003 - 005).

**1.3. Design of the technical system**

The technical system's technical performance is described in the technical documentation which includes drawings designated "vvvvvv-gggg-01" and which are included here as annex 1.

Divergence, compared with previous trial edition (VULKANUS flamethrower, trial edition, type number 600-101) involves the unit xxxx being replaced with a

( )

Mailing Address	Visiting Address	Telephone	Fax	E-mail, Internet
Högkvarteret	Lidingövägen 24	+46 8 788 75 00	+46 8 788 77 78	exp-hkv@mil.se
SE-107 85 Stockholm				www.forsvarsmakten.se/hkv
SWEDEN				

device with similar functionality but which internally has a quite different mode of operation. As a result of this, greater reliability is obtained, and the risk of an accident occurring (personal injury) has been reduced to a tolerable level.

#### 1.4. Marking

A sign with information as stated in 1.1 is attached to the flamethrower's fuel tank.



In order to allow materiel and injury reports with portable field equipment (micro-computer terminal), all parts are marked with bar codes.



#### 1.5. Use

The technical system can be used for all operational phases and the external conditions which the Operating Instructions for the VULKANUS flamethrower mod 01 with ref vvvvvvvvvvvv-lllllll specify.

### 2. Background

DesignA has, through communication to Department 14 910:XXXX decided on a safety approval for the system VULKANUS flamethrower Mod 01, M2101-xxxxxx. DesignA has therefore also presented restrictions on its use along with support documentation for FM's preparation of instructions and Safety regulations to ensure safe handling.

### 3. SSWG-2



Workgroup System Safety (SSWG-2) and details regarding this have been decided. The work group's assignments and manning are described in annex 2.

### 4. Restrictions and supplementary safety provisions



Restriction: The flamethrower may only be used with water as ammunition until the approved munitions have been determined.

Additional safety rule: When firing with water, the minimum firing distance towards a person is 15 m.

### 5. Consultation

C MARKI has signed a cooperation agreement.

## 6. Central Safety Compliance Decision (CCSB)

The manager of PROD hereby decides on the CCSB for the VULKANUS flamethrower mod 01 as a basis for the FM Decision regarding use (BOA).

In so doing, the instructions for the technical system and constituent sub-systems as described by the materiel descriptions (or equivalent), regulations and instructions are applied. The current publications are listed in annex 3.



The technical system can be used while being carried by a person, it can be mounted on the Combat vehicle 90 and a light armoured vehicle 2000.



The technical design/version is hereby established and may not be altered without a new CCSB from the Manager for PROD Armé. The technical design is described in annex 1.

A decision regarding the above instructions in the safety instruction have been made with the support of FM ArbO.

Carl Carlsson  
Unit Manager

Sven Svensson  
MSA

### Annexes



1. Safety Statement (DesignA)

2. Workgroup System Safety, (SSWG-2) details and representatives.



3. Applicable publications

Sent to:  
PROD  
FMV

For information within HQ  
SÅKINSP  
GL  
LEDS  
INS

## Comments Regarding the Central Safety Compliance Decision


**Time.** When can this take place? The supplier's system safety approval, 5.27, cannot be obtained before the prototype has been tested and is ready. Often, this is not before the series type test is ready. Only then can DesignA's safety statement, 5.31, be generated and submitted.

**The Armed Forces' requirements.** Naturally, the Armed Forces wants DesignA's documentation as soon as possible. The Armed Forces must produce its documentation and the CSSB, 5.33, before the materiel can be used by the unit. The solution may involve cooperation, so that the supporting documentation is produced in stages and the circulation of the report for comments/obtaining approval from the Armed Forces with preliminary documentation is made before DesignA's safety statement is decided. This provides the Armed Forces with the opportunity to start the work of preparing the documentation in accordance with paragraphs 4 and 6 in the example, see below under test materiel.

**Test materiel.** The production of systems is usually a complicated process which takes a long time. The process often includes several successive field trials before series-produced units can be obtained. Prior to each field trial (series of tests), on specific pilot units of the system, a decision (CSSB, 5.33) is taken regarding use. However, it is sufficient that the documentation, according to 3 and 4 in the example above, is limited to the activity and the conditions under which the systems, in each individual case, are intended to be used.

## Safety Certificate

### Examples of the Design of DesignA's Safety Certificate

	<p style="text-align: center;">SAFETY CERTIFICATE</p> <p>Date 2010-06-14      FMV designation ÅAFMVXXXX-1</p>	<p>Page 1 (4)</p>						
<p>Sent to:</p>								
Your reference	Your date	Your designation						
FMV dept, issued by AK Sjö, name name, tel.	FMV prev. date	FMV prev. designation						
<p><input type="radio"/> <b>MS 211. Tugboat type Large. Tugboat DRAGAREN</b> (x annexes)</p>								
<p><input type="radio"/> <b>1 Background</b> Trial run to be carried out in accordance with PTK order XXXXX. Agreements for maritime safety system between FMV and the Armed Forces in accordance with FMV ref. XXXXX</p> <p>Previously issued Safety Approval as the basis for / is hereby repealed:</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;">Document name</th> <th style="text-align: left; border-bottom: 1px solid black;">Document designation</th> <th style="text-align: left; border-bottom: 1px solid black;">Date</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>			Document name	Document designation	Date			
Document name	Document designation	Date						
<p><input type="radio"/> <b>2 System identification</b></p> <p><b>2.1 Storage designation etc.</b></p> <p>The system/service unit includes the following:</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;">Stock number:</th> <th style="text-align: left; border-bottom: 1px solid black;">Vessel name</th> <th style="text-align: left; border-bottom: 1px solid black;">Designation</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>			Stock number:	Vessel name	Designation			
Stock number:	Vessel name	Designation						
<p><input type="radio"/> <b>2.2 Technical design</b></p> <p>The configuration is defined in the following general design drawing.</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid black;">Designation</th> <th style="text-align: left; border-bottom: 1px solid black;">Drawing number</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table> <p>The modification is determined with TO MF XXXXXXXXX</p>			Designation	Drawing number				
Designation	Drawing number							
<p style="font-size: small; text-align: left;">Service / Uppdrags handling / Var 0.2</p> <p style="text-align: center;"><b>Försvarets materielverk</b></p> <table border="0" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; border-bottom: 1px solid black;">Postal address 115 88 Stockholm</td> <td style="width: 25%; border-bottom: 1px solid black;">Street address Banérgatan 62 (T-Karlaplan)</td> <td style="width: 25%; border-bottom: 1px solid black;">Telephone 08 - 782 40 00</td> <td style="width: 25%; border-bottom: 1px solid black;">Telefax 08 - 667 57 99</td> <td style="width: 25%; border-bottom: 1px solid black;">Internet www.fmv.se e-mail: registrator@fmv.se</td> </tr> </table>			Postal address 115 88 Stockholm	Street address Banérgatan 62 (T-Karlaplan)	Telephone 08 - 782 40 00	Telefax 08 - 667 57 99	Internet www.fmv.se e-mail: registrator@fmv.se	
Postal address 115 88 Stockholm	Street address Banérgatan 62 (T-Karlaplan)	Telephone 08 - 782 40 00	Telefax 08 - 667 57 99	Internet www.fmv.se e-mail: registrator@fmv.se				



