Försvarsmaktens handbok
Systemsäkerhet 2011
Del 2 – Metoder

H SystSäk

Försvarsmakten 2010-06-08 14 910:60224
Högkvarteret

Försvarsmaktens handbok Systemsäkerhet 2011 (H SystSäk 2011)
M7739-352022 H SystSäk 2011 del 1 och M7739-352023 del 2 fastställs för tillämpning från och med 2011-01-01.

Från samma tidpunkt upphävs H SystSäk 1996-års utgåva, M7740-784851 fastställd med HKV 1996-09-27 14 910:72214.

Beslut i detta ärende har tagits av överste Anders Emanuelson. I den slutliga beredningen har deltagit kmd Mikael Wendel, övlt Per-Axel Schön, luftvärdighetsinspektör Carl Stålberg och öing Ragnar Ekholm, FMV varav den sistnämnde varit föredragande.

Anders Emanuelson

Ragnar Ekholm

Boken är publicerad i samarbete med **Sörman Information AB**
Sakavdelning: Försvarsmaktens Säkerhetsinspektion och FMV
Redaktör: Mats Lundgren
M7739-352023 H SYSTSÄK 2011 DEL 2

Central lagerhållning: Försvarets bok- och blankettförråd
Tryck: Fälth & Hässler, Värnamo, 2011

Innehåll

1 Kravställning
- 1.1 Grunder ... 11
- 1.2 Kravnumrering ... 12
- 1.3 Innebörd av kravnivå ... 13

2 Materielkrav
- 2.1 Konstruktion ... 15
- 2.2 Tillverkning ... 17
- 2.3 Underhåll ... 18
- 2.4 Avveckling ... 18

3 Systemsäkerhetsaktiviteter
- 3.1 Krav på aktiviteter för systemsäkerhetsverksamheten ... 19
- 3.2 Val av aktiviteter (Tailoring) ... 21
  - Urval av aktiviteter ... 21
  - Samband mellan aktiviteter ... 23
  - Val av ledningsrelaterad systemsäkerhetsverksamhet ... 25
  - Val av kravhanteringsaktiviteter ... 25
  - Val av analysmetoder ... 25
  - Val av aktiviteter vid studieuppdrag ... 28
  - Val av aktiviteter vid utvecklingsuppdrag ... 28
  - Val av aktiviteter vid anskaffning av COTS ... 32
  - Val av aktiviteter vid RENO/REMO/HTM ... 32
  - Val av aktiviteter vid ändringsåtgärd ... 33
  - Val av aktiviteter inför avveckling ... 33
  - Val av aktiviteter för framtagning av alternativa reparationsmetoder ... 34
  - Val av aktiviteter för tillfällig reparation och krigsskadereparation ... 34
  - Val av aktiviteter för kommunikationssystem ... 35
  - Val av aktiviteter för expertsystem ... 35
  - Val av aktiviteter för utbildningsmateriel ... 35

4 H SystSäk och MIL-STD-882C
- 4.1 Allmän tolkning och vägledning till MIL-STD-882C ... 37
- 4.2 Generell beskrivning av aktiviteter i H SystSäk ... 39
- 4.3 Översikt över samtliga systemsäkerhetsaktiviteter ... 41

5 Beskrivning av aktiviteter
- 5.1 System Safety Program (SSP) – Task 101 ... 43
  - Syfte ... 43
  - Avvikelser ... 43
  - Jämförbara aktiviteter/dokument ... 44
  - Ytterligare information ... 44
  - Indata ... 44
  - Utdata ... 44

5.2 Systemsäkerhetsvärdering (SSE) – S10 46
Syfte 46
Aktivitetsbeskrivning 46
Indata 47
Utdata 48
5.3 Systemsäkerhetskrav i TTEM (TTEM) – S11 49
Syfte 49
Aktivitetsbeskrivning 49
Indata 49
Utdata 50
5.4 Kravställning vid anbudsförfrågan (RFP) – S12 51
Syfte 51
Aktivitetsbeskrivning 51
Indata 55
Utdata 56
ALARP 56
5.5 System Safety Program Plan (SSPP) – Task 102 58
Syfte 58
Avvikelser 58
Jämförbara aktiviteter/dokument 58
Ytterligare information 58
Indata 59
Utdata 59
5.6 Integration/Management of Subcontractors (IMSC) – Task 103 60
Syfte 60
Avvikelser 60
Jämförbara aktiviteter/dokument 60
Ytterligare information 60
Indata 61
Utdata 61
5.7 System Safety Program Reviews/Audits (SSPR) – Task 104 62
Syfte 62
Avvikelser 62
Jämförbara aktiviteter/dokument 62
Ytterligare information 62
Indata 63
Utdata 63
5.8 System Safety Working Group (SSWG) – Task 105 64
Syfte 64
Avvikelser 64
Jämförbara aktiviteter/dokument 64
Ytterligare information 65
Indata 65
Utdata 65

5.9 Hazard Tracking and Risk Resolution (HTRR) – Task 106 66
Syfte 66
Avvikelser 66
Jämförbara aktiviteter/dokument 66
Ytterligare information 66
Indata 67
Utdata 67
5.10 System Safety Progress Summary (SSPS) – Task 107 68
Syfte 68
Avvikelser 68
Jämförbara aktiviteter/dokument 68
Ytterligare information 68
Indata 68
Utdata 69
5.11 Safety Critical Functions (SCF) – S13 70
Syfte 70
Aktivitetsbeskrivning 70
Indata 75
Utdata 75
5.12 Preliminary Hazard List (PHL) – Task 201 76
Syfte 76
Avvikelser 76
Jämförbara aktiviteter/dokument 76
Ytterligare information 76
Indata 77
Utdata 77
5.13 Preliminary Hazard Analysis (PHA) – Task 202 78
Syfte 78
Avvikelser 78
Jämförbara aktiviteter/dokument 78
Ytterligare information 78
Indata 79
Utdata 79
5.14 Safety Requirements/Criteria Analysis (SRCA) – Task 203 80
Syfte 80
Avvikelser 80
Jämförbara aktiviteter/dokument 80
Ytterligare information 80
Indata 81
Utdata 81
5.15 Subsystem Hazard Analysis (SSHA) – Task 204 82
Syfte 82
Avvikelser 82
Jämförbara aktiviteter/dokument 82
Ytterligare information 83
Indata 83
Utdata 83

5.16 System Hazard Analysis (SHA) – Task 205 84
Syfte 84
Avvikelser 84
Jämförbara aktiviteter/dokument 84
Ytterligare information 85
Indata 85
Utdata 86
5.17 Operating and Support Hazard Analysis (O&SHA) – Task 206 87
Syfte 87
Avvikelser 87
Jämförbara aktiviteter/dokument 87
Ytterligare information 88
Indata 88
Utdata 88
5.18 Health Hazard Assessment (HHA) – Task 207 90
Syfte 90
Avvikelser 90
Jämförbara aktiviteter/dokument 90
Ytterligare information 91
Indata 92
Utdata 92
5.19 Riskanalys för yttre miljö (EHA) – S21 93
Syfte 93
Aktivitetsbeskrivning 93
Indata 96
Utdata 97
5.20 Functional Hazard Assessment (FHA) – S22 98
Syfte 98
Aktivitetsbeskrivning 98
Indata 100
Utdata 100
FHA för civila flygburna system 101
Syfte 101
Aktivitetsbeskrivning 102
Indata 103
Utdata 103
5.21 Safety Assessment Report (SAR) – Task 301 104
Syfte 104
Avvikelser 104
Jämförbara aktiviteter/dokument 104
Ytterligare information 104
Indata 105
Utdata 105
5.22 Test and Evaluation Safety – Task 302 106

5.23 Safety Review (SR) – Task 303 106
Syfte 106
Avvikelser 106
Jämförbara aktiviteter/dokument 106
Ytterligare information 107
Indata 107
Utdata 107
5.24 Safety Verification (SV) – Task 401 109
Syfte 109
Avvikelser 109
Jämförbara aktiviteter/dokument 109
Ytterligare information 109
Indata 110
Utdata 110
5.25 Säkerhetsföreskrifter (SI) – S41 111
Syfte 111
Aktivitetsbeskrivning 111
Indata 112
Utdata 113
5.26 Safety Compliance Assessment – Task 402 114
5.27 Systemsäkerhetsutlåtande (SCA) – S42 114
Syfte 114
Aktivitetsbeskrivning 114
Indata 116
Utdata 117
5.28 Felrapporteringssystem (FRACAS) – S43 118
Syfte 118
Aktivitetsbeskrivning 118
Resulterande rapport 120
Indata 120
Utdata 121
5.29 Explosive Hazard Classification and Characteristics – Task 403 122
5.30 Explosive Ordnance Disposal Source Data – Task 404 122
5.31 Systemsäkerhetsgodkännande (SS) – S51 122
Syfte 122
Aktivitetsbeskrivning 122
Indata 127
Utdata 127
5.32 Användarmanualer och utbildning (TSR) – S52 129
Syfte 129
Aktivitetsbeskrivning 129
Indata 131
Utdata 132

5.33 Centralt systemsäkerhetsbeslut (CSSB) – S53 133
Syfte 133
Aktivitetsbeskrivning 133
Indata 134
Utdata 134
5.34 Riskanalys inför avveckling av system (RADS) – S61 135
Syfte 135
Aktivitetsbeskrivning 135
Indata 138
Utdata 138

6 Programvarusäkerhet
6.1 Allmänt 139
6.2 Programvaruegenskaper 139
6.3 Säkerhetskrav på programvara 142
6.4 Verifiering av programvara 144

7 Checklista för materielkrav och aktiviteter

8 Systemsäkerhetsanalyser
8.1 Principer för systemsäkerhetsanalyser 149
8.2 Felträdsanalys (FTA) 151
Kvalitativa felträdsanalyser 152
Kvantitativa felträdsanalyser 153
8.3 Feleffektanalys (FMEA) 156
Kvalitativa feleffektanalyser 157
Kvantitativa feleffektanalyser 158
8.4 Händelseträd (ETA) 160
8.5 Hazard and Operability (HAZOP) Study 162

Bilaga 1 Exempel på beslutsdokument 165

Definitioner 183

Akronymer/förkortningar 197

Referenser 205

FÖRORD

H SystSäk del 2 – Metoder innehåller alla de systemsäkerhetsaktiviteter som anses lämpliga att använda för samtliga faser under ett tekniskt systems livslängd. Flertalet av dessa aktiviteter är hämtade från MIL-STD-882C och för dessa ges här tolkningar och förtydliganden om när och hur de ska tillämpas. Fullständig beskrivning återfinns endast i MIL-STD-882C som återfinns på H SystSäk CDR. Dessutom finns unika svenska materielkrav och aktiviteter vilka är fullständigt beskrivna här i del 2 av H SystSäk. För att underlätta samläsning av dokumenten, används standardens engelska namn på respektive aktivitet, såväl i löpande text som i rubrik och innehållsförteckning.

Detta förord avser specifikt del 2. För H SystSäk generellt hänvisas till förord i del 1.

1 KRAVSTÄLLNING

1.1 GRUNDER

Kapitel 2 och *3* anger de materielkrav och systemsäkerhetsaktiviteter som är generella för de flesta tekniska system. Det är nödvändigt att göra ett klokt urval av dessa aktiviteter för att uppnå acceptabel säkerhet. Med begreppet system avses i handboken tekniskt system och begreppet risk avser olycksrisk.

Kraven är uppdelade på systemens olika faser under livslängden.

Ett tekniskt system medför under sina användningsskeden olika olycksrisker vid förvaring, transport, hantering, användning, underhåll och avveckling. Vid konstruktion och tillverkning begränsas riskerna genom att såväl konstruktiva åtgärder (analyser, omkonstruktion med mera) som produktionsåtgärder (till exempel kvalitetsstyrning) vidtas.

Vissa olycksrisker kan dock kvarstå efter tillverkning. Sådana kan vara ljudtryck, termisk strålning eller vibration. Dessa olycksrisker ska begränsas genom varningar, säkerhetsföreskrifter samt utbildning i ett korrekt handhavande.

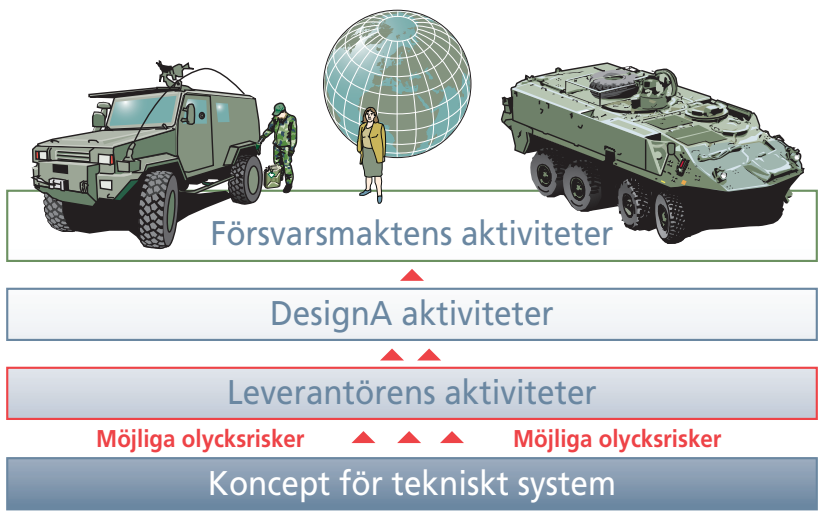


Bild 1:1 Systemsäkerhetsaktiviteter

Systemsäkerhetsaktiviteterna kan i princip beskrivas enligt *bild 1:1* där alla inblandade parter såsom utvecklare, tillverkare, konstruktionsansvarig och brukare tar sitt ansvar och bidrar till att förhindra att olyckor sker.

Syftet med dessa aktiviteter är att innehålla de krav på systemsäkerhet som ställts för det tekniska systemet avseende person, egendom och yttre miljö.

1.2 Kravnumrering

Kraven är antigen obligatoriska (utmärks med fet stil och på mörkblå bakgrund) eller valbara (ljusblå bakgrund).

För de valbara kraven sker urval först då de anses tillämpliga för ett visst tekniskt system, varvid de anges i kravspecifikation/systemsäkerhetsplan/kvalitetsplan (ISO 9001, *[29]*)/miljöplan (ISO 14001, *[32]*) eller motsvarande.

H SystSäk omfattar bland annat ett antal krav avseende dels verksamhetens utförande, dels materielens egenskaper. Kraven är avsedda att användas vid anskaffning i förekommande anbudsinfordran och avtal.

Begynnelsesiffra för visst krav anger varifrån kravet härstammar, till exempel 0 anger att kravet kommer från H SystSäk del 2.

De två följande siffror anger kapitlet, till exempel 31 som anger att kravet kommer från kapitel 3 avsnitt 1. Slutligen har varje krav ett löpnummer som gäller inom respektive avsnitt. Till exempel anger 0.31.001 det första kravet i kapitel 3 avsnitt 1 i H SystSäk del 2.

Begynnelsesiffrorna är fördelade enligt följande:

0 H SystSäk del 2

1 H VAS (FMV Handbok Vapen- och Ammunitionssäkerhet) *[24]*

2 H SystSäk del 1

3 H FordonSäk (FMV Handbok Fordonssäkerhet) *[21]*

6 H ProgSäk (FM handbok för programvara i säkerhetskritiska tillämpningar) *[18]*

1.3 Innebörd av kravnivå

Försvarsmakten är som beställare även kravställare. När DesignA har mottagit beställning från Försvarsmakten, är också DesignA beställare och kravställare. Handbokens krav fördelar sig på obligatoriska och valbara krav. Det är för kravställaren som begreppen obligatorisk/valbar utgör anvisning.

De obligatoriska kraven är av avgörande betydelse för systemsäkerheten. För att uppfylla lagar, förordningar och föreskrifter med inriktning mot systemsäkerhetsverksamheten, behöver alla obligatoriska krav uppfyllas. Om ett obligatoriskt krav inte kan uppfyllas av exempelvis taktiska skäl eller kostnadsskäl, kan en avvikelse tolereras om det kan visas att acceptabel säkerhet ändå kan erhållas. Beslutsunderlaget för denna avvikelse ska dokumenteras.

En styrning av vilka systemsäkerhetsaktiviteter som ska genomföras för det tekniska systemet av aktuella aktörer, sker vid Försvarsmaktens kravställning i exempelvis TTEM, se *5.3*. Detta sker även då DesignA ställer krav i anbudsförfrågan (RFP, se *5.4*).

I leverantörens systemsäkerhetsplan framgår vilka aktiviteter som denne avser utföra samt till vilken ambitionsnivå.

Observera att omfattningen av aktiviteterna alltid ska anpassas efter det tekniska systemets komplexitet och ställda krav avseende systemsäkerhet.

För ytterligare vägledning, se *avsnitt 3.2 Val av aktiviteter (Tailoring)*.

2 Materielkrav

2.1 Konstruktion

Innan utveckling eller anskaffning av ett tekniskt system sker, ska systemsäkerhetskraven definieras och dokumenteras i relevant kravdokumentation. Nedan anges systemsäkerhetskrav som är tillämpliga för flertalet tekniska system.

Kravnumrering framgår av *avsnitt 1.2*.

Tabell 2:1 Kravlista

0.21.001	Tekniskt system bör konstrueras så att säkerhetsföreskrifter inte behöver tillämpas för transport, förvaring, handhavande, underhåll, användning och avveckling. Villkor för när en konstruktionslösning får ersättas av skyddsanordningar, varningar och utbildning ska regleras, lämpligen i System Safety Program Plan (SSPP se *5.5*). Se även Säkerhetsföreskrifter (SI se *5.25*) och Användarmanualer och utbildning (TSR se *5.32*).
0.21.002	Tekniskt system skall konstrueras så att enkelfel inte resulterar i vådahändelse, om inte sannolikheten för vådahändelsen kan visas vara acceptabelt låg och/eller konsekvenserna av vådahändelsen kan accepteras. Kravställd risk framgår av kravspecifikation eller motsvarande.
0.21.003	Tekniskt system bör konstrueras så att fel på två eller flera komponenter på grund av en gemensam orsak, ”common cause”, inte resulterar i vådahändelse, om inte konsekvensen av vådahändelsen kan accepteras.
0.21.004	En konstruktion bör tåla att utsättas för de abnorma miljöer som kan uppkomma till exempel vid olyckor och fientlig attack, så att den aktuella konstruktionen inte ökar det tekniska systemets totala sårbarhet.

0.21.005	En egenskap eller detalj som direkt påverkar säkerheten (exempelvis enkelfel) hos det tekniska systemet klassificeras som en säkerhetskritisk egenskap/detalj. Varje sådan egenskap/detalj skall listas i produktdokumentationen. Avvikelse från denna egenskap eller fel på denna detalj klassificeras som kritiskt fel, se Safety Critical Functions (SCF se *5.11*).
0.21.006	En egenskap eller detalj som påverkar säkerheten (exemepelvis dubbelfel eller fel av högre ordning) hos det tekniska systemet klassificeras som en säkerhetsrelaterad egenskap/detalj. Varje sådan egenskap/detalj skall listas i produktdokumentationen. Avvikelse från denna egenskap klassificeras som allvarligt fel, se Safety Critical Functions (SCF se *5.11*).
0.21.007	Grundkrav enligt anvisningar i *kapitel 6* skall vara uppfyllda av säkerhetskritisk programvarudel. (Dessa grundkrav utgörs av kvalitetskrav för all typ av programvara, såväl kritisk som icke-kritisk)
0.21.008	Det urval av säkerhetskrav enligt anvisningar i *kapitel 6*, vilket är relevant för den säkerhetskritiska programvaran i aktuellt tekniskt system, skall vara uppfyllda. Urvalet skall avse det tekniska systemets samtliga programvarudelar och avspegla dess högsta kritikalitet, såvida inte oberoende mellan delar av olika kritikalitet kan påvisas. Ett urval per kritikalitetspartition är tillåten för programvarudelar, där oberoende mellan delar av olika kritikalitet kan påvisas.
0.21.009	För att underlätta försäljning av tekniskt system vid avveckling bör dispenser från lagar samt specifikt militära lösningar undvikas. För komponenter och delsystem som ingår i det tekniska systemet bör även CE-märkning övervägas (CE-märkning kan dock inte ske av specifikt militära tekniska system i dess helhet).
0.21.010	Sammanfogningsmetoder som hindrar demontering bör ej användas.
0.21.011	Identifiering av plastmaterial bör ske genom märkning i produkten/komponenten.

2.2 Tillverkning

Varje brist eller fel som kan orsaka vådahändelse eller farligt tillstånd, ska identifieras under utvecklingen. Brist som kan uppkomma vid tillverkningen, och som kan bidra till vådahändelse eller farligt tillstånd, ska undvikas genom noggrann produktionsstyrning och kvalitetssäkring.

Tabell 2:2 Kravlista

0.22.001	Produktionsstyrning eller allkontroll av alla egenskaper som kan leda till kritiskt fel skall ske, se Safety Critical Functions (SCF se *5.11*). Kommentar: Det finns vissa egenskaper som inte kan kontrolleras fullständigt beroende på att förstörande provning måste tilllämpas. I dessa fall måste produktionsstyrningen vara sådan att sannolikheten för att fel uppstår är liten.
0.22.002	Produktionsstyrning eller allkontroll av alla egenskaper som kan leda till allvarligt fel bör ske, se Safety Critical Functions (SCF se *5.11*).
0.22.003	Vid kontroll av egenskaper som kan leda till kritiskt fel skall utrustning användas som upptäcker felaktiga delar och förhindrar att de passerar kontrollstationen, se Safety Critical Functions (SCF se *5.11*). Kommentar: Automatisk testutrustning kan användas för denna typ av kontroll. I de fall automatisk testutrustning inte är tillgänglig måste kontrollen upprepas för att ge avsedd effekt.
0.22004	Kontroll av egenskaper som kan leda till allvarligt fel bör utföras på samma sätt som vid kritiska fel, se Safety Critical Functions (SCF se *5.11*). Kommentar: Kontrollen kan ske genom att använda automatisk testutrustning.

0.22.005	Kontrollutrustning skall inspekteras och kalibreras med regelbundna intervall. Kommentar: Jämför kalibreringssystem enligt riktlinjer i SS-EN ISO 9001 *[29]*.
0.22.006	Tillverkningsprocessen skall effektivt avskilja felaktiga enheter. Kommentar: Felaktiga enheter ska avskiljas från korrekta enheter. Där så är möjligt ska de felaktiga enheterna märkas. Jämför riktlinjer i SS-EN ISO 9001 *[29]*.

2.3 Underhåll

Vådahändelse eller farligt tillstånd som kan uppkomma vid brist på underhåll eller vid felaktigt genomfört underhåll ska undvikas genom en noggrann ILS-verksamhet.

Tabell 2:3 Kravlista

0.23.001	Ett tekniskt systems säkerhet bör inte vara beroende av speciella underhållsåtgärder. Kommentar: Om underhållsåtgärder behövs för att bibehålla säkerheten bör dessa ingå i den planerade ordinarie underhållsverksamheten.
0.23.002	Säkerheten hos ett tekniskt system skall inte försämras efter genomfört underhåll.

2.4 Avveckling

Vådahändelse eller farligt tillstånd som kan uppkomma vid avveckling ska undvikas genom bland annat riskanalys av avvecklingsverksamheten.

Tabell 2:4 Kravlista

0.24.001	Krav på återanvändnings- och återvinningsgrad bör definieras.

3 Systemsäkerhetsaktiviteter

3.1 Krav på aktiviteter för systemsäkerhetsverksamheten

Detta avsnitt anger de aktivitetskrav som är relevanta för de flesta tekniska system. Aktiviteterna tillämpas för de tekniska systemens faser enligt *avsnitt 3.2*.

Kravnumrering framgår av *avsnitt 1.2*.

Tabell 3:1 Kravlista

0.31.001	System Safety Program (SSP) – Task 101 skall genomföras enligt *avsnitt 5.1*.
0.31.002	Systemsäkerhetsvärdering (SSE) – S10 bör genomföras enligt *avsnitt 5.2*.
0.31.003	Systemsäkerhetskrav i TTEM (Taktisk Teknisk Ekonomisk Målsättning) – S11 skall upprättas enligt *avsnitt 5.3*.
0.31.004	Systemsäkerhetskrav vid anbudsförfrågan (RFP) – S12 skall upprättas enligt *avsnitt 5.4*.
0.31.005	System Safety Program Plan (SSPP) – Task 102 skall upprättas enligt *avsnitt 5.5*.
0.31.006	Integration/Management of Sub Contractors (IMSC) – Task 103 sker enligt *avsnitt 5.6*.
0.31.007	System Safety Program Reviews/Audits (SSPR) – Task 104 sker enligt *avsnitt 5.7*.
0.31.008	System Safety Working Group (SSWG) Support – Task 105 inrättas enligt *avsnitt 5.8*.
0.31.009	Hazard Tracking and Resolution (HTRR) – Task 106 genomförs enligt *avsnitt 5.9*.
0.31.010	System Safety Progress Summary (SSPS) – Task 107 upprättas enligt *avsnitt 5.10*.

0.31.011	Safety Critical Functions (SCF) – S13 skall genomföras enligt *avsnitt 5.11*.
0.31.012	Preliminary Hazard List (PHL) – Task 201 genomförs enligt *avsnitt 5.12*.
0.31.013	Preliminary Hazard Analysis (PHA) – Task 202 genomförs enligt *avsnitt 5.13*.
0.31.014	Safety Requirement Criteria Analysis (SRCA) – Task 203 genomförs enligt *avsnitt 5.14*.
0.31.015	Subsystem Hazard Analysis (SSHA) – Task 204 genomförs enligt *avsnitt 5.15*.
0.31.016	System Hazard Analysis (SHA) – Task 205 genomförs enligt *avsnitt 5.16*.
0.31.017	Operating and Support Hazard Analysis (O&SHA) – Task 206 genomförs enligt *avsnitt 5.17*.
0.31.018	Health Hazard Assessment (HHA) – Task 207 genomförs enligt *avsnitt 5.18*.
0.31.019	Riskanalys för yttre miljön (EHA) – S21 genomförs enligt *avsnitt 5.19*.
0.31.020	Functional Hazard Assessment (FHA) – S22 genomförs enligt *avsnitt 5.20*.
0.31.021	Safety Assessment Report (SAR) – Task 301 upprättas enligt *avsnitt 5.21*.
0.31.022	Safety Review (SR) – Task 303 genomförs enligt *avsnitt 5.23*.
0.31.023	Safety Verification (SV) – Task 401 genomförs enligt *avsnitt 5.24*
0.31.024	Säkerhetsföreskrifter (SI) – S41 utformas enligt *avsnitt 5.24*.
0.31.025	Systemsäkerhetsutlåtande (SCA) – S42 skall upprättas enligt *avsnitt 5.27*.

0.31.026	Felrapporteringssystem (FRACAS) – S43 upprättas enligt *avsnitt 5.28*.
0.31.027	Systemsäkerhetsgodkännande (SS) – S51 skall upprättas enligt *avsnitt 5.31*.
0.31.028	Användarmanualer och utbildning (TSR) – S52 bör upprättas enligt *avsnitt 5.32*.
0.31.029	Centralt systemsäkerhetsbeslut (CSSB) – S53 skall upprättas enligt *avsnitt 5.33*.
0.31.030	Riskanalys inför avveckling av system (RADS) – S61 skall genomföras enligt *avsnitt 5.34*.

3.2 Val av aktiviteter (Tailoring)

Detta avsnitt innehåller anvisningar för urval och tillämpning av de olika aktiviteter som utgör bas för systemsäkerhetsverksamheten.

3.2.1 Urval av aktiviteter

Den systemsäkerhetsverksamhet som ska bedrivas för ett tekniskt system ska anpassas efter vilka riskkällor/farliga tillstånd det tekniska systemet anses innehålla och vilka potentiella olycksrisker som med anledning av detta bedöms kunna finnas. I princip ska samtliga aktiviteter enligt *bild 3:1* alltid ingå i systemsäkerhetsverksamheten även om i vissa fall någon aktivitet kan uteslutas efter noggrann avvägning. I det fall där myndighetskrav i form av lagstiftning och/eller normer och standarder finns, för visst tekniskt system, så kan detta utgöra grund för att vissa aktiviteter väljs bort.

Tabell 3:2 är ett exempel på val av aktiviteter. I *tabell 4:1* ges vägledning om i vilken fas de olika aktiviteterna lämpligen tillämpas. Beställare specificerar de aktiviteter som leverantören ska genomföra samt vilka systemsäkerhetsdokument som ska levereras, och när detta ska ske.

Omfattning av respektive beställd aktivitet får anpassas av leverantör (för att undvika onödiga kostnader).

Observera att myndighetskrav ibland kan vara mer omfattande än handbokens krav, se *H SystSäk del 1*.

Urval av aktiviteter och deras omfattning måste ofta diskuteras mellan Försvarsmakten och DesignA samt aktuell leverantör. När en aktivitet har valts och omfattning har överenskommits, dokumenteras detta i systemsäkerhetsplanen (SSPP *5.5*).

Om det tekniska systemet innehåller vapen och ammunition eller annan produkt med explosiv vara, tillkommer flera aktiviteter vilka framgår av H VAS *[24]*. Motsvarande gäller för fordon respektive fartyg och ubåtar, se även *H SystSäk del 1*.

För anskaffning av COTS som avses att användas fristående från annat tekniskt system, och i enlighet med leverantörs handhavandebeskrivning, räcker det oftast med att i anbudsskedet begära in aktuella säkerhetsdatablad och den riskanalys som ligger till grund för eventuell CE-märkning. Vid anskaffning av färdigt tekniskt system ska SAR *5.21* och SCA *5.27* infordras i anbudsskedet. Vid utveckling av tekniskt system, med eller utan integrerad COTS, ska H SystSäk tilllämpas i sin helhet, se även *H SystSäk Del 1, avsnitt 5.6*.