**SAFETY CERTIFICATE**

Date 2010-06-14 FMV designation ÅAFMVXXXX-1

**2.3 Labelling, traceability, etc.**

All units have been assigned a military designation as follows:

Stock title	Stock number	Designation
-------------	--------------	-------------

**2.4 Documentation / Publications**

The following publications are applicable for the use, care and maintenance of the system:

Stock title	Stock number	Remark
-------------	--------------	--------

**2.5 Extent of system safety**

System safety activities and this Safety Approval include implemented and completed new installations including modifications and their integration into an existing system.

**2.6 Interfaces to other systems/service units**

Document name	Document designation	Date
---------------	----------------------	------

**3 Area of use**

Trial run order and trial run instructions are available in XXXX

The area of use for the system is defined in YYYY

**4 Description of the implemented system safety work**

**4.1 General**

The supplier's system safety work has been continuously monitored and has been found to be satisfactory. The safety statement issued has been examined and has been found to correctly describe the implemented safety work and residual risks.

**4.2 Registration inspection/Certification**

**4.3 Part-approvals, sea-worthiness approvals etc.**

Senicec / Uppskådd handling / Ver 8.2





**SAFETY CERTIFICATE**

Date  
2010-06-14

FMV designation  
ÅAFMXXXX-1

Page 3 (4)

**5 Requirements fulfilment**

Assessment of tolerable risk level has been made for system safety requirements in HKV document XXXX / YYY TTFO.

A tolerable level of risk has, subject to specified restrictions, been achieved for all risks.



**6 Restrictions**

To obtain a tolerable risk level, it is important that ....



Prior to using the vessel, there must be an approved seaworthiness inspection certificate from MFI (Marinens Fartygsinspektion).

**7 Safety certificate**

The safety work has been completed. As this work progresses, it aims to remove restrictions in accordance with section 6 above.

In the safety statement, "specified measures" to bring the risks to a tolerable level, have been implemented. Constructive measures have been introduced, operation and maintenance publications have been updated and warning signs have been erected in accordance with the "specified measures" in the safety statement.

In order to maintain the level of risk, handling and operational rules, instructions on how to care for equipment and restrictions as described above must be followed.



The Military Maritime Safety Inspectorate has signed a cooperation agreement regarding this Safety Certificate.

The tugboat Dragaren has hereby been approved from a safety point of view.




A decision in this matter has been taken by X nn. This has been submitted by PRL MS 2XX nn, and in the final preparation, PRL nn and PRL nn have participated.

Swedish Defence Materiel Administration

nn  
VGL x

nn  
PRL MS 2xx

Service / Utredningshandling / Ver 82

	<b>SAFETY CERTIFICATE</b>
	Date: 2010-06-14      FMV designation: ÅAFMVXXXX-1
	Page 4 (4)
 <b>Sent to:</b>	
HKV	(Intended for SJÖI and PROD MARIN)
MarinB	(Intended for FC Dragaren)
 <b>For information</b>	
MarinB O	(intended for TeK Ftg)
 <b>Within FMV</b>	
<input type="radio"/>	TC Sjö
<input type="radio"/>	VGL X
<input type="radio"/>	PRL MS 2xx
<input type="radio"/>	Archive
 <b>Annexes</b>	
Annex 1	Safety Statement from supplier XX
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	
<small>Senaste Uppgrädd handling / Ver 92</small>	

Comments Regarding the Safety Certificate

**Time.** If no other demands have been made in this regard, the safety certificate, 5.31, is submitted to the Armed Forces before PTK begins to use the vessel for sea-going activities.

## Definitions

To facilitate the understanding of the manual, the concepts and acronyms used are provided in the glossary below. Swedish Standard SS 441 05 05, MIL-STD-882C and specialist literature in systems security, has served as the basis for most of these definitions. Note that certain terms have slightly different definitions in various standards. For example, there are differences between Swedish and American military standards.

A number of definitions are specific to the Handbook.

Concept	Explanation
Accident risk	<p>Relates to a risk of harm to a person, property or the external environment.</p> <p>Expressed as a function of the probability of an accident happening and its consequences (the consequences are usually divided into the four injury/damage classes for individuals and the economy).</p> <p>Is distributed, if possible, at sub-risk levels for the four injury/damage classes.</p>
Accident, Mishap	<p>Occurs when someone/something is exposed to a hazardous event or hazardous condition and is therefore injured/damaged (injury/damage to a person, to property or the external environment). An accident is always unplanned, not the result of a hostile act for example.</p> <p>The term “mishap” is used only in the United States.</p>
ALARP	<p>As Low As Reasonably Practicable, as low as practically and reasonably possible (implies a certain risk).</p> <p>A term used in British law – it means that actions to reduce a particular risk should be continued as long as the operation provides an appreciable effect on the risk at a reasonable cost.</p>
Ammunition	<p>Materiel/technical systems intended to produce a harmful effect, smoke or lighting effect, blasting, the laying of mines, mine-clearance and materiel/technical systems which following training replace this. The materiel/technical system may contain explosives or other chemicals.</p>

Concept	Explanation
Approved processes (RML - Rules for Military Aviation)	Every authorization issued is based on an appropriate operational management system. The operational management system includes defining the processes which, among other things, are critical to the quality of the products and services that are delivered. These processes should therefore be approved by the aviation authorities.
Aversion factor	This means that a major injury is tolerated to a lesser extent than with a comparable accident that results in minor injuries.
Barrier	Protective device, such as a sheet metal plate in front of spinning wheels, axles, chains, live tracks, but also in the form of soft parts, which provide a direct, protective function. Even personal protective equipment can be regarded as a part of the barrier.
Battle damage repair	Method of corrective maintenance aimed at quickly restoring technical systems to battle readiness after they have been damaged. Battle damage repairs are carried out only during war or warlike conditions. The repairs should be acceptable from a system safety point of view (see STANAG 2418).
Cause of Failure	The conditions giving rise to a failure.
Central operator	Head of the Armed Forces' command staff, the production manager and operation manager are both central operators.
CIP Convention	The CIP Convention (Permanent International Commission for Firearms Testing) ensures that every civilian firearm, and all civilian ammunition that is sold in the participating countries, is safe for the user. The CIP convention covers 14 countries (Sweden is not a member). The Commission Internationale Permanente pour l'Épreuve des Armes à Feu Portatives.

Concept	Explanation
CIP proof mark	<p><b>Civilian firearms</b></p> <p>Manufacturers and importers of firearms in a country that is a member of the CIP are required to ask an approved testing agency to perform the testing of any firearm they manufacture or import. Upon completion and approval, the tested weapon parts are provided with a CIP label.</p> <p><b>Ammunition</b></p> <p>The CIP Convention requires manufacturers and importers of ammunition to be sold to a CIP country to continuously test the ammunition during production in accordance with CIP specifications. Such ammunition is provided with a CIP proof mark.</p>
Civil ammunition	Civilian ammunition that is traded (COTS - Commercial off the Shelf) and is equipped with a CIP proof mark (replaces the CE mark).
Civilian handgun	Civilian small arms (handgun) that is traded (COTS) and is equipped with a CIP proof mark (replaces the CE mark).
Configuration decision	Product documents which specify the scope and configuration of a technical system.
Contributing causes	In order for the damaging effects of a source of a risk to be activated, a certain mechanism is required (see <i>Trigger</i> .)
Critical characteristics	A characteristic (tolerance, surface finish, material, manufacture, assembly) of a product, material or process which may result in the failure of a critical item in the event of non-fulfilment of requirements.
Critical defect	Deviation from stipulated requirements regarding a certain characteristic which may lead to an unsafe condition.
Critical fault	A deviation from specified demands in respect of certain characteristics and which can therefore lead to an unsafe condition.
Critical items	A part, assembly, installation or production process with one or several characteristics which results in an unsafe condition in the event of non-fulfilment of requirements.

Concept	Explanation
Customer order KB	The ordering of a product or service from the Armed Forces to DesignA. Includes a decision about money and a specification as to what must be delivered, time constraints and more. If the order relates to a technical system (a reference to) Tactical-Technical-Financial Objectives (TTEM)/Technical Financial Objectives for Training Materiel (TEMU) is included.
Danger/Hazard	A condition which is a prerequisite for an accident, includes both a source of risk and a hazardous condition.
Decision document for system safety	Collective term used in the handbook for the following three decision documents: <ul style="list-style-type: none"> <li>• Safety Compliance Assessment (SCA).</li> <li>• Safety Statement (SS).</li> <li>• Central Safety Compliance Decision (CSSB).</li> </ul>
Defect	Deviation from stated requirements regarding a specified characteristic.
Design review	Aimed at examining all technical records in a quality-assured and traceable manner.
Deterministic risk analysis	Deterministic risk analysis is based on the physical risks involved, i.e. that could happen. In this respect, this could either be the worst possible incident which leads to injury or a dimensioning incident (see probabilistic risk analysis).
EASA	The European Air Safety Agency (EASA) via a European Commission (EC) regulation has taken over the European national administrative data for the approval of aircraft equipment for the open European market.
Effect/Damage	The consequence of an accident/incident consists of any injury to a person or damage to property and the external environment.
Environment	Areas in which an organization operates, which includes air, water, land, natural resources, flora, fauna and humans and how they interact.
Expedient repair	Method for non-permanent corrective maintenance of operating damage and/or battle damage involving unconventional repair methods and/or alternative spare materiel supplies. The repair must be acceptable from a system safety aspect.
Expert system	See <i>Neural networks</i> .
F-code	Storage code under IFTEX. It forms the basis of how the Armed Forces' ammunitions stores may be kept.

Concept	Explanation
Facility	For certain functions or activities, a prepared area of land, a building or a room, including the requisite installations for the function or activity, such as fortifications, the building of barracks, a base area, links etc. A facility also includes any military fortifications that are required. Facility-bound supplies are also required for the facility.
Fail safe	Characteristic of a unit which prevents defects from becoming critical faults. A fail-safe design is one which ensures that the system moves into a safe state if a fault occurs.
Failure	The discontinuation of a unit's capability to fulfil its required function.
Failure probability density	Failure frequency rating at a given point in time.
Fault effect, Fault consequence	The result which is a direct or indirect consequence of a fault.
Fault mode	One of the possible fault conditions in a unit.
Handling	Handling relates to manufacturing, processing, treatment, packaging, storage, transport, use, disposal, destruction, marketing, maintenance, conveyance and other similar procedures. (The definition comes from the Flammable and Explosive Goods Act.)
Harm	Injury to a person, damage to property or the external environment. The term injury/harm relates to all H SystSäk E possible outcomes.
Hazard severity category	For personal injury: death, serious personal injury, minor personal injury and negligible injury. For financial damage: comparable to total system loss, major loss, limited loss and minor loss. Details can be found in <i>H SystSäk E Part 1, section 4.2.3</i> .
Hazardous condition	A physical situation that could lead to an accident occurring.
Hazardous event	An event that occurred by misadventure, that is, without intention, unplanned, and which may result in an accident or incident if someone or something is exposed.
Incident	A hazardous event that does not lead to an accident, as nothing is exposed during a hazardous event.

Concept	Explanation
Incremental development	First the central parts of the system are constructed. This ensures that they function in accordance with the specified requirements. Later additional functions are added and they are inspected in the same way. Once all the required features are in place, the system is ready.
Individual risk	The rate at which an individual is likely to be exposed to a given level of injury/harm caused by specified dangers (Institution of Chemical Engineers – IChemE). It is usually based on an average person in the group.
Interface	Actual environment for certain technical systems. May be made up of other technical systems, power supply (voltage, frequency, current), water, sewage, fuel supplies, repair facilities, air traffic control and more.
Item	A term used to designate a subsystem apparatus, component, part, etc., which may be regarded as separate.
Less serious injury	An injury that a person recovers from following hospital care (e.g. a fracture).
Limited tolerable	A certain level of risk. The Request For Proposal (RFP) specifies who can decide on a risk at this level.
Managing activity	The term often refers to a procurement organisation such as the Armed Forces and DesignA, but may also include suppliers or subcontractors who require an activity of their subcontractor.
Mandatory requirement	A requirement which is of crucial importance to system safety.  Comments: If a <i>mandatory requirement</i> cannot be met, for example for tactical or cost reasons, non-compliance is permissible if it can be demonstrated that an acceptable level of safety can still be maintained.
Materiel system	See <i>Technical system</i> .
Military accident risk	Risk of injury during a battle caused by deficiencies in materiel design and function. Especially crucial is the advantage the enemy could receive from this in a combat situation.
Military ammunition	Ammunition, regardless of origin, which is intended for use to conduct military operations.
Military materiel (equipment)	Technical systems that have been specifically designed and manufactured (even through integration) to carry out military operations.
Military purpose	Activities aimed at preparing and implementing organized, armed combat.