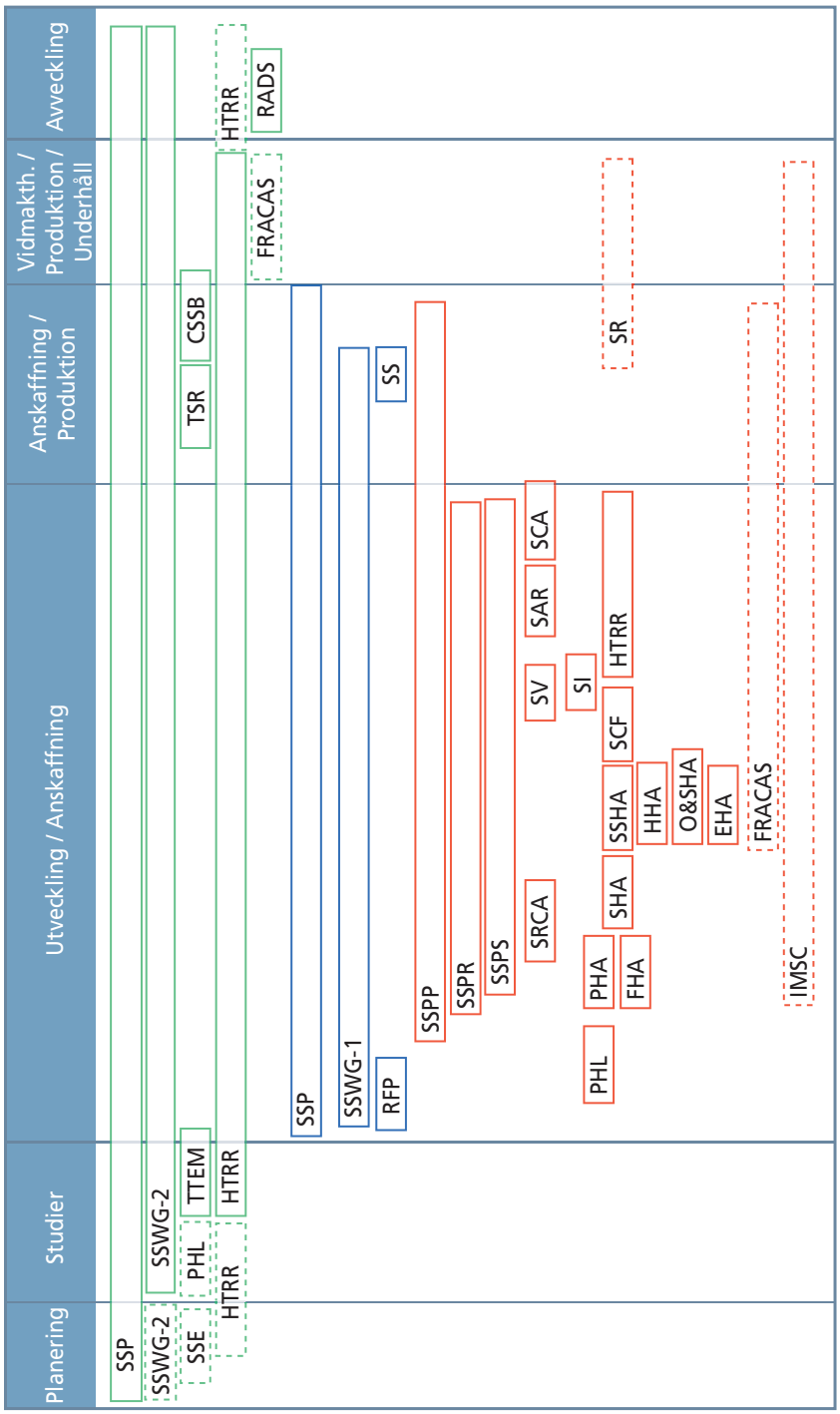
Systemsäkerhetsverksamheten kan indelas i verksamhetsledning, kravhantering respektive riskhantering. Respektive del anpassas individuellt med avseende på potentiella leverantörers erfarenhet av systemsäkerhetsverksamhet samt utifrån det tekniska systemets nyttjandegrad av känd teknik samt användningssätt. För varje aktivitet ska krav på dokumentation från aktiviteten specificeras.

3.2.2 Samband mellan aktiviteter

Ur graferna nedan framgår sambanden mellan de olika aktiviteterna samt av vem och när de kan utföras. Valet av aktiviteter och val av ambition måste anpassas till det tekniska systemets potentiella risknivå.

Innebörd av utformning av ram runt viss aktivitet.

Streckad	Selektivt tillämpbart/Selectively Applicable
Heldragen	Generellt tillämpbart/Generally Applicable



Försvarsmaktens aktiviteter markerade med grönt, DesignA:s aktiviteter markerade med blått och leverantörs aktiviteter markerade med rött.

Bild 3:1 Systemsäkerhetsaktiviteternas samband

3.2.3 Val av ledningsrelaterad systemsäkerhetsverksamhet

Systemsäkerhetsverksamheten regleras av styrdokumenten SSMP och SSPP samt genom verksamheten IMSC. Dess efterlevnad styrs och kontrolleras av SSWG-1, SSWG-2 och SSPR. Leverantörs fortlöpande rapportering sker via SSPS.

Efter genomförd verksamhet deklareras verksamhetsåtaganden och kravuppfyllelse i SCA, SS och CSSB. Som underlag för SCA finns en SAR.

För tekniskt system som kan förknippas med olycksrisker ska alltid minst aktiviteterna SSPP, SCA, SS och CSSB genomföras.

3.2.4 Val av kravhanteringsaktiviteter

Kravhanteringen sker genom TTEM, RFP, SRCA samt SV. De operativa kraven i TTEM omvandlas och kompletteras i RFP till funktionsinriktade krav. RFP utgör en del av anbudsinfordran som besvaras av leverantör. Leverantör genomför SRCA för att komplettera, detaljera och bryta ner kraven till konstruktionskrav.

Den del som utgörs av krav på verksamheter (aktiviteter) genereras genom SSP och dokumenteras i SSMP samt framkommer vid RFP. Dessa kompletteras och anges i SSPP.

För tekniskt system som kan förknippas med olycksrisker ska alltid minst aktiviteterna TTEM, RFP, SRCA och SV genomföras.

3.2.5 Val av analysmetoder

Analysverksamheten syftar till att identifiera och analysera orsakerna till potentiella olycksrisker. Detta sker genom PHL, PHA och FHA. Efter identifieringen analyseras olycksriskernas grundorsaker. Detta kan ske med den fortsatta analysverksamheten i form av SHA, SSHA, O&SHA, HHA och EHA. Inför avveckling sker motsvarande analys med RADS. När orsakerna har identifieras ska dessa elimineras eller reduceras så att ställda krav

på olycksrisk för det tekniska systemet innehålls. Alla identifierade olycksrisker samt vidtagna riskreducerande åtgärder dokumenteras enligt HTRR.

Ur analyserna identifieras hur kritiska det tekniska systemets olika egenskaper och delar är. Denna identifiering med efterföljande åtgärder styrs av SCF. Vid ändringar i konstruktion eller avvikelser för de kritiska egenskaperna/delarna ska SR tillämpas.

Om de riskreducerande åtgärderna består av varningar eller andra säkerhetsföreskrifter gäller SI och TSR.

Om fel inträffar vid användning eller provning används FRACAS. Om dessa fel är säkerhetsrelaterade ska detta dokumenteras enligt HTRR för vidare åtgärd enligt SSWG.

Vilka av ovanstående aktiviteter som ska tillämpas måste anpassas för aktuellt tekniskt system. I *tabell 3:2* nedan ges vägledning till hur detta kan ske för olika tillämpningar och anskaffningsuppdrag. Den vänstra kolumnen (Tillämpning) beskriver verksamheter eller situationer och kryssen anger vilken analysteknik/aktivitet som är mest tillämpbar.

Tabell 3:2 Tillämpningar

Analysteknik/aktivitet Verksamhet/situation	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
Färdiga tekniska system												×
Konceptstudier	×											
Systembeskrivning		×	×	×	×	×	×	×	×	×		
Systemanalyser		×	×	×	×	×	×	×	×	×		
Riskkällor/Farliga tillstånd		×										
Vådahändelser			×									
Funktionsanalyser				×								
Kravanalyser					×							
Delsystemanalyser						×						
Interaktioner							×					
Operativa faser								×				
Systemhändelser			×			×	×					
Användningsinstruktioner								×			×	
Identifiering av farliga ämnen		×	×						×	×		
Identifiering av risker med farliga ämnen						×	×	×	×	×	×	
Identifiering av vådahändelse för användare			×					×	×		×	
Effekt av vådahändelse			×			×	×	×	×	×	×	
Riskvärdering	×		×	×		×	×	×	×	×	×	
Effekt av planerad åtgärd		×	×	×	×	×	×	×	×	×		
Effekt av införd åtgärd			×			×	×	×	×	×		
Felutfall i liknande tekniska system		×	×			×	×	×	×	×		
Ändringar			×			×	×	×	×	×	×	
Manualer								×			×	
Avveckling											×	

3.2.6 Val av aktiviteter vid studieuppdrag

Ett studieuppdrag sker oftast i ett tidigt skede av materielanskaffningen. Studieuppdraget kan omfatta såväl studier av olika tekniker som av prototyper/demonstratorer av tekniska system. Ett studieuppdrag innefattar inte framtagning av serielika tekniska system. Studieuppdraget initieras normal av Försvarsmakten. De demonstratorer/prototyper som tas fram i samband med studieverksamheten kommer endast i ringa omfattning att användas av militära förband samt normalt aldrig i operativ användning.

I planerings- och studieskedet jämförs olika koncept för att under utveckling/anskaffningsskedet omsättas till ett tekniskt system. Under dessa tidiga skeden är detaljeringsnivån på koncepten varierande. De aktiviteter som är bäst tillämpliga för att ur systemsäkerhetssynpunkt värdera olika koncept är systemsäkerhetsvärdering (SSE) och Preliminary Hazard List (PHL). De övriga aktiviteterna som bör bedrivas är initiering av en systemsäkerhetsverksamhet, System Safety Program (SSP), samt bildandet av en arbetsgrupp för styrning och övervakning av det totala systemsäkerhetsarbetet, System Safety Working Group (SSWG).

3.2.7 Val av aktiviteter vid utvecklingsuppdrag

Varje utvecklingsuppdrag är unikt varför en anpassning alltid måste ske så att rätt aktiviteter utförs till rätt nivå. Detta medför att relevanta aktiviteter måste väljas och att nivån på varje aktivitet måste anpassas så att den täcker behovet för att erhålla ett acceptabelt säkert tekniskt system.

I de fall som en studie föregår utvecklingen ska även aktiviteter enligt *avsnitt 3.2.6* genomföras. Därutöver formuleras de övergripande systemsäkerhetskraven i Taktisk Teknisk Ekonomisk Målsättning (TTEM) och ett riskuppföljningssystem (HTRR) etableras för det tekniska systemet. Detta riskuppföljningssystem ska användas under hela det tekniska systemets livslängd.

En arbetsgrupp för systemsäkerhet (SSWG-1) etableras hos DesignA. Denna grupp ska återföra all information till Försvarsmaktens systemsäkerhetsgrupp (SSWG-2). Praktiskt kan detta ske genom att man tillfälligt slår samman dessa grupper till en grupp.

DesignA formulerar systemsäkerhetskraven från TTEM till krav för anbudsförfrågan (RFP).

I samband med att leverantör svarar på anbudsförfrågan genomförs ofta en analys i form av en Preliminary Hazard List (PHL) för att identifiera potentiella olycksrisker med det offererade tekniska systemet. I den kravspecifikation som leverantör upprättar ska krav infogas för att kontrollera att dessa olycksrisker identifieras. Vidare ska tillkommande systemsäkerhetskrav, såsom lagbundna krav, identifieras (SRCA) och infogas i kravspecifikationen. Det urval av aktiviteter som leverantör ska genomföra under utvecklingsuppdraget ska beskrivas i systemsäkerhetsplanen (SSPP). En systemsäkerhetsplan (SSPP) ska ingå i anbudsunderlaget från leverantör.

Efter erhållen beställning etablerar vald leverantör oftast en intern arbetsgrupp för systemsäkerhetsfrågor eller medverkar i DesignA arbetsgrupp för systemsäkerhetsfrågor (SSWG-1). I dessa grupper görs bedömningar och avväganden avseende säkerhetsrelaterade frågor i projektet. Frågor av större betydelse kan tas upp i Försvarsmaktens systemsäkerhetsgrupp (SSWG-2). Leverantör rapporterar verksamhetens framskridande i avtalade säkerhetsrapporter (SSPS).

Ansvarig leverantör styr sina underleverantörer och samarbetspartner via leverantörsstyrningsverksamheten (IMSC).

Den egentliga riskanalysverksamheten genomförs med inledande analyser (PHL, PHA, FHA) och följs av de djupare analysverksamheterna (SHA, SSHA, HHA, EHA och O&SHA).

Syftet med Preliminary Hazard List (PHL) är att i första hand identifiera alla riskkällor/farliga tillstånd i det tekniska systemet för att ta bort eller byta dessa mot mindre farliga.

En fördjupning av Preliminary Hazard List (PHL) är Preliminary Hazard Analysis (PHA) och Functional Hazard Assessment (FHA) som används för att identifiera potentiella vådahändelser vilka därefter kan analyseras vidare för att identifiera grundorsakerna till dessa vådahändelser. Dessa grundorsaker och farliga tillstånd kontrolleras eller elimineras effektivast genom konstruktionsändringar.

Som ett resultat av riskanalysverksamheten identifieras kritiska egenskaper och kritiska delar i det tekniska systemet (SCF). Dessa kritiska eller systemsäkerhetsrelaterade egenskaper ska identifieras på tillverkningsunderlaget såsom på ritningar och i specifikationer, för att val av lämplig tillverkningsmetod som säkerställer att tillräckligt litet felutfall ska kunna förväntas under tillverkningsskedet.

Alla identifierade vådahändelser och farliga tillstånd med relaterade olyckor samt vidtagna och planerade åtgärder för att hantera tillhörande olycksrisker, ska tas om hand i en riskhanteringsverksamhet (HTRR). Redovisning av riskuppföljningen sker i leverantörsinterna arbetsgrupper eller i DesignA:s systemsäkerhetsgrupp (SSWG-1) för identifiering av lämpliga riskreducerande åtgärder.

Den avtalade systemsäkerhetsverksamheten granskas genom revisioner såsom normala kvalitetsrevisioner eller i specifika systemsäkerhetsrelaterade revisioner (SSPR) i enlighet med beställningen. Resultat från revisionerna meddelas systemsäkerhetsgruppen (SSWG-1).

Om säkerhetsrelaterade fel uppträder vid provning, rapporteras dessa enligt avtalat felrapporteringssystem (FRACAS). Informationen i felrapporteringssystemet tas över av Försvarsmakten från leverantör efter genomförd utveckling och produktion.

Begränsningar i användningen av ett tekniskt system måste ibland införas grundat på:

- reglerande lagstiftning
- riskreducerande åtgärd.

Begränsningar införs genom säkerhetsföreskrifter (SI). Dessa utgör även underlag för leverantörens systemsäkerhetsutlåtande (SCA) samt underlag till Försvarsmaktens olika instruktioner (TRS).

Alla systemsäkerhetskrav från RFP och SRCA ska verifieras. Denna verifiering beskrivs i säkerhetsverifieringen (SV).

Resultaten från riskanalysverksamheten (SHA, SSHA, HHA, EHA och O&SHA) och säkerhetsverifieringen (SV) utgör tillsammans med säkerhetsföreskrifter (SI) underlag för systemsäkerhetsrapporten (SAR).

I systemsäkerhetsrapporten (SAR) samlas all väsentlig systemsäkerhetsrelaterad information om det tekniska systemet. Systemsäkerhetsrapporten utgör grund för leverantörens systemsäkerhetsutlåtande (SCA), där leverantören förklarar att det tekniska systemet är tillräckligt säkert för användning, förutsatt att säkerhetsföreskrifter (SI) efterlevs.

Systemsäkerhetsutlåtandet ligger till grund för DesignA:s systemsäkerhetsgodkännande (SS) samt Försvarsmaktens centrala systemsäkerhetsbeslut (CSSB).

Efter det att det tekniska produktionsunderlaget har färdigställts, rapporteras ändringar enligt ändringstjänsten (SR) för ställningstagande av DesignA.

Ovanstående beskriver kort den totala systemsäkerhetsverksamheten under ett utvecklingsuppdrag. Flera av aktiviteterna kommer att genomföras flera gånger under den iterationsprocess som används vid utvecklingen. För tekniska system med små konsekvenser i händelse av olycka, behöver inte alla aktiviteter enligt ovan genomföras. De aktiviteter som oftast måste genomföras är någon form av tidig riskidentifiering (PHL, PHA, FHA), enklare analys på delsystemsnivå (SSHA) i form av exempelvis en feleffektanalys (FMECA), verifiering av systemsäkerhetskrav (SV) samt ett systemsäkerhetsutlåtande (SCA) som innehåller en sammanfattning av den totala systemsäkerhetsverksamheten. Vidare krävs att DesignA utfärdar systemsäkerhetsgodkännande (SS) samt att Försvarsmakten utfärdar centralt systemsäkerhetsbeslut (CSSB).

3.2.8 Val av aktiviteter vid anskaffning av COTS

Vid anskaffning av kommersiella produkter föreligger ofta svårigheter att få tillräcklig information om tidigare genomförda riskanalyser. Beroende på hur dessa produkter avses användas kan de bli säkerhetskritiska, se även *kapitel 6* avseende programvara som COTS.

För vissa enklare produkter såsom handverktyg, som planeras att användas såsom tillverkaren anger att produkten ska användas, räcker det med att produkten är CE-märkt. Detta ger en säkerhetsnivå som accepteras av det civila samhället. En produkt av denna karaktär fordrar inte något systemsäkerhetsgodkännande (SS) eller centralt systemsäkerhetsbeslut (CSSB) förutsatt att den inte ska integreras i ett militärt tekniskt system.

Om produkten är planerad att användas utanför den tillämpning som CE-märkningen omfattar, måste en formell analysverksamhet, exempelvis PHA, FHA, SHA, SSHA, O&SHA, HHA och EHA, genomföras. Resultatet från analysverksamheten ska rapporteras i en SAR som ligger till grund för ett systemsäkerhetsgodkännande (SS) och centralt systemsäkerhetsbeslut (CSSB). Denna verksamhet ska i dessa fall utföras av DesignA om inte ansvarig leverantör kan genomföra verksamheten.

Då en COTS-produkt integreras i ett tekniskt system, måste denna anses som vilket delsystem som helst i det totala tekniska systemet, och därför ska aktiviteter tillämpas som vid utvecklingsuppdrag enligt *avsnitt 3.2.7*. Se även *H SystSäk Del 1, avsnitt 5.8*.

3.2.9 Val av aktiviteter vid RENO/REMO/HTM

Renovering och modifiering kan vara mycket olika för olika tekniska system. Därför är det svårt att ge en generell anvisning för val av tillämpliga aktiviteter. En säkerhetsbedömning måste alltid ske om huruvida de planerade åtgärderna har någon systemsäkerhetspåverkan eller inte. Denna säkerhetsbedömning bör göras av SSWG-2 som besitter kunskap och erfarenheter om det aktuella tekniska systemet. Vid en mer omfattande renovering/modifiering

ska verksamheter i likhet med de aktiviteter som krävs vid utvecklingsuppdrag enlig *avsnitt 3.2.7* tillämpas. Om mindre modifieringar genomförs måste ändå en systemsäkerhetsanalys göras av eventuell påverkan på övriga delsystem för att utröna om detta kan medföra ytterligare olycksrisker.

3.2.10 Val av aktiviteter vid ändringsåtgärd

Vid behov av ändring eller vid rapporterad avvikelse ska detta ske enligt överenskommet förfarande. Varje förslag till ändring samt varje rapporterad avvikelse ska analyseras och värderas med avseende på systemsäkerhetsaspekter. Metodiken för detta framgår av Safety Review (SR) *5.23*.

3.2.11 Val av aktiviteter inför avveckling

Inför avveckling av ett tekniskt system behöver alla olycksrisker som kan förknippas med den totala avvecklingsprocessen identifieras och om möjligt elimineras. I den mån riskerna inte kan elimineras ska de åtgärdas till en acceptabel nivå enligt Arbetsmiljöverkets föreskrifter. Avvecklingen genomförs oftast av civil personal på civila företag.

En av aktiviteterna för detta är Riskanalys inför avveckling av system (RADS). Avsikten med denna är att systematiskt analysera en definierad avvecklingsprocess med avseende på inneboende olycksrisker. Om det tekniska systemet är relativt modernt, det vill säga att H SystSäk har tillämpats vid utveckling/anskaffning för systemet, finns mycket information om systemets potentiella olycksrisker i samband med planerad avveckling redan identifierat. Denna analys sker då som en del av den ordinarie analysverksamheten. Likaså kan kravställningen i TTEM och RFP ha säkerställt att det tekniska systemet är särskilt konstruerat för att möjliggöra säker och kostnadseffektiv avveckling.

Om det tekniska systemet inte har utvecklats enligt den metodik som anges i H SystSäk måste RADS tillämpas fullt ut. Metodiken i aktiviteten RADS anger att potentiellt farliga material som ingår i det tekniska systemet ska kartläggas samt skyddsåtgärder vidtas

om hälsovådliga eller miljöpåverkande ämnen förekommer. Vidare ska planerad avvecklingsprocess analyseras med avseende på eventuella olycksrisker som är direkt förknippade med det tekniska systemet, avvecklingsmetoden, verktygen och restprodukterna.

3.2.12 Val av aktiviteter för framtagning av alternativa reparationsmetoder

Anvisningar för alternativa reparationsmetoder utvecklas och bereds fortlöpande.

Härvid tas nya metoder fram liksom nya reparationskomponenter (ersättning för originalreservdel). Underlag för framtagning av alternativa reparationsmetoder kan vara inrapporterade reparationer utförda med okonventionella metoder. För beredningsarbetet väljs systemsäkerhetsaktiviteter enligt *avsnitt 3.2.7*. DesignA beslutar fortlöpande om alternativa reparationsmetoder. Beslut kungörs genom TO (Teknisk Order) som följs upp med att TA (Teknisk Anvisning) ges ut.

3.2.13 Val av aktiviteter för tillfällig reparation och krigsskadereparation

Syftet med tillfällig reparation och krigsskadereparation är att tillfälligt, då tid eller resurser för verifierade reparationsmetoder saknas, avhjälpa drift- eller stridsskada på tekniskt system, för att härigenom möjliggöra lösandet av pågående uppgift.

Tillfällig reparation tillämpas normalt endast vid internationell insats och reparationen ska vara acceptabel från systemsäkerhetssynpunkt.

Krigsskadereparation utförs endast under krig eller krigsliknande förhållanden. Reparationens huvudsyfte är att så snabbt som möjligt göra tekniskt system användbart efter stridsskada.

Anvisningar för dessa typer av åtgärder behandlas endast i *H SystSäk Del 1, avsnitt 5.11.3*.

3.2.14 Val av aktiviteter för kommunikationssystem

Då kommunikationssystem används för att styra enheter som vid fel i kommunikation eller i informationsöverföring kan resultera i vådahändelser eller farliga tillstånd, ska kommunikationssystem betraktas som en komponent i det tekniska systemet och behandlas lika med övriga komponenter enligt exempelvis *avsnitt 3.2.7*.

3.2.15 Val av aktiviteter för expertsystem

Då expertsystem används i tekniska system som kan orsaka vådahändelse eller farlig tillstånd, ska expertsystemet betraktas som en komponent i det tekniska systemet och behandlas lika med övriga komponenter enligt exempelvis *avsnitt 3.2.7*. Se även *H SystSäk Del 1, avsnitt 5.10.7*.

3.2.16 Val av aktiviteter för utbildningsmateriel

För en utrustning som avser att simulera funktionerna hos visst vapen/ledningssystem är det väsentligt att säkerställa att den tillräckligt väl efterliknar det verkliga tekniska systemet. Om inte så kan felaktiga och säkerhetspåverkande beteenden övas in. Systemsäkerhetsarbetet vid anskaffning av simulatorer ska därför inriktas på att identifiera sådana skillnader mellan simulator och verkligt system som kan medföra riskframkallande operatörsavvikelser. Vidare ska övriga olycksrisker kartläggas och behandlas enligt *avsnitt 3.2.7*.

Omfattning och djup i systemsäkerhetsarbetet ska anpassas och kan koncentreras på likhet med skarpt vapen/ledningssystem i gränsytan till operatör, likhet i användning, versionshantering och risk för felaktig inlärning. Normalt ska systemsäkerhetsutlåtande/ -godkännande och CSSB omfatta helt tekniskt system, till exempel vapen/ledningssystem i det tekniska systemet inklusive tillhörande simulatorer vid skola eller övningsanläggning. Systemsäkerhetsaktiviteter väljs enligt *avsnitt 3.2.7*.

4 H SystSäk och MIL-STD-882C

4.1 Allmän tolkning och vägledning till MIL-STD-882C

Nedan ges en anvisningar om vilka delar av MIL-STD-882C som är tillämpbara.

FOREWORD: Inte tillämpbart för svenska förhållanden, ersätts av *H SystSäk Del 1, kapitel 1*.

1. SCOPE: Inte tillämpbart för svenska förhållanden, ersätts av *H SystSäk Del 1, kapitel 1*.
2. APPLICABLE DOCUMENTS: Standarden anger uttryckligt att den inte har några referenser. I H SystSäk del 2 är varje aktivitet självförklarande.
3. ACRONYMS AND DEFINITIONS: MIL-STD-882C akronymer återfinns i *Akronymer/förkortningar*. Definitionerna är tillämpbara med följande tillägg och justeringar;

3.2.2	Contractor: ”DOD” motsvaras av Försvarsdepartementet, ”MA” se *3.2.8* nedan.
3.2.4	Hazard: Motsvaras av vådahändelse eller farligt tillstånd.
3.2.6	Hazard severity: Se *H SystSäk Del 1, kapitel 1* och *4*.
3.2.8	Managing activity: Motsvaras av Försvarsmakten (FM) och DesignA som ansvarar för anskaffning av tekniskt system, eller leverantör (underleverantör) som begär aktiviteter av sin underleverantör.
3.2.9	Mishap: Motsvaras av OLYCKA.
3.2.10	Nondevelopmental item; b: ”United States” motsvaras av Sverige.
3.2.21	System safety group/working group: ”MA” se *3.2.8*. Se aktiviteter för SSWG *avsnitt 5.8* samt *H SystSäk Del 1, avsnitt 7.4* och *avsnitt 6.8*.

3.2.24 System safety program: Se aktivitet för SSP, *avsnitt 5.1*.

3.2.25 System safety program plan: Se aktivitet för SSPP, *avsnitt 5.5*.

4. GENERAL REQUIREMENTS: Inte tillämpbart för svenska förhållanden, ersätts av *H SystSäk del 1*.
5. DETAILED REQUIREMENTS: Inte tillämpbart för svenska förhållanden, ersätts av *H SystSäk del 1*.
6. NOTES: Inte tillämpbart för svenska förhållanden, ersätts av *H SystSäk del 1*, *H VAS*, *H FordonSäk*, *RML*, *RMS* med flera.

CONCLUDING MATERIAL: Inte tillämpbart för svenska förhållanden.

TASKS: Denna del är generellt tillämpbar med tillägg av att även de unika svenska aktiviteterna enligt *kapitel 5* ska beaktas. Dessa har separata aktivitetsnummer som inte finns i MIL-STD-882C.

APPENDIX A. GUIDELINES FOR IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS: Inte tillämpbart för svenska förhållanden, ersätts av *avsnitt 3.2*, respektive aktivitetsbeskrivning i *kapitel 5* samt *H SystSäk del 1*. (Del av appendix A kan dock ha använts vid framtagning av YTTERLIGARE INFORMATION för viss aktivitet i handboken.)

APPENDIX B. SYSTEM SAFETY PROGRAM ACTIVITIES RELATED TO THE LIFE CYCLE PHASES: Inte tillämpbart för svenska förhållanden, ersätts av *avsnitt 3.2*, respektive aktivitetsbeskrivning i *kapitel 5* samt *H SystSäk del 1*.

APPENDIX C. SUPPLEMENTARY REQUIREMENTS: Inte tillämpbart för svenska förhållanden, ersätts av *kapitel 2* samt respektive aktivitetsbeskrivning i *kapitel 5*.

APPENDIX D. DATA REQUIREMENTS FOR MIL-STD-882: Inte tillämpbart för svenska förhållanden, ersätts av *H SystSäk del 1* och respektive aktivitetsbeskrivning i *kapitel 5*.

4.2 Generell beskrivning av aktiviteter i H SystSäk

Avsnittet beskriver ett antal systemsäkerhetsaktiviteter. Dessa används i tillämpliga delar och i förekommande fall. *Tabell 4:1* nedan ger en vägledning om när aktiviteterna är tillämpbara.

Vid planering av åtgärd för tekniskt system framtas System Safety Management Plan (SSMP), (enligt SSP, se *avsnitt 5.1*) och System Safety Program Plan (SSPP, se *avsnitt 5.5*). För aktuellt dokument väljs de aktiviteter som bedöms relevanta.

De unikt svenska aktiviteterna identifieras av bokstaven ”S” följt av ett tvåsiffrigt tal.