Concept	Explanation
Negligible damage	An injury which is trivial and minor. Dealt with by using a “plaster and a few days rest”.
Neural networks	Technology for creating expert systems. Refers to algorithms for information processing that try to imitate the function of nerve cells and the brain.
Operational environment	Actual environment for a specific technical system. May be made up of other technical systems, power supply (voltage, frequency, current), water, sewage, chemical conditions, fuel supply, repair facilities, air traffic control, etc.
Operational safety	Armed Forces’ operational safety refers to the Armed Forces’ ability to manage risk in all aspects of its operations so that the constitutional requirements, in terms of the working environment and safety for the Armed Forces’ personnel and requirements with regard to safety for third parties, the external environment and property, are met.
Optional requirement	The selection of optional requirements to be implemented for a technical system adapted by the client based on the complexity of the system (see <i>Mandatory requirement</i> ).
Owner representative (ÄF)	The ÄF is responsible for the status, privacy, existence and presentation of the supplies before the government. FMV is the ÄF of materiel before delivery to the Armed Forces. The Armed Forces is the ÄF from the time of delivery (and approval) of any supplies to the Armed Forces to the time that the supplies are reported as withdrawn from the Armed Forces’ stock of supplies. This also applies to assets placed in the industry and with the FMV.
Personal safety	The capability of a system to avoid causing unacceptable personal injury.
Proactive	Anticipative and preventive.
Probabilistic risk analysis	Probabilistic risk analysis methods assume that both the probability of accidents will occur, as the consequences arising from them are important for assessing the risk level (see <i>Deterministic risk analysis</i> ).
Probability of failure	The probability of one or more failures occurring during a specified time period.

Concept	Explanation
Product	The product is understood here to be mainly products that are “sold over the counter”/are commercially available (COTS) and from a safety point of view are designed to comply with product safety and product liability laws and the relevant European Union (EU) directives.
Product safety	Capability of a product to avoid causing personal injury or damage to property or the external environment.
Qualification	Verification of a product’s characteristics.
Reactive	The subsequent action taken to try to prevent the repeat of, for example, an accident.
Responsible for design (DesignA)	The person who has this roll with technical design responsibility (see <i>Technical design responsibility</i> ). Examples of DesignA include: a government agency, a foreign government and the supplier of OPS (PPP Private Public Partnership) contracts with the Armed Forces.
Restriction	Temporary restriction within the technical system’s permitted use to temporarily deal with a certain risk and therefore contain the demands on system safety.
Risk	<i>Se Accident, Mishap.</i>
Risk acceptance	For all elements of a technical system’s accident risks, acceptance decisions are made. The acceptance decision is compared to the value of the accident risk, taken from the technical system’s risk log, with the specified risk value.
Risk analysis	Systematic use of available information so as to identify hazards and assess risks to people, property, materiel or the external environment.
Risk log	Documents for the documentation of a technical systems’ total risks. Refers to the replacement of previous documents Preliminary Hazard List (PHL), Hazard List and Risk List
Risk matrix	Two-dimensional graph used to illustrate the connection between probability and consequence. Can be graded and provided with borders showing acceptance criteria.
Risk reduction activity	Eliminate hazards. Design intended to eliminate any risk. Introduce protective devices (also referred to as barriers). Introduce active warning devices (such as audio/visual signals). Impose restrictions/training/instructions/warning signs.

Concept	Explanation
Risk source	Something that may lead to personal injury or damage to property, materiel or the external environment.
Safety	Absence of any risk of an accident occurring that could lead to unintentional injury.
Safety analysis	A collective term for those parts of the system safety activities involving both systematic identification of possible hazardous events and their causes and qualitative or quantitative assessment of the risks of a technical system.
Safety certificate	Issued by DesignA and is a form of system safety approval. The safety certificate means that DesignA, after inspecting all the relevant circumstances, has found that the vessel that Sea Trials Command (PTK) is to test has an acceptable level of safety. The safety certificate is sent to the Armed Forces Maritime safety inspection which, on agreement, submits this to the PTK.
Safety defect	A product has a safety defect if it is not as safe as can be reasonably expected.
Safety management	An applied form of quality control defined as all actions intended to influence the safety of an establishment.
Safety message	A report submitted in the special case that design has mandated for a specific technical system that a system safety approval must be issued, but where the technical system in question is found not to have an acceptable safety level.
Security	Absence of relationships involving espionage, sabotage, terrorism and other crimes against national security.
Serious (bodily) injury	Injury with a permanent loss of body function/body part.
Service life	Total time from the creation of a system until its decommissioning.
Single Failure Criterion, Single Event Criterion	Fault or incident which on its own can lead to a hazardous event.
Societal risk	The relationship between frequency and number of people affected by a specified level of damage in a given population exposed to specified risk (IChemE). It therefore calculates the number of people who are covered by an accident.
System	See <i>Technical system</i> .

## Definitions

Concept	Explanation
System hazard	Accident risk at overall system level, which is inadvertently caused by the system's required capabilities. Often appears in response to the question: Given system capacity, what may this not lead to/cause/what should not happen?
System of systems	The capability that is created through the use of existing technical systems and products in a new way, possibly along with additionally employed materiel.
System safety	Property of a technical system that does not inadvertently cause damage to a person, property or external environment. (Person: death, physical injury or illness. Property: damage to or loss of property or equipment. External environment: "superficial" damage which can be reconstituted wholly or in part or permanent damage, such as the eradication of a species).
System safety activities	The total amount of work that is carried on for a technical system during the study, development, acquisition/ procurement, refurbishment and modification, production, operation (including technical adaptation), maintenance and decommissioning, in order to identify and quantify risks and eliminate them or reduce them in accordance with the requirements that have been established.
System safety decisions	System safety decision: is a general term, which in this handbook includes: <ul style="list-style-type: none"><li>• SCA</li><li>• SS</li><li>• CSSB.</li></ul>

Concept	Explanation
System safety documentation	<p>With full system safety documentation for a specific technical system it relates to the following.</p> <ul style="list-style-type: none"> <li>• Documents from the supplier: <ul style="list-style-type: none"> <li>Risk documentation, including Risk Log, with risk decisions for each risk.</li> <li>System safety report with analytical results (from analysis activities that have been carried out such as PHL, PHA, SHA and others).</li> <li>Safety compliance assessment.</li> </ul> </li> <li>• From DesignA: <ul style="list-style-type: none"> <li>System safety approval (all the above materials from the supplier form part of the documentation).</li> </ul> </li> <li>• Within the Armed Forces: <ul style="list-style-type: none"> <li>CSSB.</li> </ul> </li> </ul> <p>To link risk documentation and system decisions to a certain technical system requires a decision on the current configuration of the technical system.</p> <p>System security decisions, when used in this handbook, relate to: SCAs, SSs and CSSBs.</p>
System safety requirement	<p>The Armed Forces' demands on DesignA includes both operational obligations and technical requirements in terms of the technical system and its system safety features. See <i>section 5.3</i>.</p>
Systematic errors	<p>An error or fault that always occurs at some point when the system has been used which produces the same outcome every time. The reason may be, for example, a logical flaw in the software that provides the same outcome (fault/error) on execution, or the physical failure of a "batch" of components that provide the same outcome when the components are exposed/used (batch = a group of components made in a sequence/with the same machine settings, the same input/raw materials etc).</p>
Systems Office (MaK)	<p>Owner Representatives' representative (ÄFR) for all the standard vehicles, COTS products and some other materiel.</p>

Concept	Explanation
<p>Technical adaptation</p>	<p>To temporarily change/adapt a technical system's design and/or function in response to a disturbance, altered threat or changed environment. This also applies when there is a change in operational, tactical or combat technical requirements.</p> <p>Applicable only in direct combat situations (war, crisis, international response).</p> <p>The change is temporary and the materiel needed will be restored to its original state.</p>
<p>Technical design responsibility</p>	<p>Technical design responsibility means determining the technical system's established technical structure and the integration of technical systems/subsystems, equipment and components that are subject to a certain allowable configuration (including maintenance solutions) and to ensure that it meets legal requirements, set objectives and other requirements regarding performance, functionality, information and system safety during the service life of the technical system.</p> <p>Technical design responsibilities, including technical systems management, are normally held by DesignA for all levels of technical systems which DesignA has delivered to the Armed Forces. Technical design responsibility is linked to the type of technical system.</p> <p>Industry and suppliers are responsible for a product and may have a technical design responsibility in relation to the procurement organization, but it is always the procuring organization that is responsible for the technical design.</p>
<p>Technical Office (TeK)</p>	<p>ÄFR for the specific materiel.</p>
<p>Technical order (TO)</p>	<p>Materiel publications issued by the Swedish Defence Materiel Administration (FMV) on behalf of the Armed Forces. Through a TO, the operation, maintenance, care and modification of supplies are governed.</p>
<p>Technical standard order (TSO)</p>	<p>A TSO is issued by the Aviation Authority and is a standard that specifies the minimum attributes of an article.</p>

Concept	Explanation
Technical system	<p>A system is defined by ISO/IEC 15 288 as: “An assembly of interacting elements organized to achieve one or more stated purposes.”</p> <p>The system in H SystSäkE always refers to the technical system.</p> <p>The technical system refers to a system that has been created through the integration of technical systems, elements from these and/or other products.</p> <p>Ammunition is always a separate technical system.</p>
Testing	<p>Testing relates to technical verification and validation. Testing, along with a review of the qualification activities, is designed to verify technical demands and expectations, for example to demonstrate that a gun barrel can resist the pressure created by the ammunition intended to be used. Testing may produce far greater risks than regulated safety-approved materiel is allowed to contain (see <i>Trial/Experiment</i>).</p>
The owner representative's representative (ÄFR)	<p>For most technical systems there is an ÄFR, designated in the form of a TeK and a Materiel Office. These act as the owner of the materiel during operation, maintenance and decommissioning. ÄFR is responsible for representing ÄF regarding operational and financial control, monitoring and analysis, configuration mode, modifications and TO operations, as well as technical support and technical development.</p> <p>FMV is the ÄFR for supplies which are mainly procured for and used in FMV's testing operations. For supplies that cannot be clearly assigned to one of the above activities the ÄFR must be regulated for each order.</p>
Tolerable level of risk (T)	A certain level of risk.
Trial/Experiment	An experiment includes: the tactical value of materiel/a system/product, which intends to show that a technical system is tactically useful and can be handled in the manner intended (see <i>Testing</i> .)
Trigger	In order for the damaging effects of a source of a risk to be activated a certain mechanism is required. In some cases a trigger may be required to achieve a hazardous event <i>Contributing causes</i> )
Validation	Ways of showing that the requirements are correct, namely that the system will function properly in its operational environment if the requirements are fulfilled.

## Definitions

Concept	Explanation
Verification	Confirmation through the drafting and examination of objective evidence that specified requirements have been fulfilled.



## Acronyms/Abbreviations

This is a complete list of acronyms and abbreviations that can be found in H SystSäke.

Acronym/abbreviation	Explanation
ADR	European Agreement Concerning the International Carriage of Dangerous Goods by Road Accord Européen Relatif au Transport International des Marchandises Dangereuses par Route
AE	Architect and Engineering Firm
ALARP	As Low As Reasonably Practicable (relates to a certain type of accident risk)
AML	The Work Environment Act
AOP	Allied Ordnance Publication, NATO
AV	The Swedish Working Environment Authority
BOA	Decision Regarding Use
BT	Limited tolerable risk level
BVKF	The Armed Forces' instruction on measures against fire and explosion hazards, water pollution and chemical health effects from flammable goods etc.
CAA	Civil Aviation Authority, Great Britain
CDRL	Contract Data Requirement List
CE	EC mark of conformity (Communauté Européenne)
CFR	Code of Federal Regulations
CI	Critical Item
CIL	Critical Item List
CIP	Permanent International Commission for Firearms Testing - commonly abbreviated as C.I.P. or CIP (Le Commission Internationale Permanente pour l'Epreuve des Armes à Feu Portatives)
CM	Configuration Management
COSHH	Control of Substances and Hazardous to Health
COTS	Commercial off the Shelf
CSP	Certified Safety Professional
CSSB	Central Safety Compliance Decision

Acronym/abbreviation	Explanation
DAL	Development Assurance Level
Def-Stan	Defence Standard (British standard)
DesignA	Organization responsible for design (including FömedC, FMLOG, FMV, FortV, PPP partner)
DF	Defence Forces
DGA	The French Military Aviation Authority (Délégation Générale pour l'Armement)
DID	Data Item Description, instructions that specify the scope and nature of reports
DLA	Defense Logistics Agency
DoD	Department of Defense (USA)
DOD-STD	Department of Defense Standard
DoDI	DOD Instruction
DOT	Department of Transportation
EASA	The European Air Safety Agency
ECP	Engineering Change Proposal
ECPSSR	Engineering Change Proposal System Safety Report
EHA	Environmental Hazard
EHC	Explosive Hazard Classification and Characteristics Data
EOD	Explosive Ordnance Disposal
ESOH	Environmental, Safety and Occupational Health
ET	Non-tolerable risk level
ETA	Event Tree Analysis
EU	European Union
FAA	Federal Aviation Authority
FC	Functional Centre
FHA	Functional Hazard Analysis
FLYGI	Military Flight Safety Inspectorate
FM	The Swedish Armed Forces
FM ArbO	The Armed Forces' regulations with work procedures for the Armed Forces (FFS 2009:2 with changes FFS 2009:3)