Kursivt markerad aktivitet finns i MIL-STD-882C men används inte i H SystSäk.

Aktiviteterna FHA (Functional Hazard Assessment) *5.20* och SCF (Safety Critical Functions) *5.11* återfinns inte i MIL-STD-882C och inte heller i tidigare utgåva av H SystSäk, men är allmänt tillämpade säkerhetsaktiviteter som ingår i såväl civila som militära standarder. Därför har dessa tagits med i denna utgåva av H SystSäk.

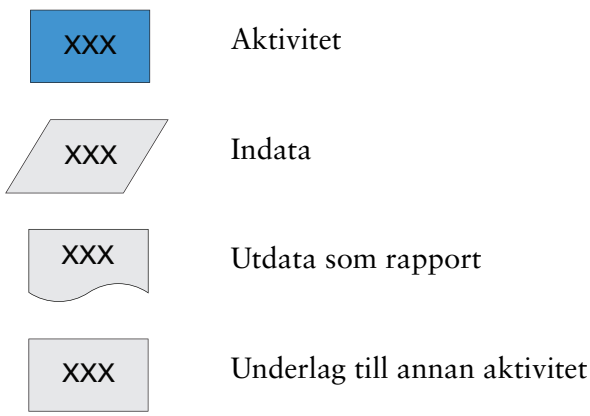
För unikt svenska aktiviteter är uppställningen enligt nedan:

- **SYFTE**, en kort beskrivning av vad aktiviteten syftar till
- **AKTIVITETSBESKRIVNING**, med en beskrivning av hur aktiviteten lämpligen utförs
- **INDATA**, anger vilka indata som behövs för att genomföra aktiviteten
- **UTDATA**, anger vad som genereras vid aktivitetens genomförande såsom resulterande rapport.

För handbokens övriga aktiviteter hänvisas till MIL-STD-882C, med avvikelser som beskrivs under respektive avsnitt nedan. Följande avsnitt finns:

- **SYFTE**, detta avsnitt innehåller en kort allmän beskrivning av aktiviteten
- **AVVIKELSER**, beskriver eventuella avvikelser mot MIL-STD-882C
- **JÄMFÖRBARA AKTIVITETER/DOKUMENT**, referens till jämförbara aktiviteter i andra standarder som kan användas till exempel vid internationellt samarbete
- **YTTERLIGARE INFORMATION**, ger ytterligare vägledning vid genomförandet av aktiviteten, ofta hämtade ur MIL-STD-882C Appendix A
- **INDATA**, anger vilka indata som behövs för att genomföra aktiviteten
- **UTDATA**, anger vad som genereras vid aktivitetens genomförande, till exempel en rapport.

För varje aktivitet finns en bild som ger en översikt av indata och utdata för respektive aktivitet. För varje aktivitet anges



Blått anger aktiviteten.
Grått anger säkerhetsrelaterad aktivitet eller rapport.
Gult anger förutsättning.
Grönt anger information som inte närmare beskrivs i H SystSäk.

4.3 Översikt över samtliga systemsäkerhetsaktiviteter

Tabell 4:1 Aktiviteter

Aktivitet/ Task	Titel/Title	Fas/Phase					
		0	I	II	III	IV	V
101	System Safety Program (SSP)	G	G	G	G	G	G
S10	Systemsäkerhetsvärdering (SSE)	S	S	N/A	N/A	N/A	N/A
S11	Systemsäkerhetskrav i TTEM (TTEM)	N/A	G	G	GC	N/A	N/A
S12	Kravställning vid anbudsförfrågan (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	Riskanalys för yttre miljö (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

Aktivitet/ Task	Titel/Title	Fas/Phase					
		0	I	II	III	IV	V
302	*Test and Evaluation Safety*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
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	Säkerhetsföreskrifter (SI)	N/A	S	G	G	GC	G
S42	Systemsäkerhetsutlåtande (SCA)	N/A	S	G	GC	GC	N/A
S43	Felrapporteringssystem (FRACAS)	S	S	G	G	G	S
403	*Explosive Hazard Classification (EHC) and Characteristics Data*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
404	*Explosive Ordnance Disposal (EOD) Source Data*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
S51	Systemsäkerhetsgodkännande (SS)	N/A	N/A	S	G	S	N/A
S52	Användarmanualer och utbildning (TSR)	N/A	N/A	N/A	G	G	N/A
S53	Centralt systemsäkerhetsbeslut (CSSB)	N/A	N/A	S	G	S	N/A
S61	Riskanalys inför avveckling av system (RADS)	N/A	N/A	N/A	N/A	N/A	G

Förklaringar:

FAS/ PROGRAM PHASE

0	Planering/Concept refinement
I	Studier/Technology development
II	Utveckling/System development and demonstration
III	Anskaffning/Demonstration, production and deployment
IV	Vidmakthållande/Operations and support
V	Avveckling/Disposal

TILLÄMPBARHET/APPLICABILITY CODES

S	Selektivt tillämpbart/Selectively Applicable
G	Generellt tillämpbart/Generally Applicable
GC	Generellt tillämpbart vid konstruktionsändring/ General Applicable to Design Change Only
N/A	Ej tillämpbart/ Not Applicable

5 Beskrivning av aktiviteter

5.1 System Safety Program (SSP) – Task 101

5.1.1 Syfte

Denna aktivitet tillämpas av Försvarsmakten och DesignA vid kravställning och planering. Planerad systemsäkerhetsverksamhet dokumenteras lämpligen i en System Safety Management Plan (SSMP). Begreppet SSMP finns inte i MIL-STD-882C men väl i senare preliminär utgåva av standarden. Därför anses begreppet lämpligt att använda i *H SystSäk*. Såväl Försvarsmakten som DesignA bör reglera respektive systemsäkerhetsverksamhet i en plan. Dokumentet SSMP är denna plan.

SSMP ska ange Försvarsmaktens/DesignA:s systemsäkerhetsverksamhet under det tekniska systemets hela livslängd. Planen ska också ange vilka aktiviteter som är obligatoriska och vad i övrigt som ska krävas av leverantör vid anbudsinfordran.

Leverantör ska beskriva planerad systemsäkerhetsverksamhet i System Safety Program Plan (SSPP) *5.5*.

5.1.2 Avvikelser

101.2.1: Referenser till ”section 4” ersätts med *H SystSäk del 1*.

101.3.1 b: Referenser till ”section 4” ersätts med *H SystSäk del 1*.

5.1.3 Jämförbara aktiviteter/dokument

Säkerhetsverksamheten i Storbritannien benämns även Safety Case. En motsvarande plan är Safety Management Plan. (JSP520 *[34]*, JSP430 *[39]*, JSP533 *[30]* och JSP454 *[35]*).

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 101, System Safety Program. Denna skiljer sig marginellt och kan tillämpas som ett alternativ.

5.1.4 Ytterligare information

Denna aktivitet är obligatorisk för alla tekniska system. Dock måste det tekniska systemets potentiella olycksrisker beaktas när de aktiviteter väljs som ska genomföras, se *avsnitt 3.2.1*.

Det ingår även i aktiviteten att definiera systemsäkerhetskrav, dessa kan komma från *H SystSäk del 1* samt *kapitel 2* och *3* i denna del eller från andra källor.

Felrapporterings- och uppföljningssystem för tillbud och olyckor bör anges/etableras i ett tidigt skede.

5.1.5 Indata

Underlag för systemsäkerhetskrav och aktiviteter, se *H SystSäk del 1* och *kapitel 2* och *3* i denna del.

5.1.6 Utdata

System Safety Management Plan (SSMP) som definierar planerade aktiviteter. Mallar/exempel på SSMP finns i H SystSäk CDR.

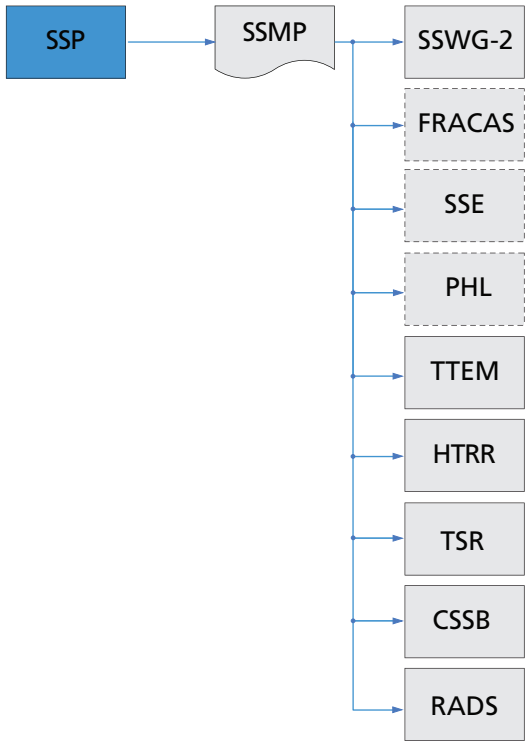


Bild 5:1 System Safety Program (SSP) för Försvarsmakten

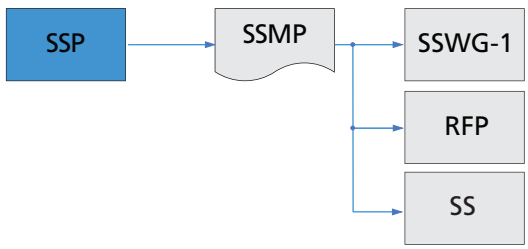


Bild 5:2 System Safety Program (SSP) för DesignA

5.2 Systemsäkerhetsvärdering (SSE) – S10

5.2.1 Syfte

Denna aktivitet tillämpas främst av Försvarsmakten för att ge Försvarsmakten verktyg för att prioritera och rangordna systemalternativ ur ett systemsäkerhetsperspektiv. Genomförande av studier och framtagning av spelkort genomförs enligt *H SystSäk del 1, avsnitt 6.4, Studier*.

5.2.2 Aktivitetsbeskrivning

Systemsäkerhetsvärdering avser att för olika koncept/spelkort identifiera, analysera och värdera möjliga systemsäkerhetsproblem mot generella faktorer, för att ge beslutsunderlag till prioritering av koncept i Försvarsmaktens fortsatta studieverksamhet.

Exempel på verksamheter vid systemsäkerhetsvärdering:

- Förteckna farliga tekniska system, delsystem, produkter, komponenter, kemiska ämnen, situationer med mera. PHL (*5.12*) är ett bra verktyg för att identifiera riskkällor/farliga tillstånd.
- Identifiera möjliga skador på person, egendom och yttre miljö utifrån ovanstående. PHL (*5.12*) kan användas för detta. Prioritera det koncept som innehåller minsta antalet riskkällor/farliga tillstånd med minsta potentiella påverkan på person, egendom och yttre miljö.
- Identifiera generella faktorer att värdera mot, exempelvis:
  - **Okänd teknik;** baseras det tekniska systemets säkerhetspåverkande delar på känd befintlig teknik eller finns det behov av omfattande teknikutveckling?
  - **Säkerhetsåtgärder;** kommer det tekniska systemet att ställa krav på personlig skyddsutrustning för egen personal eller kräva omfattande säkerhetsföreskrifter (såsom stora riskområden) vid användning?

  - **Miljöbelastning;** vilken miljöbelastning kan förväntas på kort respektive lång sikt vid användning samt vid avveckling av materielen? (Miljöpåverkan för normala utsläpp vid all hantering omhändertas oftast i det ordinarie miljöarbetet. I de fall som miljöpåverkan inte beaktas i det arbetet, bör detta ske under systemsäkerhetsverksamhet).
- Analysera och värdera resultatet från systemsäkerhetssynpunkt. Den totala systemsäkerhetsvärderingen (systemsäkerhet, ekonomi, effektivitet, anskaffningstid) ska även beakta systemsäkerhetsaspekterna.
- Utvärdera och dokumentera resultatet.

Tabell 5:1 är exempel på hur värdering kan genomföras, utan viktning av ingående faktorer. De olika koncepten A, B och C bygger på mer eller mindre känd teknik vars användning kan bedömas kräva olika omfattning av säkerhetsåtgärder. Beroende på val av material och framdrivningssätt belastar de olika koncepten yttre miljö i större eller mindre utsträckning. Systemsäkerhetsvärderingen visar att koncept C är det bästa konceptet.

Tabell 5:1 Värderingsmatris

Koncept	Ny okänd teknik	Krav på säkerhetsföreskrifter	Miljöbelastning	Summering och värdering
A	Omfattande (3)	Inga (0)	Liten (1)	Medel (4)
B	Liten (1)	Normala (1)	Stor (3)	Sämst (5)
C	Ingen (0)	Utökade (2)	Liten (1)	Bäst (3)

5.2.3 Indata

En beskrivning av konceptet samt eventuell PHL *5.12*.

5.2.4 Utdata

Den resulterande rapporten bör entydigt ange den systemsäkerhetsmässiga prioriteringen av de olika koncepten. Hänsyn ska inte tas till övriga värderingskriterier såsom effektivitet, anskaffningstid och ekonomi. Samlat övervägande sker utanför här beskriven aktivitet. Rapport från systemsäkerhetsvärdering kan utgöra underlag för TTEM *5.3*. Det finns ingen mall upprättad för rapporten.

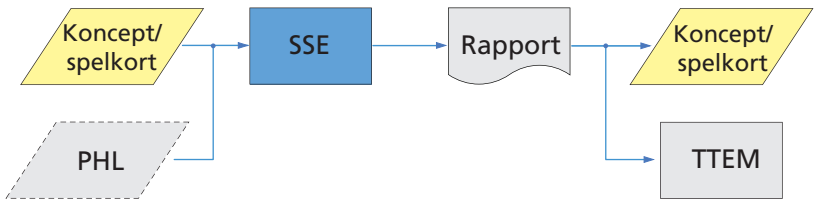


Bild 5:3 Systemsäkerhetsvärdering (SSE)

5.3 Systemsäkerhetskrav i TTEM (TTEM) – S11

5.3.1 Syfte

Denna aktivitet tillämpas främst av Försvarsmakten för att identifiera och fastställa de systemsäkerhetskrav som ska ingå i TTEM. Kraven syftar till att tekniskt system ska bli tillräckligt säkert vid avsedd användning under hela livslängden. Vid framtagning av mål för utbildningsmateriel (med krav enligt TEMU, UTEMU, PTEMU) används handboken i tilllämpliga delar.

5.3.2 Aktivitetsbeskrivning

Krav som Försvarsmakten ställer till DesignA är av två typer:

- verksamhetskrav; krav på viss verksamhet och verksamhetens utförande (skrivs i dokumentet kundbeställning, KB)
- tekniska krav, avseende aktuellt tekniskt system (skrivs i dokumentet TTEM).

Grunder för att identifiera behov av samt att formulera systemsäkerhetskrav som ställs i TTEM respektive i kundbeställning (KB) framgår närmare av *H SystSäk del 1, avsnitt 6.5*. Där redovisas också grund för särskilda överväganden vid kravberedning.

5.3.3 Indata

Spelkort från DesignA och Försvarsmaktens styrande dokument utgör indata till TTEM.

5.3.4 Utdata

TTEM, utgör senare indata till RFP *5.4*.

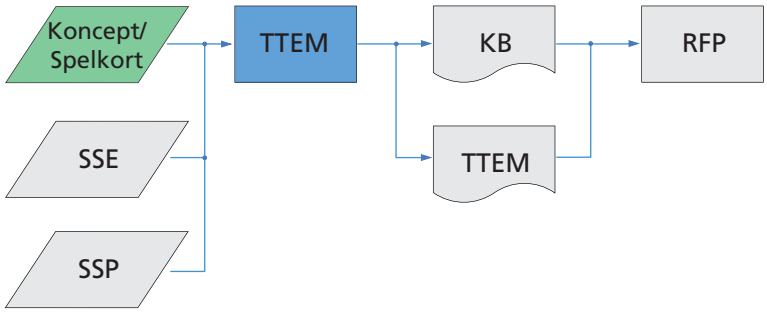


Bild 5:4 Systemsäkerhetskrav i TTEM

Exempel på krav att ta in i KB/TTEM finns i H SystSäk CDR.

5.4 Kravställning vid anbudsförfrågan (RFP) – S12

5.4.1 Syfte

Denna aktivitet tillämpas främst av DesignA för att omvandla de systemsäkerhetskrav som Försvarsmakten har angivit i kundbeställning (KB) respektive i TTEM till krav som kan ingå i anbudsförfrågan (RFP) eller för framtagning av interna krav inom DesignA vid exempelvis granskning av befintlig tekniskt system.

5.4.2 Aktivitetsbeskrivning

DesignA:s systemsäkerhetskrav för tekniskt system anges i RFP. Kraven uppdelas i tekniska krav och krav på verksamhet.

Försvarsmaktens systemsäkerhetskrav uttryckta i KB respektive TTEM rensas från motstridiga krav samt formuleras så att de är mätbara (till exempel med hänvisning till *kapitel 2, Materielkrav*, för generella krav). Tålighetskrav för ammunition i abnorma miljöer formuleras enligt H VAS *[24]* eller tillämplig standard.

Eventuellt behöver Försvarsmaktens systemsäkerhetskrav avseende ett helt tekniskt system brytas ned till teknisk delsystemnivå där olika leverantörer av tekniska delsystem får dela på de överordnade systemsäkerhetskraven.

Förutom de materielbundna säkerhetskraven, som anges i RFP, ska krav ställas på systemsäkerhetsaktiviteter, enligt *kapitel 3, Systemsäkerhetsaktiviteter*. Leverantör kommer som svar på anbudsförfrågan att ange vilka aktiviteter som förslås ingå i systemsäkerhetsarbetet samt redovisar dessa i System Safety Program Plan (SSPP *5.5*). Hur leverantörs svar på kraven bör formuleras, framgår av System Safety Program Plan (SSPP *5.5*) och Safety Requirements/Criteria Analysis (SRCA *5.14*).

Konstruktionspåverkande krav är:

Följande exempel på krav är vägledande för de krav DesignA kan behöva ställa för att tillgodose Försvarsmaktens krav (i TTEM och KB). Kraven är inte utformade för att direkt kunna klippas in.

Operativt inriktade krav:

- Maximal tid för säkerhetsinspektion vid exempelvis daglig och särskild tillsyn.
- Maximala begränsningar vid användning såsom största acceptabla säkerhetsavstånd, längsta acceptabla tid för utbildning på säkerhetsföreskrifter.

Konstruktionskrav:

- Att vissa material och ämnen inte får användas i konstruktionen eller vid drift av denna.
- Att vissa konstruktionslösningar inte får användas i det tekniska systemet, se även HVAS *[24]*, H FordonSäk *[21]* och *kapitel 6*.
- Att vissa konstruktionsprinciper och -lösningar ska tillämpas för speciellt säkerhetskritiska system/funktioner, till exempel felsäker (fail-safe), automatisk test (built-in test), redundanser, modularisering, robust konstruktion, speciella komponenter, programspråk, se *kapitel 2* och *6*.

Krav på avvecklingsbetingelser (se RADS *5.34*):

- Framtagning av Återvinningsmanual *[15]*.
- Moduluppbyggnad för att underlätta återanvändning av tekniskt delsystem.

Systemsäkerhetskrav:

Följande **exempel på krav** är vägledande vid DesignA:s kravställning på potentiella leverantörer. Efter övervägande väljs de krav som behövs för att styra aktuell anskaffning och kraven infogas i anbudsförfrågan.

Krav på leverantörens systemsäkerhetsverksamhet (ställs i RFP):

- Leverantör ska utarbeta systemsäkerhetsplan enligt H SystSäk och bifoga denna i anbudet, i preliminärt utförande. Följande aktiviteter ska ingå: SCA, SCF, RADS, xx, yy, och zz. DesignA ställer krav på vilka aktiviteter som leverantör ska genomföra (och därmed ingå i leverantörens SSPP). Se *avsnitt 3.2, Val av aktiviteter (Tailoring)*.
- I den mån leverantör genomför ytterligare systemsäkerhetsaktivitet för det tekniska systemet, än vad som krävts för SSPP, ska resultatet från dessa överlämnas till DesignA.
- Leverantör ska ha ett eget säkerhetsledningssystem som på ett spårbart sätt demonstrerar hur systemsäkerhetsverksamheten leds, följs upp, beslutas och dokumenteras samt hur detta säkerhetsledningssystem följs upp, utvärderas och kompletteras. En beskrivning av säkerhetsledningssystemet ska bifogas anbudet.
- Leverantör ska ha en särskild systemsäkerhetsorganisation med utpekade roller, ansvar, befogenheter, regler, rutiner och arbetssätt. Denna ska redovisas i anbudet tillsammans med krav på rollernas kompetens.
- Leverantör ska fortlöpande vidmakthålla detaljerad kunskap om de lagregler (föreskrifter med mera) som påverkar design av företagets produkter likväl som deras avsedda användning då de ska användas av Försvarsmakten. I anbudet ska leverantören redovisa hur detta säkerställs för aktuell anskaffning.
- Leverantör ska i anbud till DesignA redovisa namn och befattning/roll på den person som har uppgiften att besluta leverantörens systemsäkerhetsutlåtande (ska vara firmatecknaren eller person direkt underställd denne).
- Leverantör ska skyndsamt anmäla till DesignA förekomst av ej tolerabel olycksrisk (röd risk) för vilken leverantören inte kan identifiera erforderlig riskreducering.

  Olycksrisk med bestående konsekvenser för yttre miljö ska ses som ej tolerabel.

- Leverera systemsäkerhetsutlåtande med systemsäkerhetsrapport (SAR). Leveransen ska ske xx veckor före leverans av det tekniska systemet. Systemsäkerhetsutlåtandet ska, utöver innehåll i exempel i *bilaga 1*, också innehålla xx, yy, zz.

  Systemsäkerhetsutlåtanden ska också utfärdas för följande delsystem (för till exempel ingående ammunition).
- Leverera fullständig riskdokumentation omfattande risklogg, riskbeslut för varje enskild olycksrisk, underlag för instruktioner, anvisningar, handböcker med mera, för hur identifierade olycksrisker ska undvikas, samt eventuell restriktion (avser inskränkning i det tekniska systemets användning för att temporärt hantera viss olycksrisk). Leverans ska ske tillsammans med systemsäkerhetsutlåtandet.

  Dokumenten utformas enligt av Försvarsmakten tillhandahållen modell (blanketter), exempel på mallar och ifyllnad finns i H SystSäk CDR. Om leverantör önskar tillämpa egenutvecklad modell överenskoms detta med DesignA, varvid minst de data som framgår av Försvarsmaktens respektive dokument ska ingå.
- Leverera underlag för den utbildning som krävs från systemsäkerhetssynpunkt. Leverans ska ske senast tillsammans med systemsäkerhetsutlåtandet.
- Leverera föreskrifter och anvisningar för användning och underhåll (inklusive underlag till SäkI). Leverans ska ske tillsammans med systemsäkerhetsutlåtandet.
- Vid utformning av aktuellt tekniskt systems avvikelsehanteringsrutiner, ska Försvarsmaktens avvikelsehanteringssystem xx användas.
- Det tekniska systemets dokumentation ska avfattas på svenska/engelska.

  Vid utformning av detta krav se H SystSäk del 1, avsnitt 5.10.4, och infoga tillämpligt alternativ för aktuella delar av dokumentationen.
- Särskild granskning (kvalitetskontroll) ska genomföras av delsystem yyy/produkt zzz och ska redovisas med särskild granskningsrapport.

  Vid utformning av detta krav se H SystSäk del 1, avsnitt 5.12 och specificera aktuella systemdelar/produkter.

- **Militärt undantag** (Se *H SystSäk del 1, avsnitt 1.2* och *2.4.1*).
  Leverantör ska i anbud på visst tekniskt system utförligt redovisa svensk lag/föreskrift med tillämpning på aktuellt tekniskt system som innehåller någon typ av undantag för militär materiel/militär användning/motsvarande. Om lagen/föreskriften meddelar gränsvärden för civil verksamhet (motsvarande) ska leverantör under anbudstiden begära komplettering avseende Försvarsmaktens krav på aktuella gränsvärden, så att anbudet kommer att grundas på rätt förutsättningar.
- Leverantör ska redovisa vilka regler såsom lagar och förordningar som har påverkat det tekniska systemets utformning respektive vilka författningskrav som ska uppfyllas av Försvarsmakten under drift, vidmakthållande samt avveckling.
- Det tekniska systemets enskilda skade-/olycksrisker för person ska inte överskrida tolerabel risknivå enligt bifogad riskmatris för personskada.
- Det tekniska systemets enskilda skade-/olycksrisker för ekonomisk skada ska inte överskrida tolerabel risknivå enligt bifogad riskmatris för ekonomisk skada.
- Leverantören ska genomföra miljötålighetsverksamhet enligt intentionerna i SEES Handbok Miljötålighetsteknik *[38]*.
- Leverantören ska förse det tekniska systemet med följande säkerhets-/skyddsanordningar: XXX, YYY, ZZZ.
  (Kan till exempel utgöras av brandbekämpningsutrustning av speciell typ, extra utrymningsfunktioner, skydd mot viss strålning.)

5.4.3 Indata

Underlag för att formulera systemsäkerhetskrav i RFP är TTEM *5.3*.

5.4.4 Utdata

Anbudsförfrågan samt indata till SSPP *5.5* och SRCA *5.14*.

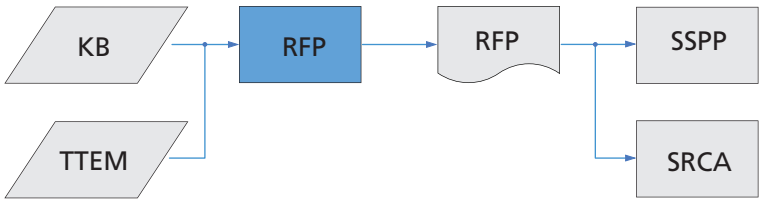


Bild 5:5 Kravställning vid anbudsförfrågan (RFP)

5.4.5 ALARP

För de fall anskaffning planeras ske i samverkan med annan nation som tillämpar ALARP-metodiken så lämnas här några vägledande synpunkter avseende innebörden av ALARP. Först kan konstateras att ALARP-metodiken medför framtagning av underlag som är väl lämpat för systemsäkerhetsverksamhet enligt H SystSäk.

Begreppet ALARP (As Low as Reasonably Practicable) har introducerats av Brittiska HSE (Health and Safety Executive). Begreppet syftar på att kostnad för viss riskreduktion identifieras.

I fall att riskmässig vinst bedöms som högre än kostnad för viss riskreducerande åtgärd, ska enligt brittisk lagstiftning, den riskreducerande åtgärden införas.

Om däremot kostnaden är högre än den riskmässiga vinsten, anses olycksrisken vara just ALARP; ”As Low as Reasonably Practicable”.

Då ett tekniskt system följer allmänt vedertagen konstruktionsstandard, anses ofta att ALARP därigenom uppnås.

Metodiken som används i H SystSäk har en liknande innebörd. Dock skiljer sig riskhanteringen något. ALARP liksom systemsäkerhetsmetodiken utgår från enskild olycksrisk. Dock måste kontrolleras huruvida den bedömda olycksrisken i ALARP-modellen redovisar alla de fyra riskdelarna från varje olycksrisk enligt H SystSäks synsätt, eller endast ”worst credible case” eller ”most credible case”. I detta senare fall behöver också de saknade riskdelarna för varje enskild olycksrisk identifieras till storlek för att systemsäkerhetsmetodiken fullt ut ska kunna tillämpas.

5.5 System Safety Program Plan (SSPP) – Task 102

5.5.1 Syfte

Denna aktivitet som definierar planerade systemsäkerhetsaktiviteter, gäller främst för leverantör. I de fall DesignA är systemsammanhållande gäller denna aktivitet även för DesignA som i dessa fall blir leverantör av ett tekniskt system bestående av integrerade delsystem.

5.5.2 Avvikelser

102.2.4 b: Referens bör även göras till den i H SystSäk del 1 beskrivna riskhanteringsprocessen.

5.5.3 Jämförbara aktiviteter/dokument

En motsvarande plan är Safety Management Plan, (Def-Stan 00-56 *[43]*).

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 102, System Safety Program Plan. Denna aktivitet har en utförligare beskrivning av främst riskanalyserna (102.2.5), men skiljer sig inte med avseende på syfte och ändamål och kan därför tillämpas som ett alternativ.

5.5.4 Ytterligare information

SSPP används för att utvärdera en potentiell leverantörs förståelse för och prioritering av den systemsäkerhetsverksamhet som erfordras vid utveckling av tekniskt system.

För tekniskt system där DesignA har systemansvaret, ska SSPP upprättas och dess aktiviteter genomföras av DesignA.

Som stöd för identifiering av de aktiviteter som bör ingå i en SSPP, lämnas vägledning i *avsnitt 3.2, Val av aktiviteter (Tailoring)*.

5.5.5 Indata

RFP *5.4* utgör underlag för framtagning av SSPP. RFP innehåller bland annat krav på leverans av en SSPP med aktiviteter och en tids- och leveransplan.

5.5.6 Utdata

Utdata från aktiviteten SSPP är dokumentet SSPP. Dokumentet SSPP redovisar alla de systemsäkerhetsrelaterade aktiviteter som ska bedrivas.

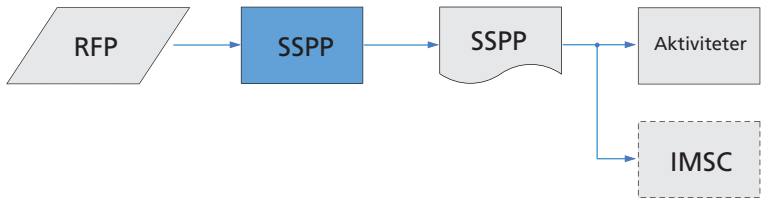


Bild 5:6 System Safety Program Plan (SSPP)

Exempel på SSPP finns i H SystSäk CDR.