Acronym/abbreviation	Explanation
FMEA	Fault Modes and Effects Analysis
FMECA	Fault Modes Effects and Criticality Analysis
FMLOG	Part of Swedish Defence
FMUK	Armed Forces' Commission of Inquiry
FMV	Swedish Defence Materiel Administration
FOI	The Swedish Defence Research Agency
FORTV	The National Fortifications Administration
FRA	The Swedish National Defence Radio Establishment
FRACAS	Failure Reporting, Analysis and Corrective Action
FSD	Defence Standard (in Sweden)
FSI	Armed Forces' Flight Safety Inspector
FTA	Fault Tree Analysis
FömedC	National Defence Medical Centre
G	Generally applicable
GC	Generally applicable for design change
GEIA	Standard institute
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GOTS	Governmental off the Shelf
HAZOP	Hazard and Operability Study
H FordonSäk	Handbook on Vehicle Safety
HHA	Health Hazard Assessment
HHAR	Health Hazard Assessment Report
HKV	Headquarters
HMI	Human Machine Interface
H Mål	Handbook for the Armed Forces' development of goals for units, supplies and facilities for the war organization's needs
HRI	Hazard Risk Index
HTM	Half-time Modification
HTRR	Hazard Tracking and Risk Resolution
H VAS-E	Weapon and Ammunition Safety Manual

## Acronyms/Abbreviations

Acronym/abbreviation	Explanation
IAEA	International Atomic Energy Agency
ICChemE	Institution of Chemical Engineers
IEC	International Electrotechnical Commission
IEDs	Improvised Explosive Devices
IFTTEX	The Armed Forces' instruction for storage and transportation of ammunition and other explosives
ILS	Integrated Logistic Support
IMSC	Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms
IRS	Interface Requirements Specifications
ISO	International Organization for Standardization
ISSPP	Integrated System Safety Program Plan
JSP	Joint Service Publication
KB	Customer order
LKA	Low-sensitivity ammunition
MA	Managing activity
MaK	Materiel Office
MB	Environmental Code
MCS	Minimal Cut Set
MFI	Navy Vessel Inspection
MIFOR	Military Vehicle Register
MIL-STD	American Military Standard
MOTS	Military off the Shelf
MPD	Materiel Product Declaration
MRAR	Mishap Risk Assessment Report
MS	Materiel System
MSA	Materiel Systems Manager in the Armed Forces HQ
MSB	The Swedish Civil Contingencies Agency
MSI	Materiel System Certificate
MTC	Materiel Type Certificate
N/A	Not Applicable
NATO	North Atlantic Treaty Organization

Acronym/abbreviation	Explanation
NDI	Non-developmental Item
O&SHA	Operating and Support Hazard Analysis
OHHA	Operating and Health Hazard Analysis
OPR	Office of Primary Responsibility
OPS	PPP Private-Public Partnership
OSHA	Occupational Safety and Health Administration
PAL	Product Liability Act
PE	Professional Engineer
PESHE	Programmatic environment, safety, and occupational health evaluation
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PHST	Package Storage and Handling Requirements
PL	Project Manager
PM	Program Manager
PPP	PPP, Private-Public Partnership
PRL	Product Manager
PTEMU	Preliminary Technical–Financial–Objectives for Training Materiel
PTK	Sea Trials Command
PTR	Program Trouble Reports
PTTEM	Preliminary Tactical–Technical–Economic Objectives
RADS	Risk Assessment at Disposal of System
REACH	Registration, Evaluation, Authorization and restriction of Chemicals
REMO	Renovation – modification
RENO	Renovation
RFP	Request for Proposal
RML	Rules for Military Aviation
RML V-5B	Rules for military aviation, Subdivision B – Materiel System Certificate and military type certificate
RML V-5G	Rules for military aviation, Subdivision G – Authorized production organizations

## Acronyms/Abbreviations

Acronym/abbreviation	Explanation
RML V-5J	Rules for military aviation, Subdivision J – Authorized design organizations – level 2
RML V-5JA	Rules for military aviation, Subdivision J – Authorized design organizations – level 3
RML-V-5D	Rules for military aviation, Subdivision D
RML-V-5N	Rules for military aviation, Subdivision N
RMM	Rules for Military Ground Operations
RMS	Rules for naval operations
S	Selectively applicable
SAR	Safety Assessment Report
SCA	Safety Compliance Assessment
SCCSC	Safety Critical Computer Software Components
SCF	Safety Critical Functions
SCG	Storage Compatibility Group
SCN	Specification Change Notices
SDB	Safety data sheet
SDR	System Design Review
SEK	Swedish krona
SEMP	Safety and Environmental Programme Plan
SFS	Swedish Statue Book
SHA	System Hazard Analysis
SHRI	Software Hazard Risk Index
SI	Safety Instructions
SIL	Safety Integrity Level
SJÖI	Military Maritime Safety Inspectorate
SOW	Statement of Work
SPR	Software Problem Reports
SR	Safety Review
SRCA	Safety Requirements/Criteria Analysis
SRR	System Requirements Review
SS	Safety Statement
SS	Swedish standard

Acronym/abbreviation	Explanation
SS-EN	Swedish Standard European Norm
SSE	System Safety Evaluation
SSHA	Sub System Hazard Analysis
SSI	Safety Significant Item
SSMP	System Safety Management Plan
SSP	System Safety Program
SSPP	System Safety Program Plan
SSPPR	System Safety Program Progress Report
SSPR	System Safety Program Review/Audits
SSPS	System Safety Progress Summary
SSR	Software Specification Review
SSS	System/Segment Specification
SSWG	System Safety Working Group, sometimes called SSWG-1 or SSWG-2
SV	Safety Verification
SäkI	The Armed Forces' safety instruction for weapons and ammunition etc
SäkI G	The Armed Forces' safety instruction for weapons and ammunition etc., – common part
SÄKINSP	The Armed Forces' Security Inspectorate
T	Tolerable risk level
TA	Technical directive
TC	Service Branch Centre
TeK	Technical Office
TEMU	Technical Financial Objectives for Training Materiel
TjF	Staff Regulations for FMV
TO	Technical Order
TO UF	Technical Order Maintenance Plans
TOEM	Tactical–Organizational–Financial Objectives
Tso	Technical standard order
TSR	Test and Safety Regulations)
TTEM	Tactical–Technical–Financial Objectives

## Acronyms/Abbreviations

Acronym/abbreviation	Explanation
UAV	Unmanned Aerial Vehicle
UhF	Handbook maintenance service during peacetime
UK	United Kingdom
UN	United Nations
US	United States
UTEMU	Draft Technical–Financial–Objective for Training Materiel
UTTEM	Draft Tactical–Technical–Financial Objectives
V&V	Verification and Validation
WBS	Work Breakdown Structure
VD	Managing Director
WEEE	Waste Electrical and Electronic Equipment
VFM	Operational System for the Armed Forces
WSESRB	Weapon System Explosive Safety Review Board
VVFS	National Road Administration’s code of statutes
ÄF	Owner Representative
ÄFR	Owner Representative’s Representative
ÖB	Supreme Commander



## References

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

Ref no	Title
1	ADR, Myndigheten för samhällsskydd och beredskaps föreskrifter om transport av farligt gods på väg och i terräng; MSBFS 2009:2. (MSB (Agency for Civil Contingencies): regulations on the transport of dangerous goods by road and terrain, MSBFS 2009:2. The letter “S” after ADR denotes that the regulations contain the Swedish version of Annex A and Annex B to the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), supplemented by provisions that only apply to national shipments in Sweden.)
2	Arbetsmiljölöag, SFS 1977:1160 (The Work Environment Act).
3	Waste which is made up of or contains electrical or electronic equipment, 2002/96/EC, WEEE.
4	Certification Considerations for Highly Integrated or Complex Aircraft Systems, SAE ARP4754.
5	Defence Standard 00–56, issue 4, part 2, 1 June 2007.
6	Design Assurance Guidance for Airborne Electronics Hardware, RTCA/DO-254.
7	Design of Munitions for Disposal, Ordnance Board Proceeding, P115.
8	DI-SAFT-80101B, Data Item Description, System Safety Hazard Analysis Report (SSHA).
9	DI-SAFT-80102B, Data Item Description, Safety Assessment Report (SAR).
10	DI-SAFT-80103A, Data Item Description, Engineering Change Proposal System Safety Report (ECPSSR).
11	DI-SAFT-80104A, Data Item Description, Waiver or Deviation System Safety Report (WDSSR).
12	DI-SAFT-80106A, Data Item Description, Health Hazard Assessment Report (HHAR).
13	European Parliament and Council Regulation EC No. 1907/2006 (REACH).

## References

Ref no	Title
14	FMV Handbok HMI, 14 910:753/2009 (FMV's Handbook HMI).
15	FMV Återvinningsmanual, 32822/2008 version 2.0 (FMV's Recycling Manual).
16	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508.
17	Förordning (2007:936) om folkrättslig granskning av vapenprojekt. (Regulation on the international legal review of weapons projects).
18	Armed Forces' Handbook for Software in Safety-Critical Applications, M7762-000621 H ProgSäk E, 2005.
19	Försvarsmaktens instruktion för förvaring och transport av ammunition och övriga explosiva varor, IFTEX. (Armed Forces instructions for the storage and transportation of ammunition and other explosives.)
20	Försvarsmaktens instruktion för åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor mm, BVKE. (Armed Forces' instruction on measures to counteract fire and explosion hazards, water pollution and chemical health effects from inflammable goods etc.)
21	Handbok Fordonssäkerhet 2000 års utgåva, M7762-000511, H FordonSäk. (FMV's Handbook on Vehicle Safety 2000 edition).
22	Handbok för Försvarsmaktens förnödenhetsavveckling, M7751-704081, H Förnavv. (Handbook for the Armed Forces' supplies decommissioning.)
23	Handbok för Försvarsmaktens målsättningsarbete (H Mål), 2006. (Handbook for the Armed Forces' development of goals for units, supplies and facilities for the war organization's needs.)
24	Weapons and Ammunition Safety Manual 2000, M7762-000212, H VAS-E.
25	Handbok Miljö för Försvarsmakten, M7740-784501, H Miljö. (Environmental Guide for the Armed Forces.)
26	ITAA Standard, Standard Best Practices for System Safety Program Development and Execution, GEIA-STD-0010, October 2008.
27	Kemikalieinspektionen Prioriteringsguiden (PRIO), <a href="http://www.kemi.se">www.kemi.se</a> (Chemicals Inspectorate Priority Guide.)
28	Ledningssystem för kvalitet - Krav, SS-EN ISO 9001:2008. (Quality management systems – Requirements.)
29	Military Airworthiness Regulations, JSP523.
30	Miljöbalken, SFS 1998:808. (Environmental Code.)

Ref no	Title
31	Miljöledningssystem - Krav och vägledning, SS-EN ISO 14001:2004. (Environmental management systems – Requirements and guidelines.)
32	MOD Sustainable Development and Environmental Manual, JSP418.
33	Ordnance, Munitions and Explosives Safety Manual, JSP520.
34	Procedures for Land Systems Equipment Safety Assurance, JSP454.
35	Produktansvarslagen, SFS 1992:18. (Product Liability Act.)
36	Safety Assessment Procedure Guidelines and Methods, SAE ARP 4761.
37	SEES Handbok Miljöårlighetsteknik. (SEES Handbook on Environmental Technology.)
38	Ship Safety Management, JSP430.
39	Software Consideration in Airborne Systems and Equipment Certification, RTCA DO-178B, 1992.
40	Svensk Standard, SS 2222. (Swedish Standard.)
41	Säkerhetsinstruktion för vapen och ammunition med mera, Gemensam del, SäKI G. (Safety instructions for weapons and ammunition etc., Common part, SäKI G.)
42	UK Def-Stan 00-56 issue 3.
43	US WSESRB Hazard Analysis Guide list.

## List of Figures

Figure 1:1	System Safety Activities .....	12
Figure 3:1	System Safety Activities – Connection .....	26
Figure 5:1	System Safety Program (SSP) for the Armed Forces .....	47
Figure 5:2	System Safety Program (SSP) for DesignA .....	47
Figure 5:3	System Safety Evaluation (SSE).....	50
Figure 5:4	System Safety Requirements in TTEM .....	52
Figure 5:5	Determining Requirements for the Request for Proposal (RFP)..	58
Figure 5:6	System Safety Program Plan (SSPP) .....	61
Figure 5:7	Integration/Management of Subcontractors (IMSC) .....	63
Figure 5:8	System Safety Program Reviews/Audits (SSPR).....	65
Figure 5:9	System Safety Working Group (SSWG) .....	68
Figure 5:10	Hazard Tracking and Risk Resolution (HTRR).....	70
Figure 5:11	System Safety Progress Summary (SSPS) .....	72
Figure 5:12	Safety Critical Functions (SCF).....	78
Figure 5:13	Preliminary Hazard List (PHL).....	80
Figure 5:14	Preliminary Hazard Analysis (PHA) .....	82
Figure 5:15	Safety Requirements/Criteria Analysis (SRCA) .....	84
Figure 5:16	Subsystem Hazard Analysis (SSHA) .....	86
Figure 5:17	System Hazard Analysis (SHA).....	89
Figure 5:18	Operating and Support Hazard Analysis (O&SHA) .....	92
Figure 5:19	Health Hazard Assessment (HHA) .....	95
Figure 5:20	Environment-Related Activities .....	99
Figure 5:21	Risk Analysis of External Environment (EHA).....	100
Figure 5:22	Functional Hazard Assessment (FHA) .....	104
Figure 5:23	Safety Assessment Report (SAR).....	109
Figure 5:24	Safety Review (SR) .....	111
Figure 5:25	Safety Verification (SV) .....	113
Figure 5:26	Safety Instructions (SI).....	115
Figure 5:27	Safety Compliance Assessment (SCA).....	119
Figure 5:28	Failure Reporting, Analysis and Corrective Action System (FRACAS) .....	123
Figure 5:29	Safety Statement (SS).....	130
Figure 5:30	Training Safety Regulations (TSR) .....	134
Figure 5:31	Central Safety Compliance Decision (CSSB).....	136
Figure 5:32	Risk Assessment at the Disposal of System (RADS).....	141
Figure 8:1	Safety Analysis .....	153
Figure 8:2	Linking of Activity to the Method.....	154
Figure 8:3	Fault Tree Symbols.....	155
Figure 8:4	The amount of & conditions.....	157
Figure 8:5	Fault Tree with Different Amounts of & Conditions.....	157
Figure 8:6	Calculations of Fault Tree Probabilities.....	158
Figure 8:7	The Stress-Strain Interference Surface.....	159
Figure 8:8	Example of Solution with Boolean Algebra .....	160
Figure 8:9	Example of Fault Tree Analysis .....	160
Figure 8:10	Example of Fault Modes and Effects Analysis .....	163
Figure 8:11	Examples of Basis for Fault Modes and Effects Analysis .....	164
Figure 8:12	Example of Event Tree Analysis .....	165