5.6 Integration/Management of Subcontractors (IMSC) – Task 103

5.6.1 Syfte

Denna aktivitet gäller vid beställning av integration av delar i ett tekniskt system, eller vid användandet av underleverantör i systemarbetet. I de fall DesignA är systemsammanhållande gäller denna aktivitet även för DesignA. Det fullständiga namnet för denna aktivitet är ”Integration/Management of Associated Contractors, Subcontractors, and Architect and Engineering Firms” (IMSC). Observera dock att akronymen IMSC inte används i MIL-STD-882C.

5.6.2 Avvikelser

103.2.1(8): Referens bör göras till krav i Handbok Vapen och Ammunitionssäkerhet *[24]* samt Handbok Fordonssäkerhet *[21]*.

5.6.3 Jämförbara aktiviteter/dokument

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 103, Integration/Management of Associated Contractors, Subcontractors, and Architect and Engineering Firms. Denna skiljer sig marginellt och kan tillämpas som ett alternativ.

5.6.4 Ytterligare information

I större projekt anlitas oftast flera leverantörer. Om detta sker genom en huvudleverantör svarar denne för att SSPP *5.5* även omfattar underleverantörernas systemsäkerhetsverksamhet.

5.6.5 Indata

SSPP *5.5* utgör grunden för de aktiviteter som ska genomföras. Definierade säkerhetskritiska delar och funktioner styr även underleverantörernas verksamhet, se SCF *5.11*. Styrning av underleverantör sker främst med SOW (Statement of Work, verksamhetsåtagande) eller med krav direkt i beställningen.

5.6.6 Utdata

De utdata som genereras (analyser med mera) inarbetas normalt i huvudleverantörs säkerhetsdokumentation. För utvecklingsuppdrag som ska utföras av underleverantör bör en separat SSPP *5.5* begäras. För färdiga tekniska delsystem bör en SAR *5.21* begäras. Dokumentet som styr underleverantörer är normalt SOW.

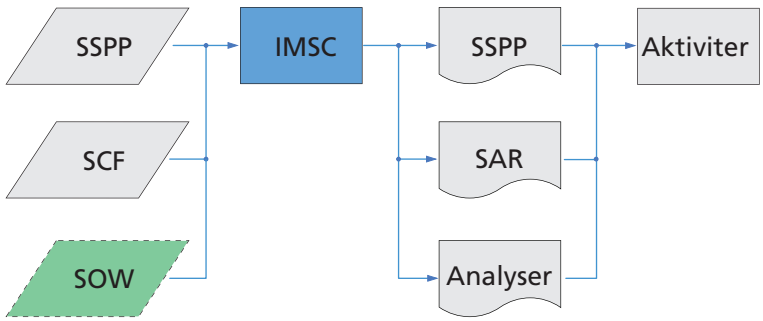


Bild 5:7 Integration/Management of Subcontractors (IMSC)

5.7 System Safety Program Reviews/Audits (SSPR) – Task 104

5.7.1 Syfte

Aktiviteten avser både företagsinterna granskningar och leverantörs medverkan vid beställarens granskningar. Denna aktivitet gäller främst för leverantör. Observera att den specifika akronymen SSPR inte används i MIL-STD-882C.

5.7.2 Avvikelser

104.2.3: Referens bör även göras till Handbok Vapen och Ammunitionssäkerhet *[24]* samt Handbok Fordonssäkerhet *[21]*.

5.7.3 Jämförbara aktiviteter/dokument

Denna granskning riktar sig i första hand mot uppfyllandet av SSPP *5.5*. Granskningar av det tekniska systemet med dess maskinvara och programvara omfattas inte av denna aktivitet. Detta kan regleras av de standarder som tillämpas under utveckling och tillverkning.

Den civila standarden GEIA-STD-0010 *[27]*] har en likvärdig aktivitet, Task 104, System Safety Program Reviews/Audits. Denna skiljer sig marginellt och kan tillämpas som ett alternativ.

5.7.4 Ytterligare information

Frekvens och omfattning av granskningar utförda av beställaren som kräver medverkan av leverantör ska särskilt regleras i beställningen.

Resultat från granskningen dokumenteras i en granskningsrapport med åtföljande åtgärdslista avseende brister som har identifierats.

Granskningar som ska genomföras av exempelvis DesignA:s rådgivningsgrupper omfattas även av denna aktivitet, se H VAS *[24]*.

5.7.5 Indata

SSPP *5.5*, med systemsäkerhetsdokument som genererats vid genomförda systemsäkerhetsaktiviteter, främst Risklogg (se HTRR *5.9*), utgör indata för granskning.

För granskningar i DesignA:s rådgivningsgrupper regleras omfattning av erforderligt underlag i H VAS *[24]*.

5.7.6 Utdata

Utdata är protokoll från säkerhetsgranskningen med eventuellt uppdaterad Risklogg (se HTRR *5.9*). Från DesignA:s rådgivningsgrupper genereras speciella granskningsprotokoll.

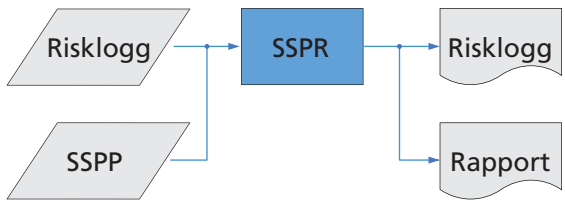


Bild 5:8 System Safety Program Reviews/Audits (SSPR)

5.8 System Safety Working Group (SSWG) – Task 105

5.8.1 Syfte

I H SystSäk del 1 definieras och beskrivs två olika utföranden för den säkerhetsrelaterade gruppen SSWG. Det fullständiga namnet för denna aktivitet är System Safety Group/System Safety Working Group Support (SSWG).

SSWG-1: Tillsätts av DesignA som stöd till projekt. Verksam under utveckling och anskaffning. Försvarsmakten, DesignA och leverantör kan medverka.

SSWG-2: Tillsätts av ÄF som del i dennes ansvar för tekniska system i drift. Verksam under tekniskt systems hela livslängd men främst med inriktning mot vidmakthållande- och avvecklingsfaserna. Försvarsmakten, DesignA och leverantör kan medverka i gruppen.

5.8.2 Avvikelser

105.1: ”Service regulations” är oftast inte tillämpbart för svenska förhållanden utan detta regleras av Försvarsmakten/DesignA.

5.8.3 Jämförbara aktiviteter/dokument

En motsvarande grupp är Safety Panel. (JSP520 *[34]*, JSP454 *[35]*, Def-Stan 00-56 *[43]*).

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 105, System Safety Group/ System Safety Working Group Support. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 kräver att leverantör svarar för mötesagenda och mötesprotokoll (105.3.d).

5.8.4 Ytterligare information

Frekvens och omfattning av leverantörs medverkan i SSWG-1 och SSWG-2 ska särskilt regleras i beställningen.

5.8.5 Indata

Reglering av mötesfrekvens och agenda kan ske i SSMP, se SSP *5.1* och SSPP *5.5*. Inför möten ska mötesagenda skickas ut. Risklogg (se HTRR *5.9*) och felrapportering (se FRACAS *5.28*) utgör ofta indata till mötena.

5.8.6 Utdata

Mötesanteckningar samt information till Risklogg eller motsvarande, se HTRR *5.9*.

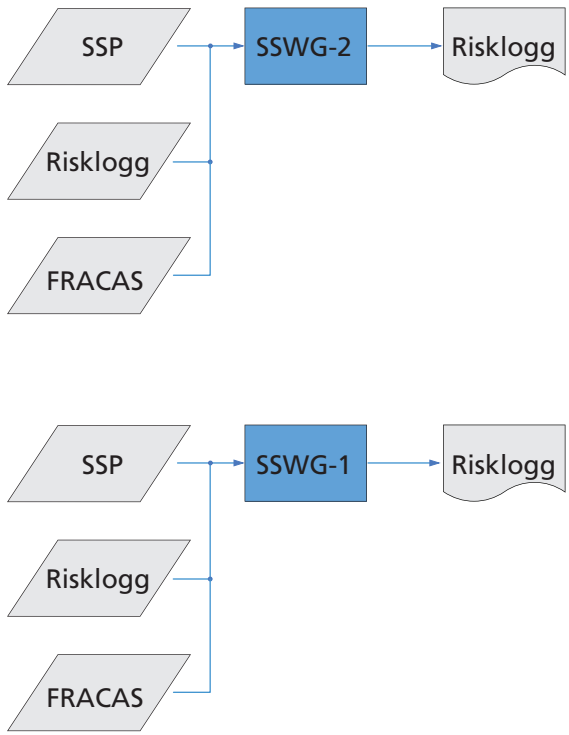


Bild 5:9 System Safety Working Group (SSWG)

5.9 Hazard Tracking and Risk Resolution (HTRR) – Task 106

5.9.1 Syfte

Aktiviteten avser etablering av en riskuppföljningsprocess med dokumentation av identifierade olycksrisker i en Risklogg (Hazard Log) där även övrig administration samt stängning av risker dokumenteras. För redan befintliga tekniska system etableras och drivs riskuppföljningsprocessen av Försvarsmakten. Akronymen HTRR används inte i MIL-STD-882C.

5.9.2 Avvikelser

–

5.9.3 Jämförbara aktiviteter/dokument

Motsvarigheten till risklogg är i UK en Hazard Log. Formatet för denna är strikt reglerat och ska vara en databas vid namn Cassandra, (Def-Stan 00-56 *[43]*).

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 106, Hazard Tracking and Risk Resolution. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 anger att alla olycksrisker ska registreras, inte bara kvarstående olycksrisker (106.2.1.d). Notera dock att oavsett tillämpad standard, så ska risklogg för tekniskt system, enligt H SystSäk, alltid omfatta samtliga identifierade olycksrisker.

5.9.4 Ytterligare information

Riskloggen är en ”databas” med information om identifierade olycksrisker. Denna ska upprätthållas under det tekniska systemets hela liv. Riskloggen initieras oftast av Försvarsmakten vid studier, tas över av leverantör vid utveckling och tillverkning, samt återgår vid leverans av det tekniska systemet till Försvars-

makten för faserna vidmakthållande och avveckling. Stängning av olycksrisker sker enligt SSPP *5.5*. Normalt redovisas risklogg-en vid SSPR *5.7* och SSPS *5.10*.

5.9.5 Indata

SSMP (se SSP *5.1*) och SSPP *5.5* initierar och definierar införandet av en Risklogg. Olycksrisker från analyser (PHL *5.12*, PHA *5.13*, SRCA *5.14*, FHA *5.20*, SHA *5.16*, SSHA *5.15*, FRACAS *5.28*) utgör indata till Risklogg (Hazard Log).

5.9.6 Utdata

Risklogg (Hazard Log) kan användas vid Säkerhetsverifiering (SV *5.24*) och vid framtagning av SAR *5.21*. Redovisning av Risklogg-en kan ske vid SSPR *5.7*, SSWG *5.8* och SSPS *5.10*.

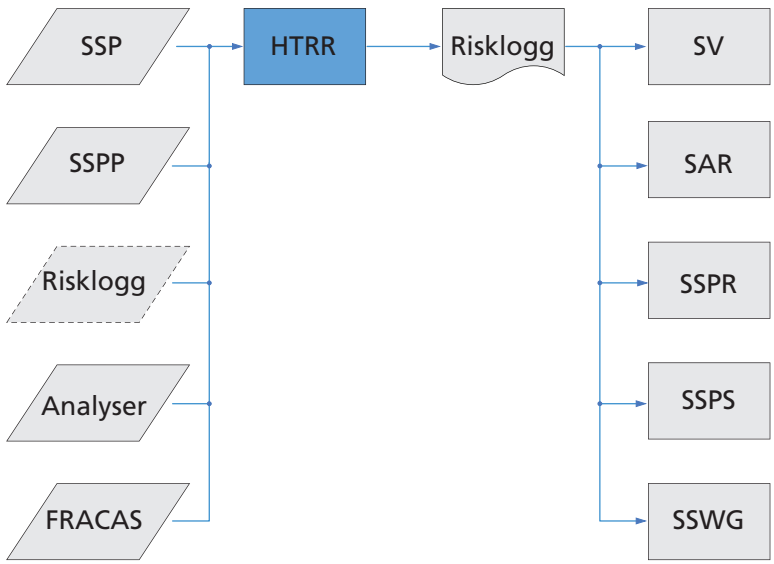


Bild 5:10 Hazard Tracking and Risk Resolution (HTRR)

5.10 System Safety Progress Summary (SSPS) – Task 107

5.10.1 Syfte

Aktiviteten avser främst leverantörs rapportering av läget för systemsäkerhetsprogrammet och systemsäkerhetsaktiviteterna. Denna aktivitet är nära kopplad till aktivitet SSWG *5.8*.

Akronymen SSPS används inte i MIL-STD-882C.

5.10.2 Avvikelser

–

5.10.3 Jämförbara aktiviteter/dokument

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 107, System Safety Progress Summary. Denna skiljer sig marginellt och kan tillämpas som ett alternativ.

5.10.4 Ytterligare information

Periodiciteten på rapporteringen måste anges i Leveransplan eller SSPP *5.5*.

5.10.5 Indata

SSPP *5.5* och aktiviteter som är genomförda under senaste perioden. Olycksrisker med status från Risklogg (se HTRR *5.9*) redovisas.

5.10.6 Utdata

Lägesrapport för säkerhet (System Safety Progress Report).

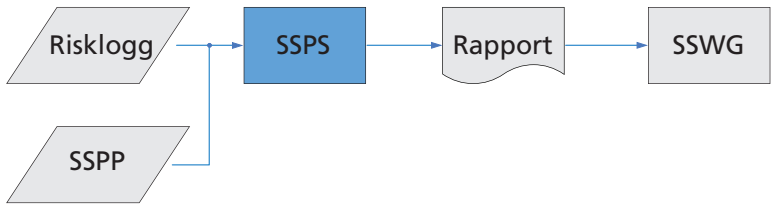


Bild 5:11 System Safety Progress Summary (SSPS)

5.11 Safety Critical Functions (SCF) – S13

5.11.1 Syfte

Som en del av kvalitetsprogrammet för ett tekniskt system ska leverantör identifiera, upprätta, dokumentera och vidmakthålla procedurer, utvecklingsprocesser, arbetsinstruktioner och processer för alla produktionsoperationer med mera som används vid utveckling och tillverkning av delar som kan karaktäriseras som kritiska ur säkerhetssynpunkt. Genom att ange kritikalitetsklasser i utvecklings- och produktbeskrivande dokument, skapas förutsättningar för att styra resurserna vid utveckling och tillverkning samt kontroll dit de bäst behövs. Motsvarande aktivitet finns i den civila standarden GEIA-STD-0010 Task 209 *[27]*. Denna aktivitet återfinns inte i tidigare utgåva av H SystSäk men är internationellt tillämpad, därför används det engelska namnet. Kritiska egenskaper återfinns under *kapitel 2, Materielkrav*.

5.11.2 Aktivitetsbeskrivning

Definition av kritiska egenskaper

Säkerhetskritiska och säkerhetsrelaterade delar är de som har sådana egenskaper (tolerans, hårdhet, ytfinhet, feltålighet hos programvara med mera) som kan resultera i vådahändelse om brist i egenskapen föreligger eller delar som i sig kan ge vådahändelse om de saknas i en installation.

De **säkerhetskritiska** egenskaperna/detaljerna är de som direkt (exempelvis vid enkelfel) påverkar säkerheten hos det tekniska systemet.

De **säkerhetsrelaterade** egenskaperna/detaljerna är de som påverkar säkerheten (exempelvis vid dubbelfel eller vid fel av högre ordning) hos det tekniska systemet.

Dessa kritiska och säkerhetsrelaterade egenskaper indelas i två grupper; de som vid brister i egenskapen kan ge KRITISKT FEL (som kan resultera i olycka med SKADEKLASS 1) och de som kan ge ALLVARLIGT FEL (som kan resultera i olycka med högst SKADEKLASS 2).

De kritiska delarna/egenskaperna identifieras vid riskanalysen genom att undersöka avvikelserna/bristernas bidrag till vådahändelsen för det tekniska systemet. För varje del/egenskap noteras sannolikhet eller felfrekvens för att fel inträffar, samt vilken konsekvens detta ger på det tekniska systemet. Om bristen på den angivna egenskapen kan påverka vådahändelsen med tillräcklig stor dignitet ska egenskaper/komponenter klassificeras på ritning eller i specifikation.

För maskinvara eller maskininriktade delar klassificeras de kritiska egenskaper (CI) enligt exempelvis SS 2222 *[41]* (Svensk Standard). För programvara med tillhörande elektronik ska kritikaliteten uttryckas enligt anvisningar i *kapitel 6* och H ProgSäk *[18]*.

Definition av kritikalitet i komplexa system

Informationen i detta avsnitt har primärt hämtats från flygmaterielområdet där det finns definierade metoder för att hantera systematiska fel i komplexa system.

De huvudsakliga källorna till information är SAE ARP4754 (Certification Considerations for Highly-Intergrated or Complex Aircraft Systems) *[4]*, RTCA/DO-178B (Software Considerations in Airborne Systems and Equipment Certification) *[40]* och RTCA/DO-254 (Design Assurance Guidance for Airborne Electronics Hardware) *[6]*.

För avgränsade komponenter kan dessas kritikalitet bestämmas genom att analysera hur de kan bidra till uppkomsten av olycksrisker samt riskens konsekvens. ARP4754 *[4]* och RTCA/DO-178B *[40]* innehåller information om hur komponenter kan klassificeras baserat på förekomst av övervakningsfunktionen och redundans. Samtliga ovan refererade dokument använder sig av en skala A-E för att klassificera komponenter, där A är de mest kritiska komponenterna och E de minst kritiska komponenterna.

Alla komponenter i ett system kan klassificeras baserat på kritikalitet men endast sådana komponenter som anses komplexa behöver underkastas en utvecklingsmetodik som är differentierad baserad på kritikalitet.

En komponent anses komplex när granskning, analys och test som genomförs som en naturlig del i komponentens utveckling inte med nödvändighet kan anses verifiera dess fulla beteende. Exempel på sådana komponenter är programvara och olika typer av programmerade kretsar. Icke komplexa komponenter anses motsvara kritikalitetsklass A när verifiering har genomförts som säkerställer dess funktionalitet och egenskaper.

Den metodik som föreskrivs av ovan refererade dokument kan sammanfattas enligt följande:

- Definiera och överenskom med kund/myndigheter vilken metodik som ska användas för kritikalitetsklassning. ARP4754 *[4]*, DO-178B *[40]* samt DO-254 *[6]* kan användas som en utgångspunkt men även IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) *[16]* kan användas.
- Identifiera alla komplexa komponenter i systemet.
- Analysera hur dessa kan bidra till identifierade olycksrisker.
- Klassificera komponenterna enligt överenskommen metodik.
- Överenskom vilka utvecklingsaktiviteter (granskning, analys, prov med mera) som ska genomföras för olika kritikalitetsnivåer. Även här kan information hämtas ur ARP4754 *[4]*, DO-178B *[40]*, DO-254 *[6]* samt IEC 61508 *[16]*.
- Utveckla system och ingående komponenter enligt överenskommen metodik.
- Rapportera resultat av utveckling (identifierade brister med mera) samt eventuell avvikelse från överenskommen metodik.

Att utvecklingen verkligen har genomförts enligt överenskommen metodik kan styrkas genom att oberoende kvalitetsrevisioner genomförs med avsikt att säkerställa just detta.

Givet att utvecklingen har bedrivits enligt överenskomna metoder, oberoende bevis föreligger för att så är fallet och att inga brister hos produkten har identifierats, så kan systematiska fel i produkten anses ha hanterats.

Driftserfarenhet kan användas som ett alternativ eller komplement till en definierad utvecklingsmetodik under förutsättning att:

- Driftsprofilen under driftstiden motsvarar den tänkta driftsprofilen i det nya systemet.
- Driftstiden anses vara tillräcklig med hänsyn tagen till systemets/komponentens kritikalitet.
- Ett fungerande felrapporteringssystem har funnits för aktuell driftsperiod.
- Eventuella fel hos produkten kan accepteras.
- Eventuella ändringar av produkten under driftstiden har identifierats och de anses inte påverka systemet/komponenten på sådant sätt att driftstiden kan ifrågasättas.

Identifiering av kritiska egenskaper

Kritiska egenskaper identifieras genom analyserna (PHL *5.12*, PHA *5.13*, SRCA *5.14*, FHA *5.20*, SHA *5.16*, SSHA *5.15*). Kritiska egenskaper kan identifieras på flera sätt (eller i kombination):

- Med felträdsanalyser (FTA); om en enskild egenskap bidrar till den kritiska vådahändelsen med tillräckligt stor dignitet så är den säkerhetskritisk. Lämpligen fastställs nivån i System Safety Program Plan (SSPP *5.5*). Metoden för dessa beräkningar är Minimal Cut Set (MCS).
- Med feleffektanalys (FMECA); om en enskild egenskap har en tillräckligt stor inträffandesannolikhet eller felfrekvens samt att den presumtiva vådahändelsen är kritisk. Nivån fastställs i System Safety Program Plan (SSPP *5.5*).
- Baserat på erfarenheter/ingenjörsmässiga bedömningar; om en enskild egenskap genom erfarenhet bedöms påverka säkerheten avsevärt eller reglerat genom olika tilllämpliga standarder. För programvara, se *kapitel 6*.

Lista över kritiska egenskaper (CIL/SIL)

Leverantör ska, om så krävs i beställningshandlingarna, förse DesignA med en lista över kända kritiska egenskaper. Listan bör även ange vilket produktions- och kontrollunderlag som gäller för den aktuella egenskapen eller detaljen. För programvara anges vilken metodik som tillämpas vid framtagningen av programvaran.

Utveckling av programvara

De egenskaper som är kritiska ska identifieras och styr valet av de metoder som ska användas vid framtagning, och verifiering av relaterad programvara. Se vidare *kapitel 6*.

Produktionsstyrning/kontroll av processer

De processer som används för att styra/kontrollera kritiska egenskaper ska anges i produktionsunderlag och kvalitetsplaner eller motsvarande.

För de processer som används ska det vara möjligt för operatören att verifiera att de har genomförts korrekt.

I de fall underleverantör används ska motsvarande krav ställas på denne, se Integration/Management of Subcontractors (IMSC *5.6*).

Kontrollutrustning

Den utrustning som används för kontroll av kritiska egenskaper ska identifieras och beskrivas.

Ändringsstyrning

En avvikelse/ändring av en kritisk egenskap bör inte kunna genomföras av leverantör utan godkännande av DesignA. Hur detta förfarande går till regleras i Konfigurationsplan eller motsvarande. Se Safety Review (SR *5.23*).

5.11.3 Indata

Underlag för SCF är samtliga genomförda analyser 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* samt krav enligt SRCA *5.14*.

5.11.4 Utdata

Lista över kritiska egenskaper/delar (CIL) samt kritikalitets- eller tillförlitlighetsnivåer (SIL).

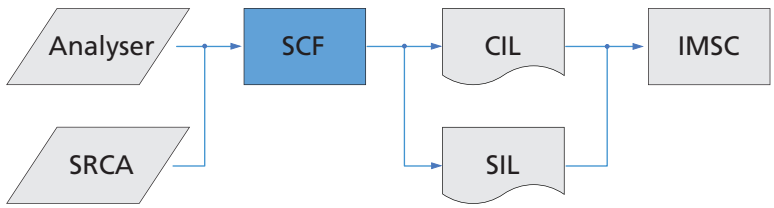


Bild 5:12 Safety Critical Functions (SCF)

5.12 Preliminary Hazard List (PHL) – Task 201

5.12.1 Syfte

Aktiviteten avser att tidigt identifiera potentiella olycksrisker. Denna aktivitet är nära kopplad till HTRR *5.9* med Risklogg (Hazard Log).

5.12.2 Avvikelser

–

5.12.3 Jämförbara aktiviteter/dokument

För programvara se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 201, Preliminary Hazard List. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en PHL (201.2.4).

5.12.4 Ytterligare information

En PHL kan krävas som del av ett anbud. En PHL följs oftast av ytterligare fördjupade analyser såsom PHA *5.13*, SRCA *5.14*, FHA *5.20*, SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18* och EHA *5.19*.

Ett stort antal hjälplistor för att identifiera potentiella olycksrisker finns att tillgå och några som kan rekommenderas är: US WSESRB Hazard Analysis Guide list *[44]* och UK Hazard Identification Checklist (Def-Stan 00-56 *[5]*).

5.12.5 Indata

Ett koncept eller en konstruktionsbeskrivning erfordras för att genomföra en PHL. Ändringar av konceptet enligt SR *5.23* följs upp i PHL.

5.12.6 Utdata

Preliminary Hazard List (PHL) samt indata till Risklogg (Hazard Log) enligt HTRR *5.9*.

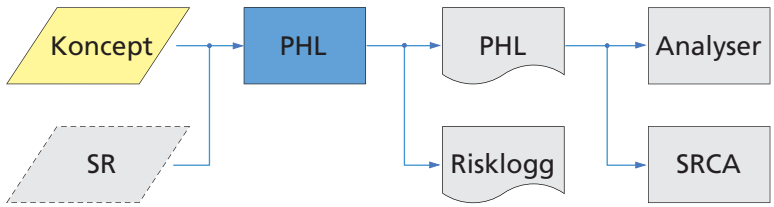


Bild 5:13 Preliminary Hazard List (PHL)

Risklogg finns som Excel-fil i H SystSäk CDR.

5.13 Preliminary Hazard Analysis (PHA) – Task 202

5.13.1 Syfte

Aktiviteten avser att tidigt identifiera potentiella vådahändelser samt att göra en inledande systemsäkerhetsvärdering. Denna aktivitet är nära kopplad till HTRR *5.9* med Risklogg (Hazard Log).

5.13.2 Avvikelser

–

5.13.3 Jämförbara aktiviteter/dokument

För programvara se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 202, Preliminary Hazard Analysis. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en PHA (202.2.2) samt krav på redovisning av olyckor istället för vådahändelser (202.3.1.b) Om GEIA-STD-0010 används tillkommer även avveckling under (202.2.2.3 b(2)).

5.13.4 Ytterligare information

PHA är oftast en inledande analys i likhet med PHL *5.12*, som uppdateras efter hand och fördjupas genom kommande mer detaljerade analyser. Resultatet av en PHA kan används vid definiering av krav.

En PHA bör innehålla:

- erfarenhetsdata
- lista över kända vådahändelser
- vidtagna åtgärder för att eliminera/minimera vådahändelserna
- krav som följd av identifierade vådahändelser
- rekommenderade åtgärder att vida för att eliminera/minimera vådahändelserna.

Underlag som behövs är koncept och konstruktionsbeskrivningar, flödesschema och information om driftprofil.

Formatet för en PHA kan variera från rent beskrivande dokument till matrisformat.

5.13.5 Indata

Ett koncept eller en konstruktionsbeskrivning, flödesscheman, driftprofil, samt oftast en PHL *5.12* erfordras för att genomföra en PHA. Ändringar av konstruktion redovisas enligt SR *5.23* och följs upp i PHA.

5.13.6 Utdata

Preliminary Hazard Analysis (PHA) samt indata till Risklogg (Hazard Log) enligt HTRR *5.9*.

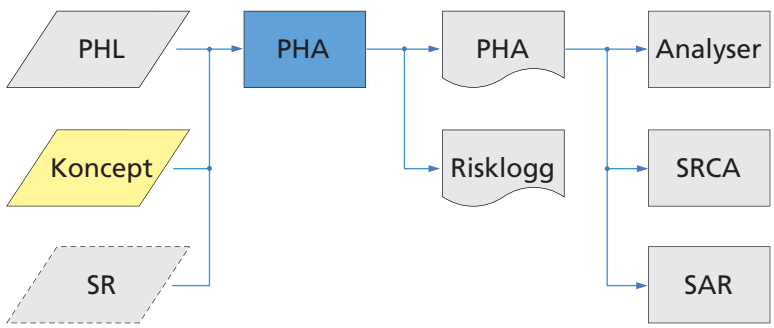


Bild 5:14 Preliminary Hazard Analysis (PHA)

5.14 Safety Requirements/Criteria Analysis (SRCA) – Task 203

5.14.1 Syfte

Aktiviteten avser att identifiera säkerhetskrav relaterade till de vådahändelser eller farliga tillstånd som identifierats i PHL *5.12*/ PHA *5.13* och FHA *5.20* samt även identifiera övriga säkerhetsrelaterade krav från exempelvis lagstiftning, kundkrav (RFP *5.4*), standarder, med mera.

5.14.2 Avvikelser

203.2.2: Här tillkommer även RFP *5.4*, H VAS *[24]*, H FordonSäk *[21]* samt *kapitel 6* för programvara.

203.2.2.e: Här ersätts ”Appendix A” med *kapitel 6*.

5.14.3 Jämförbara aktiviteter/dokument

För programvara se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 203, Safety Requirements/Criteria Analysis. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en SRCA (203.2.5). Om GEIA-STD-0010 används kan ordet ”federal” utgå under 203.2.5.1.1.

5.14.4 Ytterligare information

I ett tidigt skede ska leverantör identifiera kritiska delar och funktioner i ett tekniskt system. Avsikten är att baserat på detta definiera krav som förhindrar att dessa kritiska delar felfungerar, se aktivitet S13, Safety Critical Functions (SCF *5.11*). En SRCA kan dokumenteras enligt DI-SAFT-80101B, System Safety Hazard Analysis Report *[8]*.

5.14.5 Indata

För att genomföra en SRCA fordras en PHL *5.12*/PHA *5.13* eller FHA *5.20* samt krav från RFP *5.4* och relevanta lagar och förordningar.

5.14.6 Utdata

Underlag till kravspecifikationer (SSS, SI, IRS), identifiering av kritisk programvara (SCCSC), samt underlag till samt underlag till risklogg (se HTRR *5.9*) och CIL (se SCF *5.11*). Safety Verification (SV *5.24*) är nära anknutet till SRCA.

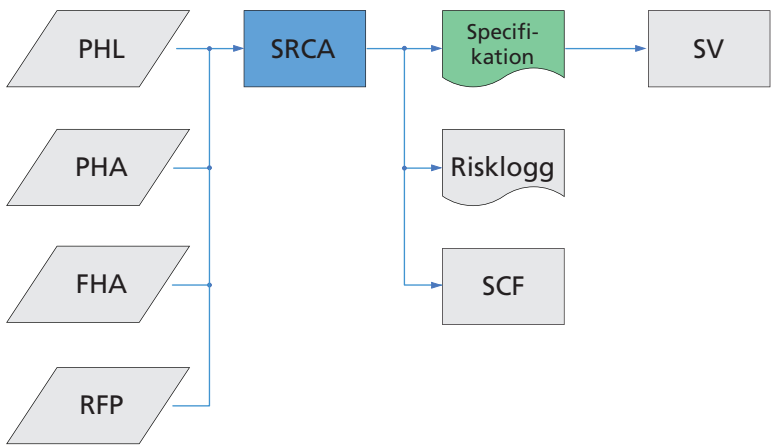


Bild 5:15 Safety Requirements/Criteria Analysis (SRCA)

5.15 Subsystem Hazard Analysis (SSHA) – Task 204

5.15.1 Syfte

Aktiviteten avser att identifiera eventuellt tillkommande vådahändelser efter den initiala riskidentifieringen samt även att verifiera överensstämmelse med säkerhetskraven för de tekniska delsystemen.

5.15.2 Avvikelser

204.2.3: De angivna standarderna DOD-STD-2167, DOD-STD-2168 och MIL-STD-1679 ersätts av anvisningar i *kapitel 6*.

204.3.1 c, d, e: Dessa kan även definieras i SSPP *5.5*.

5.15.3 Jämförbara aktiviteter/dokument

För programvara, se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 204, Subsystem Hazard Analysis. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en SSHA (204.2.5). Om GEIA-STD-0010 används tillkommer även avveckling (204.2.5.3 b(2)). GEIA-STD-0010 anger att alla olycksrisker ska registreras, inte bara kvarstående olycksrisker (204.3.b).

Notera dock att oavsett tillämpad standard, så ska risklogg för tekniskt system, enligt H SystSäk, alltid omfatta samtliga identifierade olycksrisker.

5.15.4 Ytterligare information

Denna aktivitet genomförs om det tekniska systemet består av ett antal tekniska delsystem eller komponenter. Olycksrisker som kan förknippas med felmoder eller operativ hantering analyseras. Vidare identifieras riskreducerande åtgärder. En SSHA kan dokumenteras enligt DI-SAFT-80101B, System Safety Hazard Analysis Report *[8]*. Exempel på analysmetoder framgår av *kapitel 8*.

5.15.5 Indata

En koncept- eller konstruktionsbeskrivning, flödesscheman, drift-/operationsprofil, samt oftast en PHA *5.13* eller FHA *5.20* erfordras för att genomföra en SSHA.

5.15.6 Utdata

Subsystem Hazard Analysis (SSHA) samt underlag till SHA *5.16*, SCF *5.11* och Risklogg (se HTRR *5.9*).

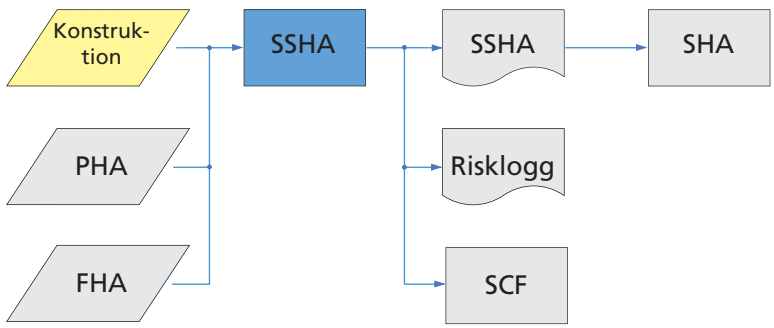


Bild 5:16 Subsystem Hazard Analysis (SSHA)

5.16 System Hazard Analysis (SHA) – Task 205

5.16.1 Syfte

Aktiviteten avser att identifiera eventuellt tillkommande vådahändelser beroende på bland annat interaktion mellan tekniska delsystem samt även att verifiera överensstämmelse med säkerhetskraven för det tekniska systemet.

5.16.2 Avvikelser

205.2.1(e) Ordet ”reasonable” ska tolkas som DEN ANVÄNDNING SOM SKÄLIGEN KUNNAT FÖRVÄNTAS för att stämma överens med Produktansvarslagens *[36]* text.

205.2.3 De angivna standarderna DOD-STD-2167, DOD-STD-2168 och MIL-STD-1679 ersätts av anvisningar i *kapitel 6*.

205.3.1 d: Detta kan även definieras i SSPP.

5.16.3 Jämförbara aktiviteter/dokument

För SHA med avseende på programvara, se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 205, System Hazard Analysis. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en SHA (205.2.5). Om GEIA-STD-0010 används tillkommer även avveckling (205.2.5.3 b(2)). GEIA-STD-0010 anger att alla olycksrisker ska registreras, inte bara kvarstående olycksrisker (205.3.b).

Notera dock att oavsett tillämpad standard, så ska risklogg för tekniskt system, enligt H SystSäk, alltid omfatta samtliga identifierade olycksrisker.

5.16.4 Ytterligare information

En SHA genomförs när det tekniska systemets kontruktion fastställs. Den fokuserar på interaktionen mellan de olika tekniska delsystemen samt tar hand om systemaspekterna. Vidare ska samverkan med andra tekniska system beaktas. Analysteknik i likhet med SSHA *5.15* kan användas. Exempel på analysmetoder framgår av *kapitel 8*.

Speciellt beaktas:

- det tekniska delsystemets interaktion med andra tekniska delsystem
- överensstämmelse med definierade säkerhetskrav
- kombinationer av oberoende och beroende fel
- om det tekniska systemet degenereras vid normal användning
- om ändringar i det tekniska systemet kan påverka systemsäkerheten.

En SHA kan dokumenteras enligt DI-SAFT-80101B, System Safety Hazard Analysis Report *[8]*.

5.16.5 Indata

En system- och konstruktionsbeskrivning, drift-/operationsprofil, samt oftast en PHA *5.13*, FHA *5.20* och en SSHA *5.15* kan fordras för att genomföra en SHA.

5.16.6 Utdata

System Hazard Analysis (SHA), underlag till SCF *5.11* samt indata till Risklogg (se HTRR *5.9*)

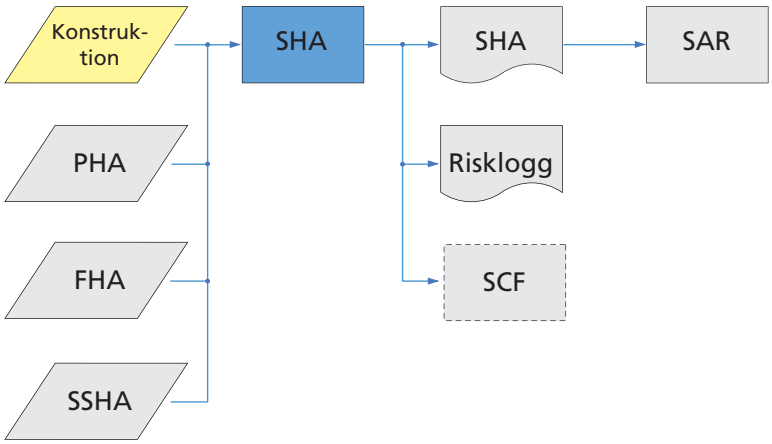


Bild 5:17 System Hazard Analysis (SHA)

5.17 Operating and Support Hazard Analysis (O&SHA) – Task 206

5.17.1 Syfte

Aktiviteten avser att analysera det tekniska systemet med avseende på olycksrisker utifrån ett användningsperspektiv samt att utvärdera föreskrifter och instruktioner.

5.17.2 Avvikelser

206.2.2: Leverantörs produktionsrelaterade operationer omfattas inte för svenska förhållanden eftersom dessa regleras av Arbetsmiljölagstiftningen *[2]*. Produktion som ska utföras av Försvarsmaktens personal omfattas dock av paragrafen.

206.3.1 c: Detta kan även definieras i SSPP *5.5*.

5.17.3 Jämförbara aktiviteter/dokument

För avveckling gäller även RADS *5.34*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 206, Operating and Support Hazard Analysis. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en O&SHA (206.2.5). Om GEIA-STD-0010 används bör även avveckling beaktas (206.2.5.3 b(2)). GEIA-STD-0010 anger att alla olycksrisker ska registreras, inte bara kvarstående olycksrisker (206.3.b).

Notera dock att oavsett tillämpad standard, så ska risklogg för tekniskt system enligt H SystSäk alltid omfatta samtliga identifierade olycksrisker.

5.17.4 Ytterligare information

FMV handbok HMI för tekniska handläggare ger ytterligare information *[14]*.

En O&SHA kan omfatta användning och hantering av det tekniska systemet vid exempelvis provning, underhåll, modifieringar, träning och installation.

Användningsfaser som även ska beaktas är nödfaser, såsom nödutrymning och räddningsoperationer.

En O&SHA kan dokumenteras enligt DI-SAFT-80101B, System Safety Hazard Analysis Report *[8]*.

Exempel på analysmetoder framgår av *kapitel 8*.

5.17.5 Indata

En systembeskrivning, drift-/operationsprofil, samt oftast PHA *5.13*, SHA *5.16*, SSHA *5.15* och HMI-rapporter erfordras för att genomföra en O&SHA. För granskning och analys av användningsinstruktioner fordras minst utkast av dessa.

5.17.6 Utdata

Operating and Support Hazard Analysis (O&SHA) samt indata till Risklogg (se HTRR *5.9*) och SI *5.25* samt TSR *5.32* genereras.

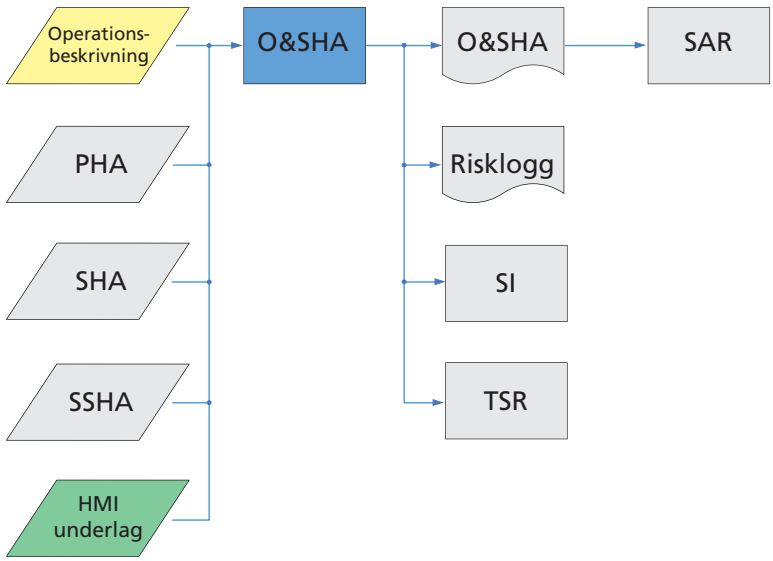


Bild 5:18 Operating and Support Hazard Analysis (O&SHA)

5.18 Health Hazard Assessment (HHA) – Task 207

5.18.1 Syfte

Aktiviteten avser att identifiera hälsorelaterade risker samt att utvärdera hälsofarliga material och ämnen. Underlaget ska ge information för det systematiska arbetsmiljöarbetet som ska bedrivas av arbetsgivaren i den organisation som ska använda det tekniska systemet.

5.18.2 Avvikelser

207.2: Inverkan på yttre miljö hanteras i aktiviteten EHA *5.19*.

207.2.2: Leverantörs produktionsrelaterade verksamhet omfattas inte för svenska förhållanden eftersom dessa regleras av Arbetsmiljölagstiftningen *[2]*. Produktion, relaterad till det tekniska systemet, som ska utföras av Försvarsmaktens personal omfattas dock av paragrafen.

207.3.1 d: Detta kan även definieras i SSPP *5.5*.

5.18.3 Jämförbara aktiviteter/dokument

För avveckling gäller även RADS *5.34*. De krav som gäller finns angivna i Arbetsmiljöverkets föreskrifter samt svensk miljölagstiftning och relevanta myndighetsföreskrifter. I UK tillämpas OHHA (Operating and Health Hazard Analysis) och COSHH (Control of Substances Hazardous to Health).

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 207, Health Hazard Assessment. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en HHA (206.2.3) men saknar de anvisningar om vad granskningen ska omfatta vilket finns angivet i MIL-STD-882C paragraf 207.2.2. GEIA-STD-0010 anger att alla risker ska registreras, inte bara kvarstående risker (206.3.b).

Notera dock att oavsett tillämpad standard, så ska risklogg för tekniskt system, enligt H SystSäk, alltid omfatta samtliga identifierade olycksrisker.

En kommentar till MIL-STD-882C paragraf (207.2.3.4.2) är att det för varje kemisk produkt ska finnas ett säkerhetsdatablad (SDB) tillgängligt. Säkerhetsdatabladens utformning regleras av Europarådets förordning *[13]* (REACH).

5.18.4 Ytterligare information

Genom att inventera farliga ämnen och andra riskkällor/farliga tillstånd för vilka användarna kan exponeras under det tekniska systemets livslängd, skapar man en bra grund för den fortsatta granskningen. Granskning och utvärdering bör ske mot Kemikalieinspektionens och Arbetsmiljöverkets regler och föreskrifter.

Följande faktorer bör beaktas vid bedömningen:

- mängden av farligt material eller farlig exponering
- utsläpp vid planerad användning
- utsläpp vid eventuell vådahändelse
- farligt avfall från det tekniska systemet
- hur omhändertas farligt material
- skyddsutrustning vid användning av det tekniska systemet
- indikatorer för utsläpp av farliga ämnen
- antal exponerade personer
- möjliga skyddsåtgärder.

Följande faktorer bör beaktas vid utvärderingen:

- tillåtna gränsvärden, både för korttids- och långtidsexponering
- kroniska hälsoeffekter
- cancerogena material
- kontaktallergirisk
- brandbenägenhet.

En HHA kan dokumenteras enligt DI-SAFT-80106A, Health Hazard Assessment Report *[12]*.

Exempel på analysmetoder framgår av *kapitel 8*.

5.18.5 Indata

En systembeskrivning, drift-/operationsprofil, samt oftast PHA *5.13*, SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HMI och materialinformation (materiallista/materialdeklaration) erfordras för att genomföra en HHA.

5.18.6 Utdata

Health Hazard Assessment (HHA), Säkerhetsdatablad (SDB) samt underlag till Risklogg (HTRR *5.9*).

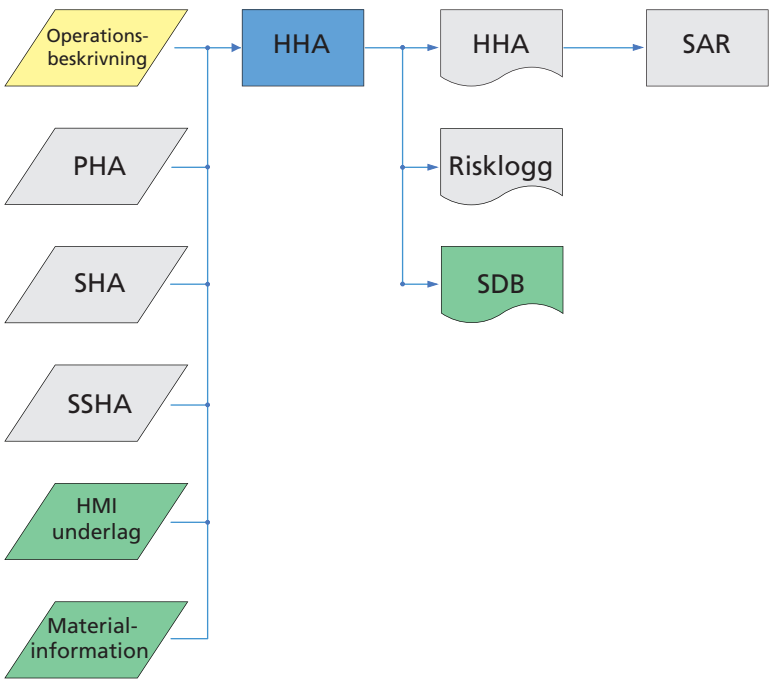


Bild 5:19 Health Hazard Assessment (HHA)

5.19 Riskanalys för yttre miljö (EHA) – S21

5.19.1 Syfte

Syftet med riskanalys för yttre miljö (EHA) är att utvärdera de potentiella olyckor, beroende på riskkällor/farliga tillstånd, som kan förekomma vid all hantering av det tekniska systemet. Hanteringen sträcker sig från första överlämningen till och med destruktionen eller avvecklingen av det tekniska systemet. Miljöpåverkan för normala utsläpp (ej olycksrelaterade) vid all hantering omhändertas oftast i det ordinarie miljöarbetet. I de fall som miljöpåverkan inte beaktas, bör motsvarande miljöarbete bedrivas inom ramen för EHA-aktiviteten. Aktiviteten genomförs av leverantör.

5.19.2 Aktivitetsbeskrivning

Denna aktivitet behandlar vådahändelser som kan leda till utsläpp till omgivningen.

Ingångsdata för denna analys är Operation and Support Hazard Analysis (O&SHA *5.17*), Preliminary Hazard List (PHL *5.12*), Preliminary Hazard Analysis (PHA *5.13*), Subsystem Hazard Analysis (SSHA *5.15*), System Hazard Analysis (SHA *5.16*), erfarenheter från exempelvis felrapporter (FRACAS *5.28*) samt materialinformation (materiallista/materialdeklaration). För EHA-analysen rekommenderas händelseträd och feleffektanalys, se *kapitel 8*.

Riskanalys för yttre miljö (EHA):

Det första steget i den miljöinriktade analysen (EHA) består i att identifiera ämnen som är potentiellt farliga för den yttre miljön. Utifrån ingångsdata beräknas hur stor skada som kan uppkomma vid en vådahändelse. Därefter görs en bedömning av sannolikheten för vådahändelsen för att kunna uppskatta olycksrisken enligt *H SystSäk del 1*. Det sista steget är att eliminera eller reducera risken för att uppfylla krav. Detta kan ske genom omkonstruktion,

införande av skyddsanordningar eller genom införande av handhavandeinstruktioner. Även emissioner förorsakade av nödsituationer, till exempel brand, ska beaktas.

Hänsyn tas till följande faktorer:

- det tekniska systemets form/tillstånd vid varje fas under livslängden
- kringutrustning som användas och dess påverkan på det tekniska systemet
- förväntad användningsmiljö och begränsningar
- abnorma miljöer som det tekniska systemet kan utsättas för.

Analysen ska:

- redovisa att lagkrav är uppfyllda
- redovisa att krav i beställningen är uppfyllda
- identifiera de olycksrisker som ska reduceras enligt krav i beställningen.

Analysen ska identifiera:

- Verksamheter som kan ge riskfyllda situationer. Vid vilka tidsperioder de inträffar och åtgärder som krävs för att minimera riskerna under dessa verksamheter/tidsperioder.
- Farliga material/ämnen som finns i det tekniska systemet, eller som kan bildas vid till exempel brand, fientlig attack med mera.
- Erforderliga ändringar på konstruktion av maskinvara/programvara/dokumentation, hjälpmedel, verktyg eller underhålls-/testutrustning för att eliminera eller kontrollera olycksrisker.
- Krav på säkerhetsanordningar och säkerhetsutrustning för att skydda yttre miljö vid vådahändelser.
- Varningar, instruktioner, skyltar, försiktighetsåtgärder och speciellt tillvägagångssätt vid till exempel brand.
- Krav på säkerhetsutbildning och krav på speciell behörighet/kompetens hos personal.

Analysen ska dokumentera systemsäkerhetsvärderingarna av de åtgärder som är aktuella för alla faser under det tekniska systemets livslängd. Exempel på analysmetoder framgår av *kapitel 8*.

Verksamhet avseende miljöpåverkan för normala (planerade) utsläpp

För utsläpp som bildas vid normal (planerad) användning, destruktion eller avveckling, ska farliga material/ämnen identifieras. Se RADS *5.34*. Detta kan ske genom att materialinformation tas fram samt att materialen granskas mot gällande lagstiftning. För emissioner vid användning och avveckling beräknas eller mäts dessa. Därefter jämförs dessa med lagstiftning och krav i beställning.

Koncession och annan tillståndspliktig verksamhet behandlas utanför H SystSäk. Dock kan underlag från EHA-aktiviteten även användas för detta.

Vid analys och granskning kan hänsyn tas till följande faktorer:

- Det tekniska systemets form/tillstånd vid varje fas under livslängden.
- Kringutrustning/verktyg som används och dess påverkan på det tekniska systemet.
- Förväntad användningsmiljö och begränsningar.

Analysen ska:

- Redovisa att lagkrav är uppfyllda.
- Redovisa att krav i beställningen är uppfyllda.
- Identifiera de farliga ämnen som kan ersättas med mindre farliga ämnen.

Analysens resultat ska dokumenteras.

Nedan finns en principbild för att få fram underlag avseende påverkan på den yttre miljön. Det ordinare systemsäkerhetsarbetet börjar med en av Försvarsmakten definierad verksamhet (dokumenterad i en SSMP enligt SSP *5.1*) med kravställning i TTEM *5.3*. DesignA omvandlar kraven från TTEM *5.3* till en RFP *5.4*. Leverantör definierar den planerade verksamheten i en SSPP *5.5* samt granskar både hälso- och miljöpåverkan av det tekniska sys-

temet (vid användning och avveckling) mot lagar och förordningar. Detta utgör underlag för säkerhetsanalyserna. Identifierade och behandlade risker dokumenteras i riskloggen samt resultatet av säkerhetsarbetet dokumenteras i en SAR *5.21*. Systemsäkerhetsutlåtandet (SCA *5.27*), som är baserat på SAR *5.21*, ligger till grund för systemsäkerhetsgodkännande (SS *5.31*) och centralt systemsäkerhetsbeslut (CSSB *5.33*). För att genomföra ett fullständigt systemsäkerhetsarbete fordras underlag från miljöverksamheten i form av materialinformation, återvinningsmanual och säkerhetsdatablad (SDB *[13]*).

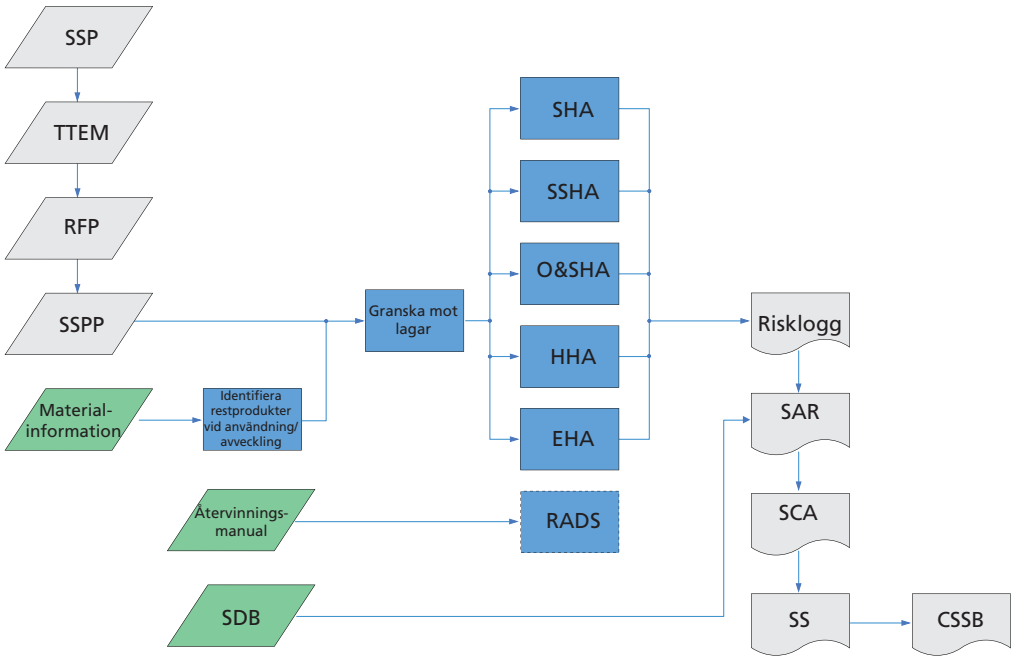


Bild 5:20 Miljörelaterade aktiviteter

5.19.3 Indata

En systembeskrivning, drift-/operationsprofil, samt oftast PHA *5.13*, SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, FRACAS *5.28*, HMI underlag *[14]* och materiallista/materialdeklaration erfordras för att genomföra en EHA.

5.19.4 Utdata

Riskanalys för yttre miljö (EHA) samt underlag till Risklogg (HTRR *5.9*).

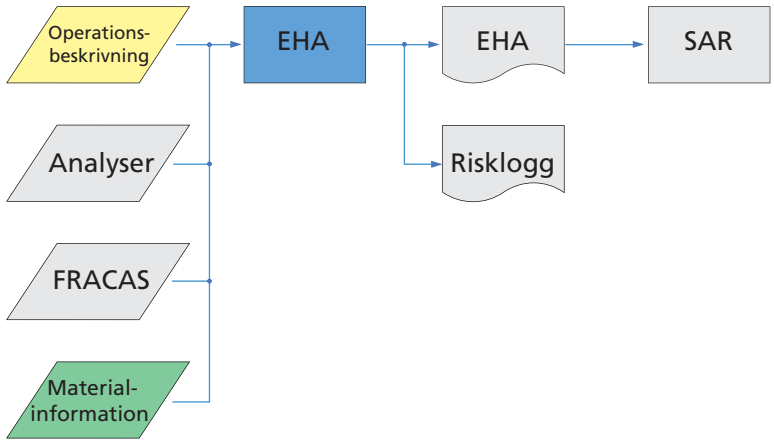


Bild 5:21 Riskanalys för yttre miljö (EHA)

5.20 Functional Hazard Assessment (FHA) – S22

5.20.1 Syfte

Att tidigt identifiera funktionellt relaterade olycksrisker för enskilda system eller för system som en del av system av system. FHA används för att identifiera och klassificera systemfunktioner (ut kritikalitetssynpunkt) och att identifiera funktionella fel. Klassificeringen används för att identifiera säkerhetskritiska funktioner (SCF *5.11*). Detta ger möjlighet att fördela kritikaliteter i en systemarkitektur, både funktionellt och fysiskt, till de olika elementen som utgör det tekniska systemet, såsom maskinvara, programvara eller HMI-delar. För definition av Säkerhetskritiska och Säkerhetsrelaterade funktioner/delar, se SCF *5.11*.

Genom att tidigt i en anskaffnings-/utvecklingsprocess tillämpa FHA erhålls möjlighet att identifiera de element/delar som ska analyseras vidare i den fortsatta analysverksamheten samt att identifiera säkerhetskritisk programvara för hantering enligt *kapitel 6*.

Motsvarande aktivitet finns i den civila standarden GEIA-STD-0010 Task 208 *[27]*. Notera att för luftfartsprodukter, vilka kräver godkännande av Transportstyrelsen, bör FHA baserad på Luftfartverkets regler användas. För flygplan och relaterad materiel finns en vägledning under *avsnitt 5.20.5*.

Denna aktivitet återfinns inte i tidigare utgåva av H SystSäk men är internationellt tillämpad, därför används det engelska namnet. Aktiviteten utförs främst av leverantör.

5.20.2 Aktivitetsbeskrivning

Leverantör ska genomföra och dokumentera en FHA för att tidig utföra en riskvärdering av ett koncept eller system.

Baserat på tillgängliga data, omfattande även underlag från felrapporter (FRACAS *5.28*) för liknande system, ska de identifierade funktionerna analyseras (omfattande indata, utdata, inter-

aktioner med andra system) för att fördela de identifierade felfunktionerna till de berörda delsystemen, samt att genomföra en allvarlighetsvärdering av dessa felfunktioner.

Som ett led i att åtgärda potentiella felfunktioner ska säkerhetskrav identifieras i kravspecifikationer, se SRCA *5.14*. Vidare identifieras konstruktiva åtgärder för att eliminera eller minska olycksriskerna till kravställd risknivå.