## List of Tables

Table 2:1	Requirements List .....	15
Table 2:2	Requirements List .....	17
Table 2:3	Requirements List .....	19
Table 2:4	Requirements List .....	19
Table 3:1	Requirements List .....	21
Table 3:2	Applications .....	29
Table 4:1	Activities .....	43
Table 5:1	Valuation Matrix .....	49
Table 8:1	Guide Words Table .....	167
Table 8:2	Example of HAZOP .....	168



*Project manager*

Arne Börtemark, FMV

*Subject experts*

Arne Börtemark, FMV (Part 1 och 2)

Ragnar Ekholm, FMV (Part 1 och 2)

Pär-Anders Wallentin, Saab Dynamics AB (Part 2)

Lars Lange, FMV (Part 2)

*Illustrations and cover*

Leif Sundberg, Sörman Information AB

Mats Lundgren, Sörman Information AB

*Original text*

Mats Lundgren, Sörman Information AB

*Digital edition*

Mats Lundgren, Sörman Information AB

*Cover photographs*

Katsuhiko Tokunaga, SAAB

Peter Nilsson, Kockums

Sörman Information AB

<b>1</b>	<b>Requirements</b>	
1.1	Basics.....	11
1.2	Requirements Numbering.....	12
1.3	Significance of Requirement Level .....	13
<b>2</b>	<b>Materiel Requirements</b>	
2.1	Design .....	15
2.2	Manufacturing.....	17
2.3	Maintenance .....	19
2.4	Decommissioning .....	19
<b>3</b>	<b>System Safety Activities</b>	
3.1	Requirements for System Safety Activities .....	21
3.2	Selection of Activities (Tailoring).....	23
<b>4</b>	<b>H SystSäke and MIL-STD-882C</b>	
4.1	General Interpretation and Guidance for MIL-STD-882C .....	39
4.2	General Description of the Activities in H SystSäk E .....	41
4.3	Overview of all System Safety Activities .....	43
<b>5</b>	<b>Description of Activities</b>	
5.1	System Safety Program (SSP) – Task 101 .....	45
5.2	System Safety Evaluation (SSE) – S10 .....	48
5.3	System Safety Requirements in TTEM – S11 .....	51
5.4	Determining Requirements for Tender Enquiry (RFP) – S12.....	53
5.5	System Safety Program Plan (SSPP) – Task 102 .....	60
5.6	Integration/Management of Subcontractors (IMSC) – Task 103 .....	62
5.7	System Safety Program Reviews/Audits (SSPR) – Task 104 .....	64
5.8	System Safety Working Group (SSWG) – Task 105 .....	66
5.9	Hazard Tracking and Risk Resolution (HTRR) – Task 106 .....	69
5.10	System Safety Progress Summary (SSPS) – Task 107 .....	71
5.11	Safety Critical Functions (SCF) – S13 .....	73
5.12	Preliminary Hazard List (PHL) – Task 201.....	79
5.13	Preliminary Hazard Analysis (PHA) – Task 202 .....	81
5.14	Safety Requirements/Criteria Analysis (SRCA) – Task 203 .....	83
5.15	Subsystem Hazard Analysis (SSHA) – Task 204 .....	85
5.16	System Hazard Analysis (SHA) – Task 205 .....	87
5.17	Operating and Support Hazard Analysis (O&SHA) – Task 206 .....	90
5.18	Health Hazard Assessment (HHA) – Task 207 .....	93
5.19	Risk Analysis for External Environment (EHA) – S21 .....	96
5.20	Functional Hazard Assessment (FHA) – S22.....	101
5.21	Safety Assessment Report (SAR) – Task 301 .....	107
5.22	Test and Evaluation Safety – Task 302 .....	109
5.23	Safety Review (SR) – Task 303 .....	110
5.24	Safety Verification (SV) – Task 401 .....	112
5.25	Safety instructions (SI) – S41 .....	114
5.26	Safety Compliance Assessment – Task 402 .....	116
5.27	Safety Compliance Assessment (SCA) – S42 .....	116
5.28	Failure Reporting, Analysis and Corrective Action System (FRACAS) – S43 .....	120
5.29	Explosive Hazard Classification and Characteristics – Task 403 .....	124
5.30	Explosive Ordnance Disposal Source Data – Task 404.....	124
5.31	Safety Statement (SS) – S51.....	124
5.32	Training Safety Regulations (TSR).....	131
5.33	Central Safety Compliance Decision (CSSB) – S53.....	135
5.34	Risk Assessment prior to Disposal of System (RADS).....	137



6	Software Safety	
6.1	General .....	143
6.2	Software Features.....	143
6.3	Safety Requirements for Software .....	146
6.4	Verification of Software .....	148
7	Checklist for Materiel Requirements and Activities	
8	System Safety Analysis	
8.1	Principles for System Safety Analyses .....	153
8.2	Fault Tree Analysis (FTA) .....	155
8.3	Fault Modes and Effects Analysis (FMEA).....	161
8.4	Event Tree Analysis (ETA) .....	164
8.5	Hazard and Operability (HAZOP) Study.....	166
	Appendix 1 Examples of Decision Documents.....	169
	Definitions .....	187
	Acronyms/Abbreviations .....	201
	References .....	209