För att genomföra en FHA ska följande punkter utföras, identifieras och beaktas:

- Maskinvarukomponenter identifieras (den fysiska uppbyggnaden av det tekniska systemet med sina delsystem ner till större komponenter).
- Kritiska interaktioner/samverkan mellan de fysiska delsystemen. Både fysisk och funktionell samverkan beaktas.
- Funktionell beskrivning av samverkan mellan delsystem och komponenter genomförs.
- En listning av olycksrisker, funktionsbortfall och felfunktioner. I likhet med en feleffektsanalys (FMEA) ska troliga effekter och följdeffekter identifieras och beaktas.
- Värdera alla de identifierade olycksriskerna. Utvärderingen ska bara göras med hänsyn till effekt/konsekvens. Ingen numeriskutvärdering av sannolikheter ska göras i detta tidiga skede av analysverksamheten. Konsekvenser definieras enligt SSPP *5.5*.
- Identifiera säkerhetskritiska funktioner/egenskaper (både CIL och SIL) enligt SCF *5.11*.
- Värdera om de identifierade funktionerna kan införas i konstruktionen eller ej.
- Lista alla identifierade säkerhetskrav som ska införs i specifikationerna, se SRCA *5.14*. Om kraven uppfylls medför detta en minskad inträffandesannolikhet för vådahändelserna vilket speglas i de efterföljande analyserna (PHA *5.13*, SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18* och EHA *5.19*).

5.20.3 Indata

En koncept och systembeskrivning, driftprofil, samt oftast erfarenheter från felrapportering FRACAS *5.28*.

5.20.4 Utdata

En FHA-rapport utgör utdata från aktiviteten. Denna bör omfatta:

- En enklare systembeskrivning främst beskrivande de fysiska delarna samt identifierade funktioner.
- Resultat av FHA:
  - En nedbrytning av det tekniska systemet (även system av system) i funktioner och hur dessa är realiserade genom fysiska enheter. Formatet för en WBS (Work Breakdown Structure) kan användas.
  - En listning av alla systemfunktionerna.
  - En listning av alla säkerhetskritiska funktioner.
  - En beskrivning av hur säkerhetskritiska funktioner relaterar till programvaruarkitekturen, inkluderande exempelvis kritikalitetsnivåer.
  - En listning av alla identifierade säkerhetskrav.
- En FHA kan vidare generera:
  - en lista med olycksrisker för PHL *5.12*/PHA *5.13*
  - indata till FMEA eller FMECA
  - en metod för att verifiera felscenarier, se SAE ARP 4761 *[37]* och *avsnitt 5.20.5*.
  - identifiering av aktuell konstruktionsstatus för säkerhetskritiska interaktioner i det tekniska systemet.

Vidare ges indata till risklogg enligt HTRR *5.9* och SRCA *5.14*.

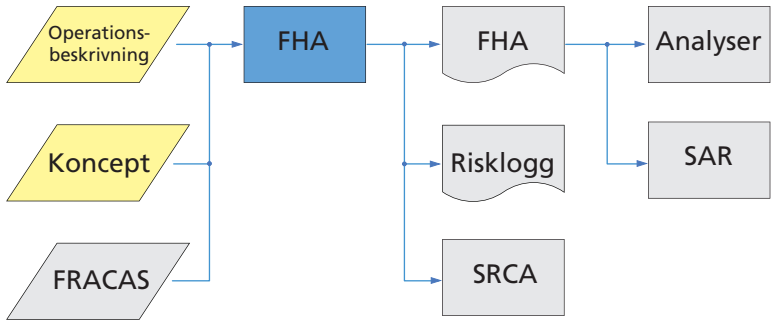


Bild 5:22 Functional Hazard Assessment (FHA)

5.20.5 FHA för civila flygburna system

Detta avsnitt beskriver aktiviteten FHA för civila flygburna system och beskrivningen är baserad på den civila standarden SAE ARP4761 (Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment) *[37]*.

5.20.6 Syfte

FHA definieras som en systematisk utvärdering av funktioner på komplett flygplan och delsystem för att identifiera felhändelser som dessa funktioner kan förorsaka. De identifierade felhändelserna klassificeras utifrån dess effekter (värsta konsekvens/olycksutfall).

FHA utförs tidigt både på komplett flygplans- och på delsystemnivå och är ett första steg att tidigt identifiera säkerhetskritiska funktioner och relaterade systemsäkerhetskrav. FHA ger på detta sätt ett underlag för att bygga robusta och feltoleranta farkoster/delsystem.

FHA ska fokusera på funktion för att så långt det är möjligt vara oberoende av realiseringen av funktionen.

5.20.7 Aktivitetsbeskrivning

Metodiken som föreskrivs i SAE ARP4761 *[37]* är densamma för både komplett flygplan och delsystem och kan sammanfattas enligt följande:

- Identifiera alla funktioner hos farkosten/delsystemet.
- Identifiera och beskriv funktionernas olika felhändelser. Beakta både enkelfel och multipla fel i normal och degraderade/avvikande tillstånd och miljöer. I händelse av att kombinationsfel av funktioner är allvarligare än de ingående funktionerna ska kombinationsfelet analyseras och föras upp som ett nytt unikt funktionsfel i FHA på komplett flygplansnivå.
- Utvärdera effekten (värsta konsekvensen/olycksutfall) av alla felhändelser som en funktion kan förorsaka genom att analysera möjliga/troliga skador på komplett flygplan, besättning, och passagerare).

  Erfarenhetsmässigt har det visats sig vara en fördel att även beakta möjliga riskreducerande åtgärder under analysen för att eliminera eller kontrollera felhändelserna som är säkerhetskritiska.
- Definiera och allokera systemsäkerhetskrav (kritikalitet/utvecklingsnivåer (DAL), redundans, oberoende felsannolikheter) utifrån resultatet från FHA av konstruktionen.
- Identifiera verifieringsmetod för att utvärdera kravuppfyllnad för definierade systemsäkerhetskraven.

FHA på komplett flygplansnivå är en kvalitativ utvärdering av en farkosts funktioner som har definierats i början av farkostens utveckling.

Notera: För att utföra en FHA på komplett flygplansnivå krävs det god kännedom och erfarenhet från liknande farkoster med liknande funktioner och därför rekommenderas konsultation och samråd med olika specialister inom berörda områden.

FHA på delsystemnivå är en kvalitativ utvärdering av funktioner hos ett delsystem i farkosten.

Notera: Målet med FHA på delsystemnivå är inte att identifiera och analysera fel i de maskinvaru- eller programvarukomponenter som är tänkt att bygga upp det nya alternativt modifierade delsystemet.

5.20.8 Indata

Indata till FHA på komplett flygplansnivå är:

- en lista med alla funktioner på komplett flygplansnivå
- farkostkrav och kundkrav.

Indata till FHA på delsystemnivå är:

- en lista med funktioner på delsystemnivå att beakta
- FHA på komplett flygplansnivå eller närmast högre delsystemnivå
- funktionella diagram som visar externa gränssnitt
- definierade konstruktionskrav och konstruktionsbeslut och motivering till dessa beslut.

5.20.9 Utdata

Följande information bör dokumenteras:

- beskrivning av aktuella driftfaser
- lista med de funktioner som har analyserats i FHA
- degraderade/avvikande tillstånd och miljöer identifierade under analys
- beskrivning av konsekvenser av felhändelser
- klassificering av effekten för respektive felhändelse
- identifierade olycksrisker för dokumentering i risklogg
- referenser till material som styrker och rättfärdigar analysen i FHA
- verifieringsmetoder för definierade systemsäkerhetskrav.

5.21 Safety Assessment Report (SAR) – Task 301

5.21.1 Syfte

Aktiviteten avser att utvärdera och sammanställa riskerna med det tekniska systemet före provning eller användning. För svenska förhållande utgör denna oftast underlag för att ett systemsäkerhetsutlåtande (SCA *5.27*) ska kunna lämnas.

5.21.2 Avvikelser

301.2.d (5): ”Material Safety Data Sheet” ersätts av SÄKERHETSDATABLAD (SDB) enligt Europarådets förordning (REACH) *[13]*.

301.3.1 c: Reglering av vem som ska underteckna SAR kan regleras i SSPP *5.5*. Undertecknandet av SCA *5.27* sker normalt av firmatecknare hos leverantör eller av denne speciellt utsedd person. Undertecknandet av SAR kan därför ske på lägre nivå.

5.21.3 Jämförbara aktiviteter/dokument

I Storbritannien används en motsvarande Safety Case Report (Def-Stan 00-56 *[43]*).

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 301, Safety Assessment Report. Denna skiljer sig marginellt och kan tillämpas som ett alternativ.

5.21.4 Ytterligare information

En användning av SAR är att redovisa kvarstående risker med det tekniska systemet vid användning, samt att uppskatta den relaterade numeriska risken. SAR kan även användas som informationskälla vid anskaffning av färdigutvecklade system.

En SAR kan dokumenteras enligt DI-SAFT-80102B, Safety Assessment Report *[9]*.

5.21.5 Indata

Som underlag för en SAR samlas all relevant säkerhetsdokumentation. Huvuddokument kommer från de genomförda analyserna 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* och relaterad Risklogg (Hazard Log) (se HTRR *5.9*) samt säkerhetsföreskrifter enligt SI *5.25* och säkerhetsdatablad (SDB). De olika underlagen för SAR kan inarbetas i SAR eller refereras till från SAR.

5.21.6 Utdata

Safety Assessment Report (SAR) som utgör underlag för systemsäkerhetsutlåtandet (SCA *5.27*).

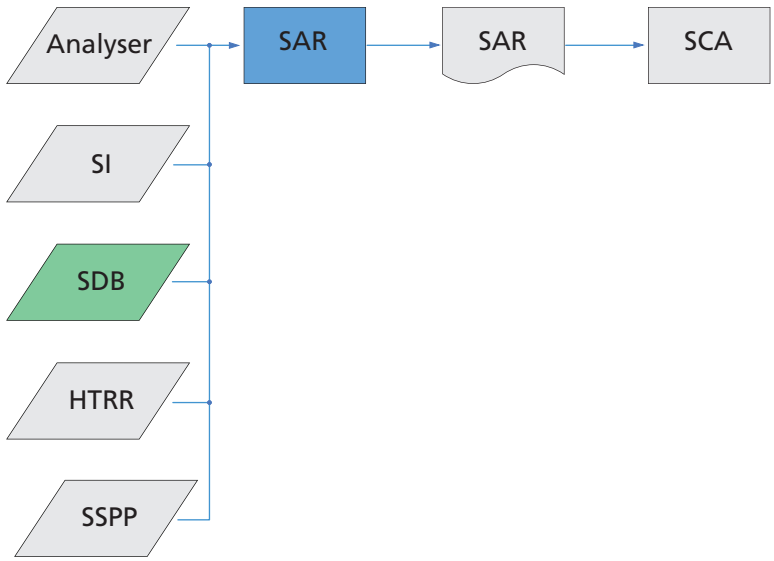


Bild 5:23 Safety Assessment Report (SAR)

5.22 Test and Evaluation Safety – Task 302

Ej tillämpbart för svenska förhållanden. Ersätts av krav från provande myndigheter/instanser.

5.23 Safety Review (SR) – Task 303

5.23.1 Syfte

Det fullständiga namnet på aktiviteten är ”Safety Review of Engineering Change Proposals; Specification Change Notices; Software Problem Reports; and Request for Deviation Waiver” (ECP/SCN/SPR/PTR/STR). Denna titel har förkortats till Safety Review (SR).

Aktiviteten avser att utvärdera ändringar och avvikelser ur säkerhetssynpunkt.

5.23.2 Avvikelser

303.3.1 b, c, d: Detta kan även regleras i Configuration Management Plan (CM-Plan) eller i SSPP *5.5*.

5.23.3 Jämförbara aktiviteter/dokument

För programvara, se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 303, Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Request for Deviation Waiver. Denna skiljer sig marginellt och kan tillämpas som ett alternativ.

5.23.4 Ytterligare information

Varje ändring måste granskas så att nya risker inte uppstår vid införandet av ändringen. Klassificeringen av ändringar måste definieras i konfigurationsplan eller motsvarande (säkerhetsrelaterade ändringar är oftast klass I).

Ett ändringsförslag kan dokumenteras enligt DI-SAFT-80103A, Engineering Change Proposal *[10]* och en avvikelse enligt DI-SAFT-80104A, Waiver or Deviation System Safety Report *[11]*.

5.23.5 Indata

Ett underlag för ändringsförslag är felrapporter (FRACAS *5.28*) eller resultat av analyser såsom SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19* och relaterad Risklogg (Hazard Log), se HTRR *5.9*.

5.23.6 Utdata

Rapporterna utgör ändringsförslag och avvikelserapporter (ECP/SCN/SPR/PTR/STR).

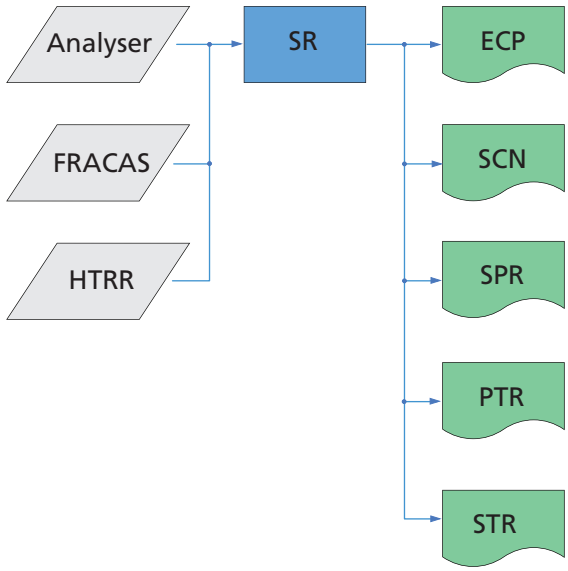


Bild 5:24 Safety Review (SR)

5.24 Safety Verification (SV) – Task 401

5.24.1 Syfte

Aktiviteten avser att definiera och genomföra den verifiering (provning, analys, granskning och demonstrationer) som behövs för att kunna verifiera säkerheten.

5.24.2 Avvikelser

401.2.a: ”Catastrophic hazards” ersätts för svenska förhållande med VÅDAHÄNDELSER ELLER FARLIGA TILLSTÅND SOM KAN GE SKADEKLASS 1. ”Marginal and Negligeable hazards” ersätts av ÖVRIGA VÅDAHÄNDELSER ELLER FARLIGA TILLSTÅND.

5.24.3 Jämförbara aktiviteter/dokument

För programvara, se *kapitel 6*.

Den civila standarden GEIA-STD-0010 *[27]* har en likvärdig aktivitet, Task 401, Safety Verification. Denna skiljer sig marginellt och kan tillämpas som ett alternativ. GEIA-STD-0010 har en utförligare beskrivning av vilka data som kan ingå i en SV (401.2.2).

5.24.4 Ytterligare information

Många av säkerhetskraven måste verifieras med analys och simuleringar. Enbart provning är oftast otillräckligt. Vid konstruktionsändringar måste förnyad verifiering ske. Provning utgör ofta ett stöd till genomförd analys. Genomförd provning kan dokumenteras enligt DI-SAFT-80102B, Safety Assessment Report *[9]* eller i separata provningsrapporter.

5.24.5 Indata

Underlag för säkerhetsverifieringen är analyser såsom SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19* samt relaterad Risklogg (Hazard Log) HTRR *5.9* och SRCA *5.14*.

5.24.6 Utdata

Rapport från verifiering av säkerhetskrav utgör ett underlag för den totala verifieringen av det tekniska systemet samt indata till SAR *5.21*.

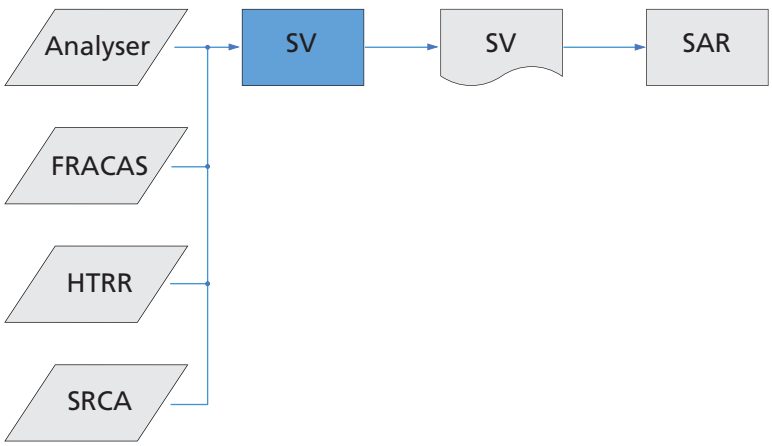


Bild 5:25 Safety Verification (SV)

5.25 Säkerhetsföreskrifter (SI) – S41

5.25.1 Syfte

Att ge ett komplement till vidtagna konstruktionsåtgärder för att förhindra felaktigt hantering av det tekniska systemet. Grundförutsättningar för upprättandet av dessa är analyserna SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19*, där det tekniska systemets konstruktion och det förväntade användandet har analyserats. Aktiviteten genomförs oftast av leverantör.

5.25.2 Aktivitetsbeskrivning

Det är oftast omöjligt att konstruera system, som är säkra oavsett hur de hanteras. För att öka säkerheten vid användandet kan vissa säkerhetsföreskrifter behöva anges. Då dessa ska inarbetas i instruktioner som finns i manualer och annan säkerhetsrelaterad information, anges de lämpligen uppdelade på de olika hanteringsfaserna som är aktuella för det tekniska systemet.

Som exempel anges här några punkter att beakta för olika hanteringsfaser:

- förvaring:
  - max och min förvaringstemperatur
  - max och min luftfuktighet
  - max temperaturändringshastighet vid förvaring
  - max livslängd vid ovanstående klimat
  - max staplingshöjd
  - max elektromagnetisk bestrålning
- transport
  - max acceleration eller tillåtna transportsätt
  - tillåtna transportförpackningar
  - maximala transporttider
  - krav på speciell transportsäkring av lasten

- handhavande
  - förpackningskrav vid handhavande
  - max tider för förvaring i bruten förpackning
  - krav på speciella handhavandeprocedurer
  - för programvara, se *kapitel 6*
- användning
  - begränsningar i användningssätt
  - max och min temperatur
  - max och min luftfuktighet
  - riskområden för splitter, ljudtryck, värme, elektromagnetisk strålning, klämning med mera.
- avveckling
  - begränsningar i avvecklingsmetoder
  - krav på hantering av restprodukter.

Målet vid utveckling av ett system ska vara att konstruera detta så att säkerhetsföreskrifterna kan minimeras. De eventuella säkerhetsföreskrifterna måste vara utarbetade inför systemsäkerhetsutlåtandet (SCA *5.27*).

5.25.3 Indata

Underlag för säkerhetsinstruktionerna är analyser såsom SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19*.

5.25.4 Utdata

Säkerhetsföreskrifter (SI) som utgör underlag för SCA *5.27* och TSR *5.32*.

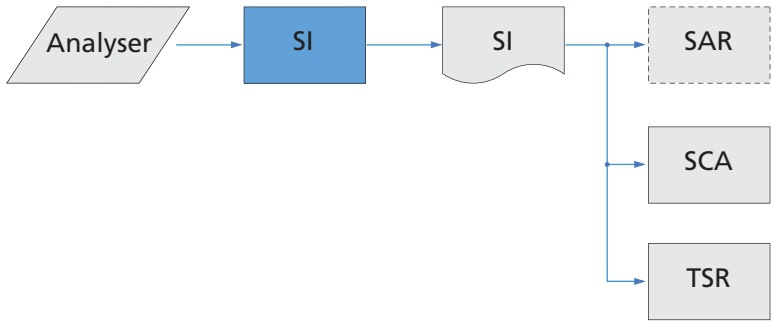


Bild 5:26 Säkerhetsföreskrifter (SI)

5.26 Safety Compliance Assessment – Task 402

Denna aktivitet regleras helt av aktiviteten systemsäkerhetsutlåtande (SCA) – S42 *5.27*.

5.27 Systemsäkerhetsutlåtande (SCA) – S42

5.27.1 Syfte

Att redovisa leverantörs ställningstagande till det tekniska systemets säkerhet. SCA ingår även i det underlag på vilket DesignA ger ett systemsäkerhetsgodkännande (SS *5.31*). Systemsäkerhetsutlåtandet kan vara en aktivitet vid beställningens avslutande. I systemsäkerhetsutlåtande ska även genomgång av att gällande lagstiftning uppfylls vara dokumenterad.

Det sammanställda underlaget för utlåtandet dokumenteras oftast i en Safety Assessment Report (SAR *5.21*).

5.27.2 Aktivitetsbeskrivning

Systemsäkerhetsutlåtandet utgör en sammanfattning av utfört systemsäkerhetsarbete, genomgång av gällande lagstiftning samt ett ställningstagande från utvecklande leverantör att det tekniska systemets säkerhet är acceptabel för användning, förutsatt att angivna säkerhetsföreskrifter följs (SI *5.25*).

För provning/försök vid Försvarsmaktens anläggningar och med Försvarsmaktens personal gäller arbetsmiljölagstiftningen, varför den verksamheten inte behandlas under SCA aktiviteten.

SCA baseras på de aktiviteter som har avtalats i System Safety Program Plan (SSPP), där analyserna (SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19*, FHA *5.20* och de delar av RADS *5.34* som genomförts), säkerhetsföreskrifterna (SI *5.25*), erfarenheter från felrapporter (FRACAS *5.28*) och utvärderingen av Safety Verification (SV *5.24*) är av central betydelse. Resultaten av dessa framgår av SAR *5.21*.

Som underlag för systemsäkerhetsutlåtandet ligger alla de säkerhetsaktiviteter som genomförts under det tekniska systemets utveckling. Dessa aktiviteter dokumenteras efterhand som de genomförs. I systemsäkerhetsutlåtandet hänvisas till dessa dokument eller görs ett sammandrag av aktiviteterna som införs i rapporten.

Systemsäkerhetsutlåtandet kan i princip omfatta följande:

- Redovisning av de säkerhetskriterier och krav som använts vid det tekniska systemets framtagning, hur risker har identifierats, klassificerats och behandlats för att elimineras eller reducerats för att erhålla en tolerabel säkerhetsnivå.
- Identifiering och redovisning av att gällande lagstiftning är uppfylld.
- Analyser och provningar som utförts för att identifiera olycksrisker och deras orsaker.
- Redovisning av de åtgärder som vidtagits för att eliminera eller begränsa orsakerna till olycksriskerna. Eventuellt ställningstagande från System Safety Working Group (SSWG *5.8*) vad gäller åtgärdernas tillräcklighet.
- Redovisning av återstående risker samt åtgärder som erfordras för att uppnå tolerabel säkerhet, exempelvis säkerhetsföreskrifter och utbildning av personal.
- Redovisning av de provningar och analyser, med förutsättningar, som ligger till grund för verifieringen av säkerhetskraven.
- Redovisning av varje vådahändelse eller farligt tillstånd, som kan tänkas ske under såväl normal användning som onormala och abnorma betingelser, tillsammans med rekommendationer och föreskrifter som ger tolerabel säkerhet.

- Redovisning av de miljö- och hälsofarliga ämnen/material som finns i det tekniska systemet som människor eller miljö riskerar att exponeras för vid vådahändelser eller farliga tillstånd under användning, underhåll eller avveckling. Redovisning av risker för människors hälsa, egendom eller yttre miljö tillsammans med föreskrifter, varningar och procedurer som förhindrar att skada uppstår.
- För kemiska produkter ska aktuellt säkerhetsdatablad (SDB *[13]*) finnas tillgängligt.
- I systemsäkerhetsutlåtandet ska alltid ingå ett entydigt uttalande från leverantör som, mot bakgrund av ovan redovisade åtgärder, anger att det tekniska systemet är säkert under givna förutsättningar.
- För det tekniska systemets programvarudelar redovisas verifieringen, som i ökande detaljeringsgrad visar, att de programvarusäkerhetskrav som gäller leverantörs personal, process, produkt samt produktionsmiljö är uppfyllda. En kravförteckning utgör ett bra underlag för systemsäkerhetsutlåtandet. Ur denna framgår i vilken grad kraven verifierats, motivering till ofullständiga verifieringar samt för uteslutna krav, förslag till åtgärder vid ofullständig kravtäckning med mera. Exempel på det senare kan vara produkt-/processförbättringar, utbildning samt säkerhetsföreskrifter.

Systemsäkerhetsutlåtande ska undertecknas av firmatecknare hos leverantör eller någon av denne delegerad. Vem som undertecknar kan regleras i System Safety Program Plan (SSPP *5.5*).

5.27.3 Indata

Underlag för systemsäkerhetsutlåtandet är SAR *5.21* samt kan vara FRACAS *5.28* och SV *5.24*.

5.27.4 Utdata

Systemsäkerhetsutlåtande (SCA) som utgör underlag för systemsäkerhetsgodkännandet (SS *5.31*). Exempel på systemsäkerhetsutlåtande (SCA) framgår av *bilaga 1*.

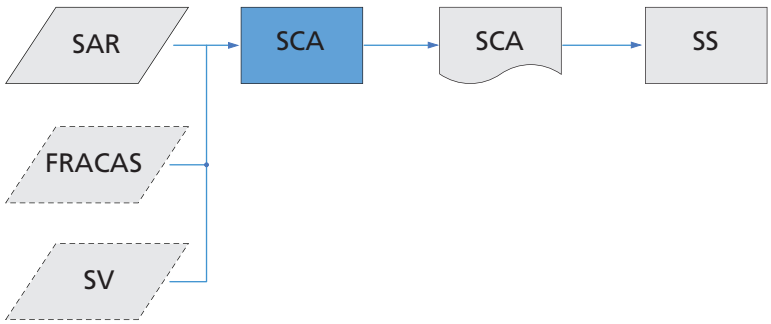


Bild 5:27 Systemsäkerhetsutlåtande (SCA)

Se exempel på SCA i *bilaga 1*. Exemplet finns som fil i H SystSäk CDR.

5.28 Felrapporteringssystem (FRACAS) – S43

5.28.1 Syfte

Att återföra säkerhetsrelaterad information till ansvariga, för att förbättra det tekniska systemets systemsäkerhet.

Felrapporteringssystem bör finnas från första provning/hantering tills det tekniska systemet avvecklas. Informationen kan användas för både det aktuella tekniska systemet och för likartade tekniska system som exempelvis använder samma delsystem. Underlaget från feluppföljningen utgör en del av underlaget för Safety Assessment Report (SAR *5.21*) och systemsäkerhetsutlåtandet (SCA *5.21*). Även analyserna (SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19* och FHA *5.20*), är mycket beroende av att information återförs, dels för att vinna erfarenhet, dels för att analysera effekten av eventuella ändringar som kan föranledas av felrapporteringen. Felrapporteringen övervakas lämpligen av arbetsgrupperna SSWG-1 och SSWG-2, vilka även har att föreslå korrigerande åtgärder. Aktiviteten genomförs av Försvarsmakten, DesignA och leverantör.

5.28.2 Aktivitetsbeskrivning

I första hand används ett i Försvarsmakten befintligt felrapporteringssystem. Finns ej sådant måste ett särskilt felrapporteringssystem upprättas. Det är bra om flera intressenter tillgodoses med ett och samma rapporteringssystem, exempelvis kan både säkerhets- och underhållsintressenter använda samma data. Avsikten med denna aktivitet är att säkerställa att ett, helst standardiserat, rapporteringssystem upprättas och hålls vid liv under det tekniska systemets hela livslängd.

Rapporteringssystemet ska förse alla intressenter med information oavsett i vilken fas det tekniska systemet befinner sig. Därför måste en ansvarig instans (Försvarsmakten, DesignA eller leverantör) utses att driva och förvalta informationen och rapporte-

ringen. Under utveckling och anskaffning då leverantör oftast svarar för rapporteringssystemet, bör även arbetsgrupper för systemsäkerhet (SSWG-1/SSWG-2) delges berörd information.

Eftersom den ”mänskliga faktorn” idag vanligen är en betydande faktor vid alla typer av tillbud och olyckor är det viktigt att alla tillbud där människan direkt eller indirekt har påverkat skeendet, rapporteras.

Vissa grundläggande förutsättningar måste fastställas innan felrapporteringssystemet utformas:

- Ansvarig för att upprätta och upprätthålla felrapporteringssystemet.
- Rapporteringsvägar under olika faser i det tekniska systemets livslängd, inkluderande återmatning till rapportförfattarna.
- Den som utför analys och beslut att införa korrigerande åtgärd i det tekniska systemet.
- Innehållet i rapporteringsunderlaget och format för rapporteringen.
- Hur informationen avses att värdesäkras för kommande system.

Viss grundläggande information måste alltid återfinnas i felrapporteringssystemet:

- Det tekniska systemets identitet
- Konfiguration av det tekniska systemet och dess delar
- Operations-/användningsbetingelser vid felets uppkomst
- Felets/tillbudets art och omfattning
- Uppgift om vem som uppmärksammade felet/tillbudet, för att kunna skaffa kompletterande information. Anomyma rapporter ger inte den möjlighten

All existerande rapportering måste användas och kompletteras så att den kan utvärderas ur systemsäkerhetssynvinkel. För att göra detta möjligt erfordras att ordinarie och existerande rapportering så långt möjligt svarar på följande tilläggsfrågor:

- Skadades person eller fanns risk för personskada?
- Skadades materiel/egendom eller fanns risk för materiel-/egendomsskada? Avser även det tekniska systemet självt.
- Skadades yttre miljön eller fanns risk för miljöskada?

Efter att felet har rapporterats ska en analys ske där felorsaken ska härledas till fysisk eller operativ betingelse. En undersökning bör ske om felet även kan förekomma i andra system än det system som felrapporten avser.

Felorsaken bör verifieras så att rätt felorsak har identifierats. Korrigerande åtgärd bör beslutas och införas. Efter eventuell modifiering av det tekniska systemet måste uppgifter om det tekniska systemets konfiguration ändras.

För att inga felrapporter ska lämnas utan åtgärd, ska, då fall är avslutat, åtgärd noteras på eller i anslutning till felrapporten eller i speciell åtgärdsrapport.

5.28.3 Resulterande rapport

Felrapporter och åtgärdsrapporter som utgör indata till risklogg (se HTRR *5.9*).

Underlag från feluppföljning utgör en del av underlaget för Safety Assessment Report (SAR *5.21*) och systemsäkerhetsutlåtande (SCA *5.27*). Även analyserna (SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19* och FHA *5.20*) är beroende av denna rapportering.

5.28.4 Indata

Underlag för FRACAS är felrapporter och avvikelserapporter av olika slag.

5.28.5 Utdata

Åtgärdsrapporter utgör indata till Risklogg (se HTRR *5.9*).

Underlaget från feluppföljningen utgör en del av underlaget för Safety Assessment Report (SAR *5.21*) och systemsäkerhetsutlåtandet (SCA *5.27*). Även analyserna SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19* och FHA *5.20* är beroende på rapporteringen.

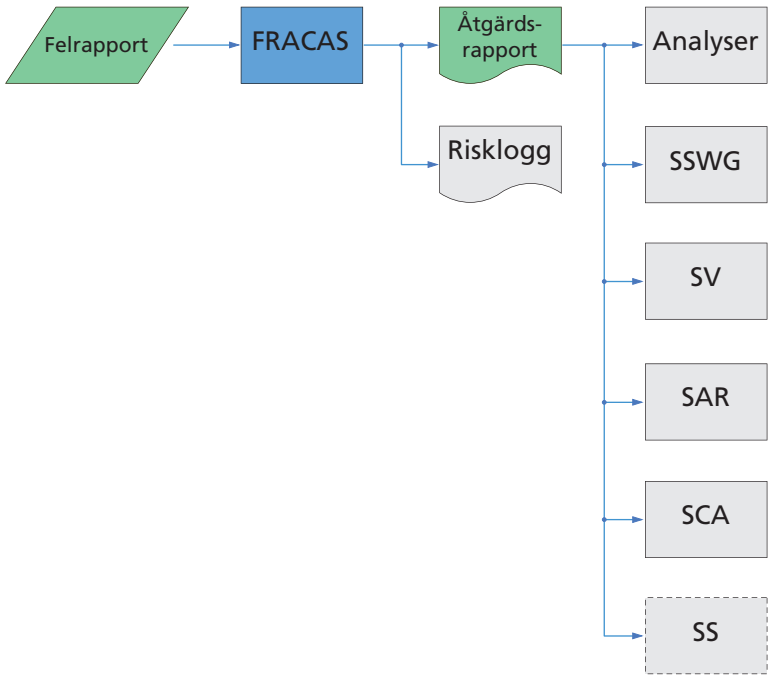


Bild 5:28 Felrapporteringssystem (FRACAS)

5.29 Explosive Hazard Classification and Characteristics – Task 403

Denna aktivitet regleras helt av H VAS *[24]*.

5.30 Explosive Ordnance Disposal Source Data – Task 404

Denna aktivitet regleras helt av H VAS *[24]*.

5.31 Systemsäkerhetsgodkännande (SS) – S51

5.31.1 Syfte

Syftet med denna aktivitet är att formellt godkänna systemsäkerheten hos utvecklat eller anskaffat system. Systemsäkerhetsgodkännandet (SS) är ett formellt beslut från DesignA. Beslutet innebär att av Försvarsmakten ställda systemsäkerhetskrav, inklusive krav på olycksrisk, är uppfyllda, att gällande lagar och förordningar samt övriga tillämpliga bestämmelser har iakttagits.

Systemsäkerhetsgodkännandet kan innehålla krav säkerhetsföreskrifter som ska iakttas. Systemsäkerhetsgodkännande för Provturskommando (PTK) benämns Säkerhetsintyg.

Indata för denna aktivitet är vid DesignA bedrivet systemsäkerhets- och granskningsarbete samt leverantörs systemsäkerhetsutlåtande (SCA *5.27*).

Systemsäkerhetsgodkännandet överlämnas av DesignA till Försvarsmakten som grund för centralt systemsäkerhetsbeslut (CSSB *5.33*).

5.31.2 Aktivitetsbeskrivning

Som ett led i utveckling och anskaffning granskas säkerheten hos det tekniska systemet fortlöpande vid System Safety Program Review (SSPR *5.7*). Antalet säkerhetsgenomgångar regleras i System Safety Program Plan (SSPP *5.5*). Samråd kan eventuellt tas med

DesignA:s rådgivningsgrupp för systemsäkerhet (i det fall att sådan är organiserad vid aktuell tidpunkt). Leverantörs systemsäkerhetsutlåtande (SCA *5.27*) granskas när detta överlämnas.

Baserat på dessa samlade granskningar och DesignA:s egna säkerhetsaktiviteter kan beslut om systemsäkerhetsgodkännande fattas. Systemsäkerhetsgodkännandet innebär att DesignA godkänner det tekniska systemet från systemsäkerhetssynpunkt.

DesignA:s säkerhetsaktiviteter, vilka är grund för beslut om systemsäkerhetsgodkännande, utgörs av:

- granskning av leverantörs systemsäkerhetsverksamhet
- granskning av analysrapporter
- granskning av risklogg
- granskning av leverantörs systemsäkerhetsutlåtande (SCA *5.27*
- kontroll av att underlag för handhavandeinstruktion finns
- kontroll av att underlag för säkerhetsföreskrifter (SI *5.25*) finns
- kontroll av att det har angivits vad som behöver följas upp, respektive hur befintliga rapporteringssystem ska tillämpas
- i förekommande fall (visst vapen) kontroll av att förteckning över vilken ammunition som är godkänd att skjutas med vapnet, är framtagen.

Genomförd granskning enligt ovan dokumenteras i granskningsrapporter. Utförande av granskning beskrivs i H SystSäk del 1.

Framtagning av system är som regel en komplex process under lång tid. Processen innehåller ofta flera moment av successiva provningar respektive materielförsök innan serieexemplar kan överlämnas till Försvarsmakten.

Det är produktledare hos DesignA som ska ha erforderlig kunskap om det tekniska systemets risker. Före varje åtgärd med det tekniska systemet avseende provning respektive försök ska denne beskriva det tekniska systemets kvarstående risker vid avsedd verksamhet. Det tekniska systemets konfiguration, kvarvarande risker, avsedd verksamhet och eventuella restriktioner vid avsedd

verksamhet, beskrivs i ett systemsäkerhetsgodkännande för avsedd verksamhet. Detta systemsäkerhetsgodkännande ska överlämnas till den som uppdras att genomföra avsedd verksamhet.

Exempel på tillfällen när systemsäkerhetsgodkännanden ska tas fram är vid:

- leverans till Försvarsmakten av färdigt tekniskt system
- leverans till Försvarsmakten av tekniskt system enbart avsett för visst försök
- överlämning till provningsenhet av tekniskt system avsett för viss provning
- överlämning till chef Provturskommando (PTK) av tekniskt system som utgörs av ett fartyg (före inledning av provturperiod.

  Systemsäkerhetsgodkännande motsvaras här av säkerhetsintyg.

Före varje överlämning till Försvarsmakten av tekniskt system (såväl färdigt som avsett för visst försök) ska systemsäkerhetsgodkännande finnas. Det är dock tillräckligt att systemsäkerhetsåtgärderna enligt ovan begränsas till den verksamhet och de förhållanden under vilka det tekniska systemet i varje enskilt fall avses användas.

Systemsäkerhetsgodkännande för vapen och ammunition

Ammunitionsobjekt är ett särskilt farligt tekniskt system som systemsäkerhetsmässigt alltid ska hanteras i två olika avseenden:

- I sin egenskap av ammunition, ofta avsett för visst eller vissa vapen eller annan specificerad användning (jämför till exempel stridsvagnsmina som är avsedd att användas självständigt eller i särskild läggningsutrustning). Härvid avses att ammunitionen är tillräckligt säker under avsedd användning i avsett vapen respektive under avsedd användning om denna ska kunna ske fristående.

- I sin egenskap av fristående transport- och förvaringsobjekt. Objekt består alltid av förpackning /transport- och förvaringsemballage med vissa specificerade egenskaper och innehållande ett visst antal ammunitionsenheter. Kraven på objektet består i att ammunitionen i sitt emballage ska vara tillräckligt säker när den utsätts för avsedd hantering i avsedd miljö.

Båda dessa aspekter ska täckas in av det separata systemsäkerhetsgodkännande som DesignA alltid ska ta fram för varje enskilt ammunitionsobjekt.

Systemsäkerhetsgodkännande för tekniskt system inför provning

Systemsäkerhetsgodkännandet baseras på en säkerhetsanalys med inriktning mot avsedd provning, konstruktionsgranskning samt en dokumentsammanställning för det tekniska systemet.

Säkerhetsintyg för tekniskt system fartyg inför provturskommando

Nya fartyg byggs eller större modifieringar av fartyg genomförs ofta i så korta serier att det inte är rimligt att ta fram prototyper för utprovning. Viss utprovning av delsystem kan göras separat, men i huvudsak måste utprovningen genomföras med seriefartyg, mest omfattande med det första fartyget i serien.

Fartygsutprovningen indelas vanligen i följande tre faser:

- verkstadsprovturer, byggnadsvarvets egen kontroll
- leveranskontroll, DesignA:s kontroll av att fartyget uppfyller krav enligt beställningen
- systemprov, DesignA:s kontroll av att fartyget uppfyller i TTEM *5.3* ställda krav.

Under samtliga tre utprovningsfaser ställer Försvarsmakten besättning till varvets respektive DesignA:s förfogande. För att lösa uppgiften inrättas ett särskilt provturskommando. Till PTK kommenderas personal med erfarenhet från liknande fartygstyper.

För att bland annat ge personalen så goda kunskaper som möjligt om den nya fartygstypen, upprättas PTK innan utprovningen planeras att starta. Under tiden vid byggnadsvarvet tjänstgör personalen huvudsakligen såsom biträden åt DesignA.

Under utprovningsfaserna ingår det också i PTK:s uppgifter att, parallellt med själva utprovningen, ta fram den dokumentation som erfordras och som inte ingår i DesignA:s leverans.

När systemprovningen har genomförts, överlämnas fartyget från DesignA till Försvarsmakten.

Vid fartygsutprovningen enligt denna princip, leds PTK-perioden direkt av designansvarig organisation varför centralt systemsäkerhetsbeslut (CSSB *5.33*) respektive Beslut om användning (BOA) ej erfordras. (Dessa senare beslut krävs först i samband med att första fartyget överlämnas från DesignA till Försvarsmakten.)

Före inledning av PTK-period erfordras dock att DesignA tar fram ett Säkerhetsintyg för aktuellt tekniskt system (fartyg).

I ett särskilt säkerhetsintyg för PTK ska DesignA, för varje åtgärd som avses genomföras med det tekniska systemet (fartygets) under PTK minst specificera:

- det tekniska systemets (fartygets) konfiguration
- kvarvarande risker
- erforderliga restriktioner.

Systemsäkerhetsintyget ska överlämnas till chefen PTK.

En förutsättning för att utfärda ett säkerhetsintyg för aktuellt tekniskt system (fartyg) inför PTK är att DesignA erhållit Militära säkerhetsinspektionens samråd. Dessutom ska fartyget före nyttjande ha godkänd sjövärdighetsbesiktning av Marinens Fartygsinspektion, MFI. Sjövärdighetsbesiktningen är inget krav för att utfärda säkerhetsintyg. MFI kan begära att få se säkerhetsintyget vid sjövärdighetsbesiktningen.

Systemsäkerhetsmeddelande

I de fall DesignA har uppdragits att för visst tekniskt system ta fram ett systemsäkerhetsgodkännande, men det tekniska systemet inte innehåller ställda krav på risk, lämnas rapport i form av ett säkerhetsmeddelande.

5.31.3 Indata

Indata till aktiviteten systemsäkerhetsgodkännande utgörs bland annat av:

- systemsäkerhetsutlåtande, SCA *5.27*
- SAR *5.21* med provningsresultat och analysrapporter
- DesignA:s granskningsrapporter
- eventuellt FRACAS *5.28*.

5.31.4 Utdata

Utdata från aktiviteten systemsäkerhetsgodkännande utgörs av dokumentet systemsäkerhetsgodkännande. Ibland kan systemsäkerhetsgodkännandet ha vissa begränsningar och till exempel enbart avse ammunition, specificerad provning av visst tekniskt system, eller omfatta den verksamhet som helt eller delvis avses ske under formen PTK. Säkerhetsgodkännandet undertecknas av DesignA utsedd Produktchef.

Dokumentet utgör underlag för centralt systemsäkerhetsbeslut (CSSB *5.33*). Exempel på systemsäkerhetsgodkännande (SS) och säkerhetsintyg framgår av *bilaga 1*.

I de fall då tekniskt system inte innehåller ställda krav på risk, utfärdas inget systemsäkerhetsgodkännande utan istället lämnas rapport i form av ett systemsäkerhetsmeddelande.

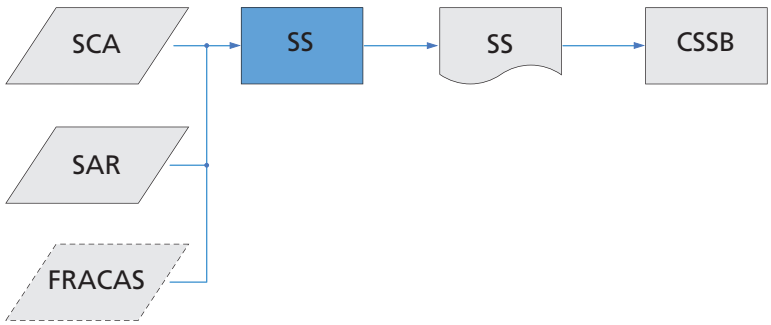


Bild 5:29 Systemsäkerhetsgodkännande (SS)

Exempel på systemsäkerhetsgodkännande och säkerhetsintyg finns i *bilaga 1* och som filer i H SystSäk CDR.

5.32 Användarmanualer och utbildning (TSR) – S52

5.32.1 Syfte

Att fastställa och utge de instruktioner som fordras för ett säkert handhavande av tekniskt system. Indata för aktiviteten är systemsäkerhetsgodkännandet (SS *5.31*) från DesignA med underlag från säkerhetsföreskrifter (SI *5.25*). Användarmanualer och utbildning (TSR) är en förutsättning för centralt systemsäkerhetsbeslut (CSSB *5.33*). Användarmanualer samt bestämmelser för utbildning utarbetas genom Produktionschef i HKV försorg med hjälp av berörd stridsskola (eller motsvarande) eller av DesignA på beställning.

5.32.2 Aktivitetsbeskrivning

Manualer med säkerhets- och skyddsinstruktioner

Säkerhets- och skyddsinstruktioner ska upprättas och delges berörda användare före det att utbildning eller handhavande sker. Underlag för instruktionerna framgår av säkerhetsföreskrifter (SI *5.25*).

Hantering innebär allt handhavande från tillverkning till slutanvändning respektive avveckling. Detta innefattar bland annat utveckling, förvaring, transport, handhavande, användning, drift, underhåll och avveckling. Hanteringsinstruktioner ska kontinuerligt tas fram för de olika faserna under utvecklingen fram till slutliga bestämmelser, vilka ska införas i SäkI *[42]* och andra skyddsinstruktioner.

Uppdragsansvarig inom DesignA är behjälplig för framtagning av underlag för användnings- och säkerhetsinstruktioner.

Säkerhetsinstruktioner bör innehålla:

- Bestämmelser för handhavande och underhåll.
- Bestämmelser för utbildning och övrig verksamhet med det tekniska systemet.
- Bestämmelser för förvaring och transport av farlig materiel under övning.
- Bestämmelser för förrådshantering och transport (vid materieldirigering, modifiering, FN-uppdrag med mera).
- Bestämmelser för åtgärder vid olyckor och tillbud samt utredningar vid dessa.

Säkerhetsinstruktioner kan framgå av:

- bruksanvisning och bilder som följer materiel och/eller utdelas till användare i samband med grund- och repetitionsutbildning
- materielbeskrivningar och instruktionsbok, som ger en fullständig beskrivning av materielen. Fördelas till förband och skolor
- reparationsbok
- instruktionsfilm
- bestämmelser för förvaring och transport av farliga varor under övning.

Sådana instruktioner, som är av avgörande betydelse för säkerheten ska inarbetas i SäkI *[42]*. Denna publikation nytrycks som regel vartannat år. Vid behov utges ändringar/kompletteringar. Övriga publikationer såsom truppslagsreglementen som gäller i strid, uppdateras vid behov. Det ska dock på sikt alltid råda överensstämmelse mellan SäkI *[42]* och motsvarande andra säkerhetsinstruktioner.

Handhavandet av materielen framgår av vederbörliga reglementen, instruktioner och beskrivningar. I vissa fall varnas också för sådana felaktigheter i handhavandet, som medför särskilda risker.

I SäkI *[42]* ingår ej bestämmelser för det exercismässiga handhavandet av materielen även om dessa i sig innebär åtgärder, som är vidtagna från säkerhetssynpunkt.

Säkerhetsinstruktioner för vapen och ammunition med mera (SäkI *[42]*) är gemensamma för Försvarsmakten. De består av en gemensam del, en del som vänder sig till förvaltningsansvariga chefer samt därutöver ett antal delar för olika vapentyper med mera. Böckerna innehåller både tvingande bestämmelser och råd. Uttrycket SäkI *[42]* används som sammanfattande benämning på hela serien. Bestämmelserna i SäkI *[42]* gäller vid utbildning i fred, under beredskapstillstånd samt vid utbildning i krig då övningen inte är direkt förberedelse för stridshandling.

Föreskrifter för transport och förvaring

I samband med centralt systemsäkerhetsbeslut (CSSB *5.33*) av förnödenhet eller system som innehåller explosivämne fastställer MSB klassificeringskod (ADR *[1]*) samt förvaringskod (F-kod enligt IFTEX *[19]*).

Utbildning

Avsikten är att utbilda användaren så att denne på ett säkert och avsett sätt kan hantera det tekniska systemet (följer utgivna användarmanualer med säkerhets- och skyddsinstruktioner).

Utvecklande leverantör lämnar förslag till utbildning. Detta framgår av säkerhetsföreskrifter (SI *5.25*) och eventuella utbildningsplaner.

I samband med truppförsök utarbetar, fastställer och utger truppslagscenter (eller motsvarande) utbildningsbestämmelser.

5.32.3 Indata

Indata till aktiviteten utgörs av säkerhetsinstruktioner, SI *5.25*.

5.32.4 Utdata

Användarmanualer och instruktioner såsom SäkI *[42]*, BVKF *[20]* och IFTEX *[19]* utgör huvudsakliga utdata. Dokumentationen utgör underlag för centralt systemsäkerhetsbeslut (CSSB *5.33*).

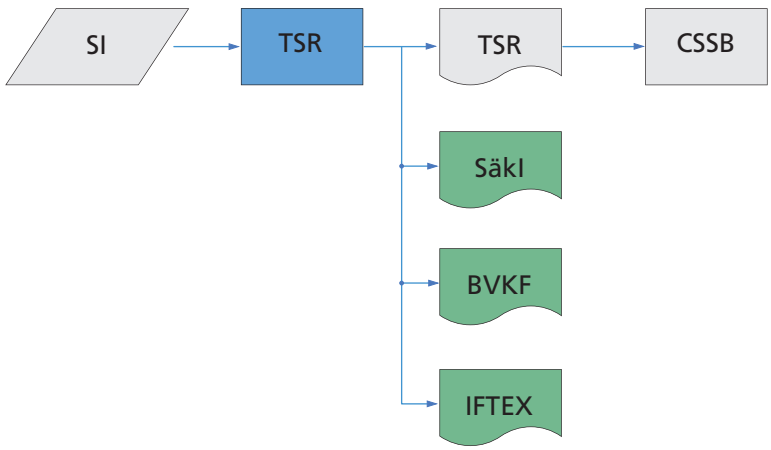


Bild 5:30 Användarmanualer och utbildning (TSR)

5.33 Centralt systemsäkerhetsbeslut (CSSB) – S53

5.33.1 Syfte

CSSB utgör Försvarsmaktens beslut att det tekniska systemet är säkert att använda ur systemsäkerhetssynpunkt. Centralt systemsäkerhetsbeslut innebär att det tekniska systemet ur systemsäkerhetssynpunkt är klart för Beslut om användning (BOA) under iakttagande av utfärdade instruktioner och föreskrifter vad avser systemsäkerheten. BOA är ett beslut om systemets lämplighet ur bland annat olika säkerhetsaspekter. BOA regleras utanför systemsäkerhetsområdet

CSSB är giltigt för ett system av viss version/utförande. Om versionen eller utförandet ändras måste nytt centralt systemsäkerhetsbeslut tas.

Beslutet baserar sig på systemsäkerhetsgodkännandet (SS *5.31*) från DesignA och att användarmanualer och utbildning (TSR *5.32*) är framtagna.

5.33.2 Aktivitetsbeskrivning

Försvarsmakten kontrollerar att erforderlig systemsäkerhetsverksamhet för det tekniska systemet har genomförts.

Centralt systemsäkerhetsbeslut grundas på att följande åtgärder är vidtagna:

- Kontroll av att systemsäkerhetskrav som ställts på system har uppfyllts.
- DesignA:s systemsäkerhetsgodkännande av system har till begärda delar erhållits.
- Instruktioner för hantering, säkerhet och skötsel är beslutade och delgivna.
- Regler för rapportering av olyckor och tillbud är beslutade och delgivna.
- Arbetsgrupp för systemsäkerhet har bildats samt uppgifter för denna är beslutade.

Framtagning av tekniskt system är som regel en komplex process under lång tid. Processen innehåller ofta flera moment av successiva materielförsök innan serieexemplar kan erhållas. Före varje materielförsök (serie av försök) med viss ”försöksutgåva” av system måste centralt systemsäkerhetsbeslut fattas. Det är dock tillräckligt att säkerhetsarbete enligt ovan, begränsas till den verksamhet och de förhållanden under vilka system i varje enskilt fall avses användas.

5.33.3 Indata

Indata till aktiviteten är systemsäkerhetsgodkännandet (SS *5.31*) samt säkerhetsinstruktioner enligt (TSR *5.32*).

5.33.4 Utdata

Centralt systemsäkerhetsbeslut (CSSB), exempel finns i *bilaga 1*. Godkännandet utgör ett underlag för Beslut om användning (BOA).

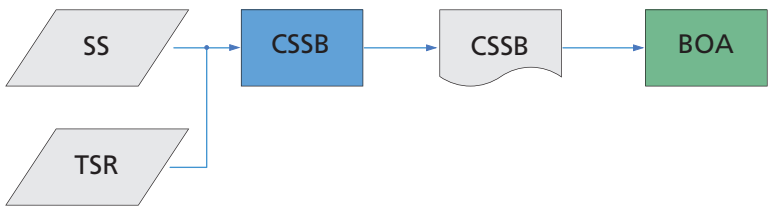


Bild 5:31 Centralt systemsäkerhetsbeslut (CSSB)

Exempel på centralt systemsäkerhetsbeslut finns i *bilaga 1* och som fil i H SystSäk CDR.

5.34 Riskanalys inför avveckling av system (RADS) – S61

5.34.1 Syfte

Att genomföra den riskanalys som sker inför avveckling. Underlaget som tagits fram under det tekniska systemets utveckling, i det ordinarie säkerhetsarbetet, ska uppdateras. Delar av RADS-verksamheten bör utföras under ordinarie analysverksamhet vid utveckling av systemet då olycksrisker, hälsorisker och miljörelaterade risker identifieras. Dessa risker kan även vara relevanta vid avveckling, därför måste avvecklingen alltid behandlas som en del av livslängden för det tekniska systemet och beaktas vid utveckling och produktion. En bra konfigurationsstyrning under hela det tekniska systemets livslängd är nödvändig, så att alla ändringar, med eventuellt nya risker, kan identifieras vid avvecklingen. Försvarsmakten har ansvar för aktiviteten.

5.34.2 Aktivitetsbeskrivning

Underlag

Riskanalys inför avveckling ska alltid ske för ett tekniskt system.

Dokumentationen från analysen ska på ett systematiskt sätt redovisa de material, ämnen eller komponenter som ingår i systemet och som kan antas ha farliga egenskaper för människa eller yttre miljö. Vidare beskrivs ett eller flera möjliga sätt att avveckla/destruera det tekniska systemet. Varje möjlig avvecklingsmetod ska analyseras/granskas med avseende på säkerhetsaspekter.

För det tekniska systemet/produkten redovisas:

- möjliga destruktions-/avvecklingsmetoder
- risker förknippade med avvecklingsproceduren.

För varje potentiell farlighet/ farligt ämne redovisas:

- hälsofaror
- miljöfaror.

Dessa egenskaper ska vägas mot föreskrivna gränsvärden eller andra beslutade krav.

Möjligheten till återanvändning av material eller ämnen redovisas med förslag till ny användning. För ämnen som på grund av sina egenskaper inte kan återanvändas, återvinnas, energiutvinnas eller destrueras anges hur dessa ska slutförvaras.

Risker på grund av lagrad energi, exempelvis i form av trycksatta kärl, spända fjädrar, reaktiva ämnen och energi i elkomponenter ska redovisas. Säkra metoder för att eliminera dessa risker vid demontering eller destruktion anges.

Analyser och aktiviteter

För system som utvecklats enligt *H SystSäk* metodik tas avvecklingsanalyser tas fram enligt RADS. För enklare system kan den ordinarie analysverksamheten (PHA *5.13*, SHA *5.16*, SSHA *5.15*, O&SHA *5.17*, HHA *5.18*, EHA *5.19* och FHA *5.20*) även behandla avvecklingen, varför ingen separat RADS behöver genomföras.

Vid avveckling av äldre system, framtaget utan stöd av systemsäkerhetsverksamheten och där underlaget saknas eller är ofullständigt genomförs alltid analyser enligt RADS i tillämpliga delar.

Material/ämnesidentifiering:

- lista alla komponenter i det tekniska systemet
- lista all material inklusive ytbehandlingar för varje komponent
- jämför ämnen med Kemikalieinspektionens PRIO-guide *[28]*.

Analys av avvecklings/destruktionsmetoder:

- beskriv avvecklingsprocessen
- beskriv varje steg i processen
- ange eventuella begränsningar/varningar för de olika stegen i processen
- analysera risker i varje steg, exempelvis enligt UK Ordnance Board P115 *[7]*
- justera processen i syfte att minimera eventuella risker
- demonstrera att processen kan genomföras enligt beskrivningen
- dokumentera den slutliga processen med dess analysresultat.

UK Ordnance Board P115 *[7]* anger att varje steg ska analyseras med avseende på risk för olycka, hälsa och miljöpåverkan.

Konfigurationsstyrning

Den som ansvarar för systemdokumentationen efter leverans från leverantör, i regel materielsystemansvarig vid DesignA, ska även ansvara för uppdatering av ändringar av konfigurationen för att kunna utföra en slutlig riskanalys inför avveckling. Tvingande krav med stor betydelse för en säker avveckling av det tekniska systemet dokumenteras i redovisningssystemet. Detta ska vara knutet till F-beteckning (M-nummer).

Försäljning

Om restprodukter eller system ska säljas i samband med avveckling krävs särskilda kontroller.

För skrot ska intyg lämnas om att skrotet är fritt från rester av explosiva varor och att det inte innehåller brandfarlig vara eller gas. Detta krav gäller allt militärt skrot som har levererats av Försvarsmakten eller DesignA, oavsett om det har innehållit explosivämnen eller inte. Skrotet ska även deklareras i fråga om eventuellt miljöfarliga ämnen (miljöfarligt avfall) som kan ingå i skrotmängden.

För helt eller delvis användbara system ska eventuella defekter eller riskkällor/farliga tillstånd dokumenteras skriftligt och denna dokumentation ska åtfölja objektet vid försäljning. I vissa fall krävs att det farliga eller förbjudna ämnet/delen tas bort före försäljning.

Försvarsmaktens detaljerade regler för försäljning och annan avyttring tillsammans med regler för ledning, planering och genomförande av sådana åtgärder, framgår av H Förnavv *[22]*.

5.34.3 Indata

Indata till aktiviteten utgör en konstruktionsbeskrivning samt om möjligt även SAR *5.21* och risklogg enligt HTRR *5.9*. Från miljörelaterade aktiviteter kan det finnas en Återvinningsmanual *[15]*, denna kan utgöra underlag vid RADS.

5.34.4 Utdata

Avvecklingsinstruktion samt riskanalysrapport inför avveckling. Identifierad risk kan dokumenteras i risklogg enligt HTRR *5.9*.

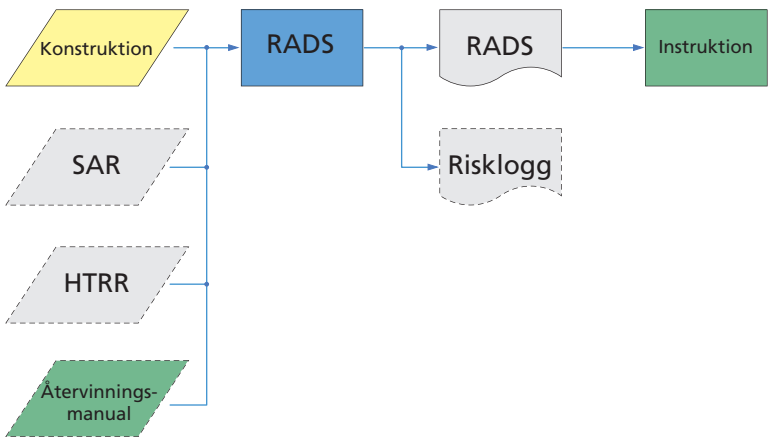


Bild 5:32 Riskanalys inför avveckling av system (RADS)

6 PROGRAMVARUSÄKERHET

6.1 ALLMÄNT

Programvarusäkerhet tillämpar de principer och den verksamhet, som fastlagts för systemsäkerhetsarbetet, på det tekniska systemets programvarubaserade delar. Olika procedurer, aktiviteter och metoder används, för att bygga in systemsäkerhetsegenskaper i den övergripande systemarkitekturen och vidare ned i programvarans arkitektur och implementation. Hur detta sker ska beskrivas i System Safety Program Plan, (SSPP *5.5*). Denna verksamhet beror av de egenskaper som en realisering i programvara medför, vilket inte enbart berör programvara som produkt, utan också de parter som är involverade i dess framtagning, drift och underhåll samt de processer dessa använder sig av. Grunderna för framtagning av programvara framgår av H ProgSäk *[18]*.

6.2 PROGRAMVARUEGENSKAPER

En programvaruprodukt representeras av dess samlade dokumentation över krav, arkitektur/ design, gränsytor, implementation, analysresultat, ändringsbeskrivningar eller feldatabaser.

En realisering i programvara kan uppvisa egenskaper som inte återfinns för komponenter realiserade med hjälp av andra tekniker, till exempel:

- Abstrakt, konceptuell beskrivning av komplexa samband utan fysiska begränsningar.
- Diskontinuerligt beteende: en liten förändring i någon av förutsättningarna för vilket komponenten är byggd, kan leda exekveringen in på andra grenar i exekveringsträdet med ett radikalt annorlunda beteende som följd.
- Uppvisade egenskaper styrs av det sammanhang i vilket programvaran infogas och används (system, systemomgivning, användningsprofil).

- Systematiska fel (logiska misstag) dominerar över slumpmässiga fel.
- Relevant skattning av felfrekvenser inte möjlig före driftsättning för programvara med mycket låga felsannolikheter (höga SIL-nivåer).
- Säkerhetshot direkt initierade av programvaran kan härröra från programvaruprodukten (specifikations-/design-/implementationsfel), dess produktionsprocesser, produktionsverktyg eller personalens handhavande (till exempel för leverantör: kod återanvänd under förändrade förutsättningar, slutanvändare: drift utanför avsett användningsområde, handhavande i strid mot specifikationer och instruktioner).
- Dolda säkerhetshot i det tekniska systemets gränssnitt kan oavsiktligt aktiveras vid programvarans interaktion med övriga komponenter (programvara, maskinvara, operatörer), trots att varje enskild komponent uppvisat säkert beteende.

Dessa egenheter påverkar de sätt på vilka programvarusäkerheten kan tillgodoses i och med att:

- En realisering där delar av högre kritikalitet inte kan isoleras från de av lägre eller ingen kritikalitet är i sin helhet kritisk av dess högsta grad.
- Programvarans konstruktion måste grundas på en säkerhetsfilosofi för hela det tekniska systemet i avsedd användningssituation.
- Programvara betraktad som säker i ett visst sammanhang behöver inte vara det i ett annat.
- Återanvändning av programvara, som inte har konstruerats för återanvändning, är vansklig och fordrar speciella säkerhetskontroller och åtgärder. Detta gäller även vid återanvändning i mycket närbesläktade system eller i oförändrat system med andra driftsförhållanden.
- En slutgiltig bedömning av programvarans egenskaper måste baseras på programvaran som integrerad del av det tekniska systemet i den omgivning och den användning detta är avsett för.

- Riskreducering för programvara inriktas i första hand mot omkonstruktion (snarare än genom tillägg av skyddsfunktioner).
- Riskreducering i form av redundans kan enbart baseras på diversitet, ej identiska kopior.
- Programvarudel för vilken krav ställs på mycket låga felfrekvenser (höga SIL-nivåer) fordrar oftast en omkonstruktion till en lösning så att högre felfrekvens kan tillåtas för programvarudelen och därmed möjlighet att, före operationellt bruk, verifiera kravet med hjälp av statistiskt säkerställda skattningar.

En medveten, säkerhetsinriktad systemutformning grundad på allmänna konstruktionsprinciper är nödvändig, för att bemästra dessa egenheter. Till de mer väsentliga hör:

- **Enkelhet, determinism och verifierbarhet** prioriteras vid konstruktion från översta systemnivå och ned till programvarunivå. Dessa egenskaper är nödvändiga, för att kunna genomföra olika riskanalyser. Enkelhet, för att praktiskt kunna göra en bedömning. Determinism, för att kunna bedöma det tekniska systemets beteenden ur givna förutsättningar. Verifierbarhet, för att kunna avgöra att specificerade systemegenskaper har realiserats.
- **Säkerhetsinriktade arkitekturer** definieras med strategier för hur systemsäkerheten ska upprätthållas. För system av system fordras en hierarki av arkitekturer, vilka samverkar för att tillgodose systemsäkerheten sett från den översta nivån. För identifierade systemsäkerhetshot fastläggs på vilka nivåer och av vilka (del)system dessa ska bemötas. För kvarvarande säkerhetshot, vilka inte kunnat elimineras eller reduceras enligt krav genom omkonstruktion, kompletteras konstruktionen med speciella säkerhetsmekanismer.
- **Kritikalitetspartitionerad programvara** skapas för att undvika att kritisk programvarudel direkt eller indirekt kan påverkas av del med lägre eller ingen kritikalitet.

- **Diversitet** övervägs som första alternativ vid riskreducering, i synnerhet för programvara, där krav på lågfrekventa felsannolikheter ställs.
- **Onödig och överflödig funktionalitet** elimineras eller deaktiveras i säkerhetskritisk kod, för att förhindra oavsiktlig exekvering. Detta innebär bland annat att död kod rensas bort, att funktionalitet avsedd för viss systemmod eller viss systemkonfiguration förhindras att exekvera under annan mod/konfiguration, att ej efterfrågad funktionalitet avskärmas (aktuellt till exempel för återanvänd programvara).

Tidiga insatser, som syftar till att bygga in dessa egenskaper i det tekniska systemet på högsta nivå och ned i de enskilda realiseringsenheterna, fordras för bästa effekt av investerat säkerhetsarbete. Bevakning av hur dessa egenskaper senare detaljeras och realiseras utförs såväl vid leverantörs granskningar som vid System Safety Working Group (SSWG *5.8*) uppföljningar, se *avsnitt 6.4*.

6.3 Säkerhetskrav på programvara

Programvara, som kan åstadkomma att en vådahändelse inträffar, eller vars uppgift är att förhindra detta, är säkerhetskritisk, se Safety Critical Functions (SCF *5.11*). Typiska exempel kan vara programvara för styrning, övervakning, skydd samt kommunikation med avseende på säkerhetskritisk aktivitet, utrustning eller information.

De allmänna krav, som kan ställas på denna typ av programvara, avser inte enbart programvaruprodukter i dess olika stadier, utan även personalkvalifikationer samt de processer, som tillämpas på ett programvarusystem under dess livslängd. Dessa krav berör såväl Försvarsmakten i egenskap av uppdragsgivare och slutanvändare som den beställande parten, DesignA samt leverantör. En sammanställning över de krav, som kan vara aktuella för nyutvecklad och återanvänd programvara i säkerhetskritiska system, återfinns i H ProgSäk *[18]*. Dessa är graderade efter programvarans kritikalitet och ges ibland i flera varianter. Ett urval av de krav, som är tillämpliga för de säkerhetskritiska programvarudelarna i aktuellt system, är därför nödvändigt. Detta styrs av kritikaliteten hos de enskilda delarna samt kravets relevans. För ute-

slutet krav fordras motiveringar, vilka blir föremål för omprövning vid förändrade förutsättningar. Endast där oberoende kan visas mellan skilda delar, är det möjligt, att i samma system tillämpa krav av olika kritikalitet. Urvalet av krav kommer därför att skilja mellan kritikalitetsseparerade delar. Stöd för dokumentation av valda krav samt uppföljning av i vilken grad dessa krav är tillgodosedda kan ges i form av ett antal korsreferenslistor.

Kraven i H ProgSäk *[18]* är indelade i två kategorier: grundkrav samt generella säkerhetskrav. Programvarusäkerhetskrav avseende viss komponent, funktion eller (del)system ingår ej, däremot anvisningar hur dessa kan härledas. Dessa specifika krav utgör därmed tillägg till krav listade i H ProgSäk *[18]*. Den resulterande kravmängden blir styrande för efterföljande aktiviteter under Safety Verification (SV *5.24*) samt systemsäkerhetsutlåtande (SCA *5.27*), se *avsnitt 6.4*.

Processen att ta fram en alltmer komplett uppsättning programvarusäkerhetskrav är iterativ och sker parallellt med den traditionella kravnedbrytningen och detaljeringen av det tekniska systemet i underliggande programvarudelar. Denna kravspecificering, en delaktivitet under Safety Requirements/Criteria Analysis (SRCA *5.14*), baseras på analyser utförda under 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*) och Operating and Support Hazard Analysis (O&SHA *5.17*). Vådahändelser med dess orsaker, som identifieras under dessa analyser, omformuleras till systemspecifika säkerhetskrav samt säkerhetsinriktade restriktioner på programvarans arkitektur.

Återanvändning av det tekniska systemets säkerhetskritiska programvarudelar kan underlättas genom en stegvis härledning av de systemspecifika säkerhetskraven. Analyserna inriktas därvid mot att först identifiera de domängemensamma säkerhetskraven, för att därefter komplettera med de domänspecifika säkerhetskraven samt avsluta med de systemspecifika. Domängemensamma säkerhetskrav utgörs av krav med avseende på en individuell programvarufunktion/-komponent/system utan hänsyn till dess samman-

hang (till exempel ett vapensystem för flyg, marin, armé), medan domänspecifika krav avser en viss applikationsdomän (till exempel ett vapensystem för marinen).

6.4 Verifiering av programvara

Syftet med Safety Verification (SV *5.24*) är att säkerställa att det tekniska systemets säkerhetskrav är uppfyllda. Dessa utgör en delmängd av övriga krav. Säkerhetsverifiering (SV *5.24*) med avseende på programvara blir därigenom integrerad med den verifieringsprocess, som krävs för all typ av programvara och som fortlöpande utförs under uppbyggnad och integration med övriga systemdelar. För säkerhetskritisk programvara innebär säkerhetsverifieringen, att såväl grundkrav som systemsäkerhetskrav ska verifieras, se *avsnitt 2.1*.

Verifiering kan bestå av granskning/uppföljning samt olika analyser (statiska/dynamiska/systemsäkerhetsinriktade). Procedurer och verktyg, som stödjer denna verksamhet, ingår i den traditionella programutvecklingsmiljön. Stöd vid genomgång av ingående produkter och aktiviteter hos säkerhetskritisk programvara kan ske med hjälp av checklistor inriktade på programvarusäkerhet. För uppföljning av säkerhetskravens uppfyllnad finns korsreferenslistor framtagna, som kopplar krav med aktuellt status över verifieringsläge samt belägg för utförda verifieringar. Denna sammanställning ger en god bild av programvarans säkerhetsverksamhet och säkerhetsläge, vilket gör den användbar som underlag vid leverantörs System Safety Progress Summary (SSPS *5.10*) rapportering.

Vid verifiering av programvara framtagen enligt någon annan säkerhetsinriktad handbok eller standard utförs först en avbildning av dess krav på den mer heltäckande kravmängden i H ProgSäk *[18]*, innan programvarans kravuppfyllnad kan utvärderas.

7 Checklista för materielkrav och aktiviteter

Checklistan används vid framtagning av krav till RFP, genomförande av projektuppföljningar samt redovisningar i granskningsgrupper (SSPR *5.7*), rådgivningsgrupper och arbetsgrupper för systemsäkerhet (SSWG *5.8*). Fullständig beskrivning av kraven framgår av *kapitel 2* och *avsnitt 3.1*.

Krav nr	Benämning	Tilllämplighet			Kommentar
		Ja	Nej	N/A[a]	
Materielkrav					
0.21.001	Minimala säkerhetsföreskrifter				
0.21.002	Enkelfel				
0.21.003	Gemensamma orsaker				
0.21.004	Tålighet mot abnorma miljöer				
0.21.005	Egenskaper som kan leda till kritiskt fel definieras i produktdokumentation				
0.21.006	Egenskaper som kan leda till allvarligt fel definieras i produktdokumentation				
0.21.007	Programvarans grundläggande kvalitetskrav				
0.21.008	Urval av generella programvarusäkerhetskrav				
0.21.009	Undvik att använda dispenser				
0.21.010	Sammanfogningsmetoder				
0.21.011	Identifiering av plastmaterial				
0.22.001	Allkontroll av egenskaper som kan leda till kritiskt fel				
0.22.002	Allkontroll av egenskaper som kan leda till allvarligt fel				
0.22.003	Kontroll av egenskaper som kan leda till kritiskt fel				

Krav nr	Benämning	Tilllämplighet			Kommentar
		Ja	Nej	N/A[a]	
0.22.004	Kontroll av egenskaper som kan leda till allvarligt fel				
0.22.005	Kalibrering av kontrollutrustning				
0.22.006	Avskiljande av defekta enheter				
0.23.001	Underhåll för säkerhetens upprätthållande				
0.23.002	Säkerhet efter underhåll				
0.24.001	Återanvändning- och återvinningsgrad				
Aktiviteter					
0.31.001	System Safety Program (SSP)				
0.31.002	Systemsäkerhetsvärdering (SSE)				
0.31.003	Säkerhetskrav i TTEM (TTEM)				
0.31.004	Kravställning vid anbudsförfrågan (RFP)				
0.31.005	System Safety Program Plan (SSPP)				
0.31.006	Integration/Management of Subcontractors (IMSC)				
0.31.007	System Safety Program Reviews /Audits (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)				
0.31.011	Safety Critical Functions (SCF)				
0.31.012	Preliminary Hazard List (PHL)				
0.31.013	Preliminary Hazard Analysis (PHA)				
0.31.014	Safety Requirements/Criteria Analysis (SRCA)				

Krav nr	Benämning	Tilllämplighet			Kommentar
		Ja	Nej	N/A[a]	
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	Riskanalys för yttre miljö (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	Säkerhetsföreskrifter (SI)				
0.31.025	Systemsäkerhetsutlåtande (SCA)				
0.31.026	Felrapporteringssystem (FRACAS)				
0.31.027	Systemsäkerhetsgodkännande (SS)				
0.31.028	Användarmanualer och utbildning (TSR)				
0.31.029	Centralt systemsäkerhetsbeslut (CSSB)				
0.31.030	Riskanalys inför avveckling av system (RADS)				

a. N/A = Ej tillämpligt

8 Systemsäkerhetsanalyser

8.1 Principer för systemsäkerhetsanalyser

En säkerhetsanalys (även kallad riskanalys) utgörs av en systematisk procedur, där man analytiskt undersöker hur och i vilken grad, till exempel integrationsfel, komponentfel eller felaktigt handhavande kan förorsaka vådahändelser hos ett system.

Det finns ett stort antal analysmetoder som är riktade mot olika tillämpningar såsom konstruktionslösningar, operativt hantering och produktionsprocesser. Varje enskild metod har begränsningar som gör att det i många fall är lämpligt att kombinera flera metoder för att erhålla ett gott resultat.

Bilden nedan visar vad en komplett säkerhetsanalys (gulmarkerat i bilden) i princip omfattar och hur dessa olika aktiviteter samverkar.

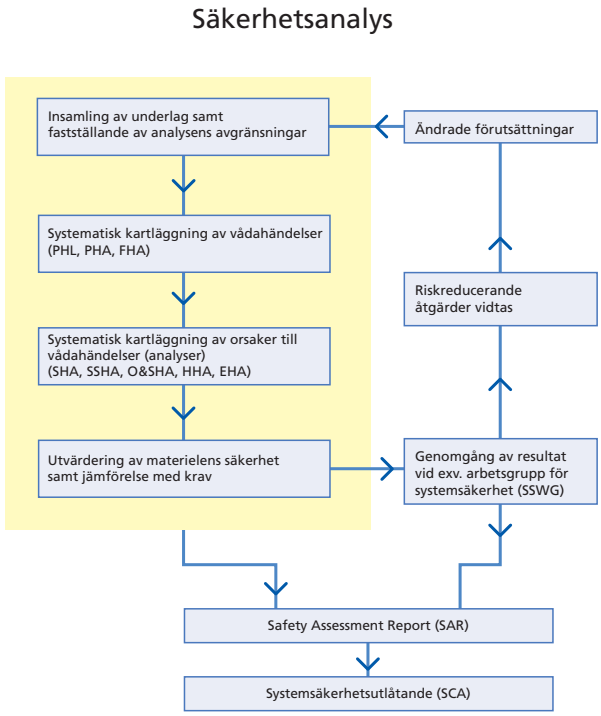


Bild 8:1 Säkerhetsanalys

Inom ramen för denna generella modell kan säkerhetsanalyser se tämligen olika ut beroende på:

- Val av analysmetod, varvid valet huvudsakligen styrs av systemets konstruktion och funktion samt analysens syfte. Om utvärderingen görs kvalitativ eller kvantitativ.
- Hur detaljerat det tekniska underlaget är vid analystidpunkten.
- Vilken nivå (underenheter, komponenter, programvarublock med mera) i systemet analysen omfattar.
- Vilken fas, konstruktion eller tillverkning, analysen omfattar.
- Hur den formella delen av analysen (symboler, blanketter och formulär) ser ut.

Nedan finns fyra vanligen förekommande analysmetoder överskådligt beskrivna. För mer detaljerade beskrivningar hänvisas till litteratur inom området.

Olycksrisker/vådahändelser som identifieras vid exempelvis PHL, PHA och FHA analyseras för att få fram de grundläggande orsakerna som kan bidra till att dessa uppstår. Aktiviteterna SHA, SSHA, O&SHA, HHA och EHA använder oftast någon eller några av analysmetoderna FMECA, FTA, ETA och HAZOP.

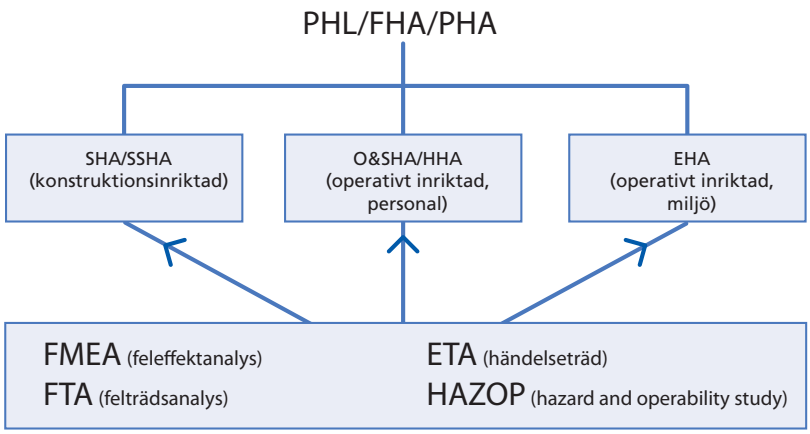


Bild 8:2 Koppling av aktivitet till metod

8.2 Felträdsanalys (FTA)

Felträdsanalys, FTA (Fault Tree Analysis), är en analysmetod där en presumtiv vådahändelse stegvis undersöks för att finna vilka underordnade händelser, eller kombinationer av sådana, som kan orsaka vådahändelsen. Detta sker deduktivt (uppifrån och ner).

Felträdsanalysen utgår från en vådahändelse i taget och påvisar först vilka omedelbart underliggande händelser eller kombinationer av sådana, som leder till vådahändelsen. Dessa händelser kan vara felfungerande komponenter, felaktigt handhavande eller specifika yttre omständigheter. De underliggande händelserna och deras orsaker uppdelas vidare på samma sätt och så fortsätter analysen ner till en detaljeringsnivå som är lämplig för riskreducerande åtgärder. Analysens lägsta nivå består av basfel i enkla komponenter eller liknande.

I ett felträd beskrivs på så sätt hur fel i olika delar av ett system kan samverka och leda till en vådahändelse. För att göra metoden systematisk och åskådlig, används en logisk schemateknik med standardiserade symboler.

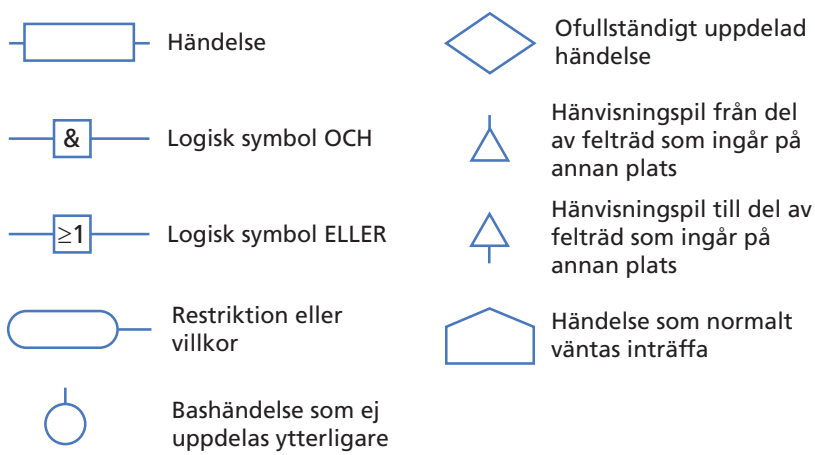


Bild 8:3 Felträdssymboler

Lämplighet: Felträdsanalysen är ett bra hjälpmedel och blir överskådlig i de fall, då en vådahändelse kräver två eller flera av varandra oberoende fel/händelser för att inträffa. Den klarar således situationer med redundanser.

Nackdelar: Uppdelningen i underordnade händelser ställer stora krav på noggrannhet och kunskaper om systemet hos den som utför analysen. Man kan lätt förbise enstaka händelser och felsätt som kan leda till eller bidra till vådahändelser. Felträdsanalysen utgör ett statiskt betraktelsesätt. Därför kan inte FTA okritiskt användas vid driftmässiga ”dynamiska” system med till exempel växlande driftmoder, stand-by situationer (till exempel passiva redundanser) eller deterministiska inslag (till exempel periodiskt underhåll). Vissa konstgrepp måste då tillgripas för att beräkningarna ska bli korrekta.

8.2.1 Kvalitativa felträdsanalyser

Felträden utmynnar i bashändelser som anger grundorsakerna till den definierade vådahändelsen. De utgörs av planerade händelser, förhållanden eller basfel. För att eliminera vådahändelsen måste åtgärder vidtas med de påverkande händelserna. Vilka åtgärder som ska vidtas beror dels på hur uppenbart de påverkar vådahändelsen (beroende på trädstrukturen), dels på hur ofta de kan tänkas inträffa.

Normalt tolereras inte sådana enkelfel som ensamma kan leda till vådahändelse och som kan elimineras genom konstruktionsändring.

För att minimera de tillverkningsmässiga bristerna vidtas olika åtgärder med basfelen. Åtgärdena beror på hur ofta felen kan förväntas inträffa samt i vilken grad de bidrar till vådahändelsen (hur många &-villkor som finns mellan bashändelsen och vådahändelsen, eller hur många ingångar det finns i &-grindarna).

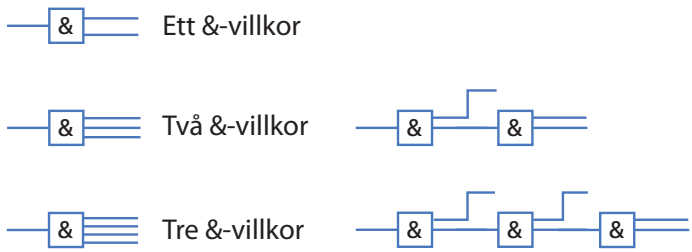


Bild 8:4 Antalet &-villkor

Exempel på hur antalet &-villkor tas fram visas i bilden nedan.

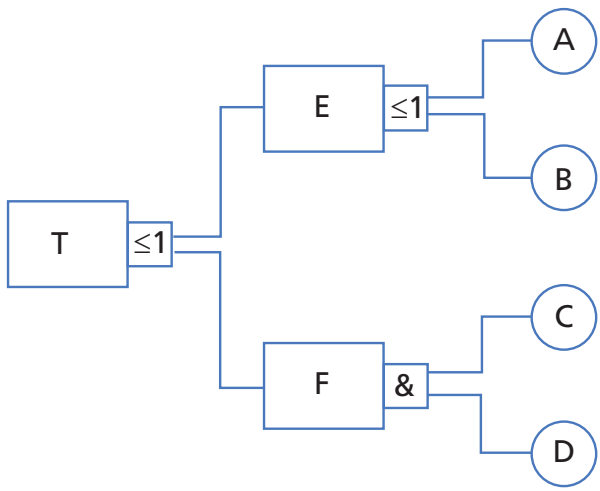


Bild 8:5 Felträd med olika antal &-villkor

Bashändelsen A har inget &-villkor till vådahändelsen T medan bashändelsen C har ett &-villkor till vådahändelsen T.

8.2.2 Kvantitativa felträdsanalyser

Då säkerhetskraven är kvantitativa sker verifieringen genom att visa att sannolikheten för vådahändelse eller olycka inte överstiger de specificerade kraven. En svårighet kan vara att erhålla relevanta ingångsvärden för beräkningarna. Det är därför olämpligt att dra för långtgående slutsatser om materielens säkerhet eller att jämföra olika system, eftersom förutsättningarna för beräkningarna kan vara mycket olika.

Beräkningarna kan ske enligt följande principiella exempel. Observera att denna förenklade beräkning förutsätter oberoende mellan de olika bashändelserna.

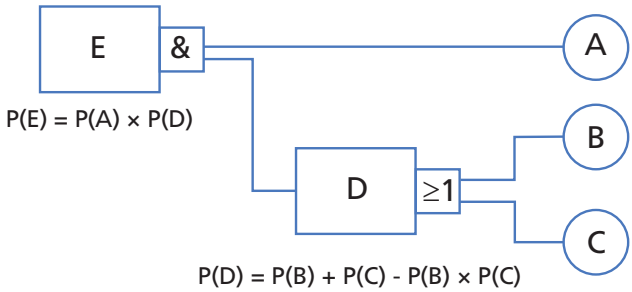


Bild 8:6 Beräkningar av felträdssannolikheter

För att erhålla sannolikheter på varje bashändelse används normalt erfarenhetsvärden (databank) eller så kan för materialrelaterade konstruktionsfel påkännings-tålighets-metoden (STRESS-STRENGTH) användas. Denna metod går ut på att beräkna sannolikheten för att styrkan hos konstruktionen överstiger miljöfaktorernas stress. I bilden illustreras hur sannolikheten, som motsvaras av interferensytan, är beroende av påkännings- och tålighetsfördelningarna.

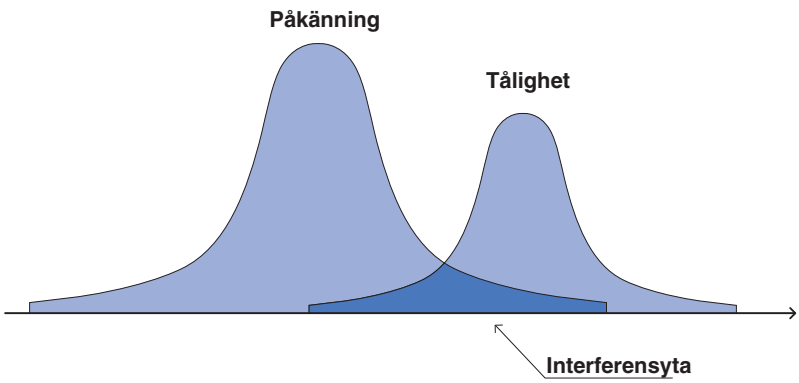


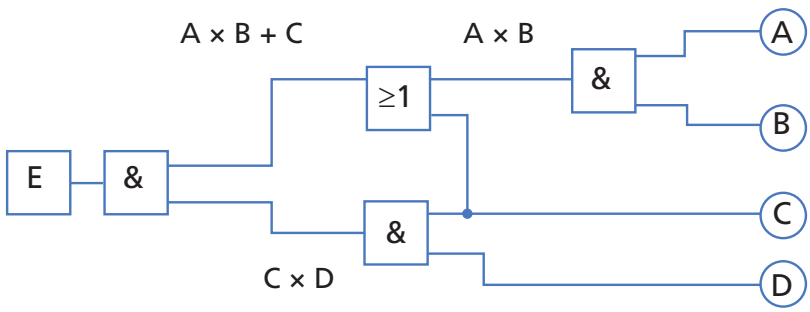
Bild 8:7 Påkännings-tålighets-metoden

Då sannolikheterna inte kan beräknas för bashändelserna, kan i stället en så kallade känslighetsanalys utföras. Här ansätts ofta lika sannolikhet för de olika bashändelserna och sannolikheten för vådahändelsen beräknas. Därefter ändras var för sig sannolikheterna för de olika bashändelserna och vådahändelsesannolik-

heten beräknas åter. På detta sätt kan de bashändelser som ger störst bidrag till vådahändelsen urskiljas. Metoden är lämpligast vid stora felträd, där överskådligheten är liten.

En annan beräkningsmetod är att använda Boolesk Algebra, där varje bashändelse benämns med till exempel en bokstav. Efter reduktion av uttrycket för vådahändelsen framgår det vilka bashändelser, som mest påverkar sannolikheten för vådahändelsen.

Beräkningar med numeriska värden ska inte ske förrän reduktion av slututtrycket har skett. Sådana reduktioner är i praktiken omöjliga att göra för hand vid stora felträd.



E = (A × B + C) × (C × D) reduceras till E = C × D

Bild 8:8 Exempel på lösning med boolesk algebra

I detta exempel har de standardiserade IEC-symbolerna använts. Olika lösningar på en felträdsstruktur kan naturligtvis förekomma.

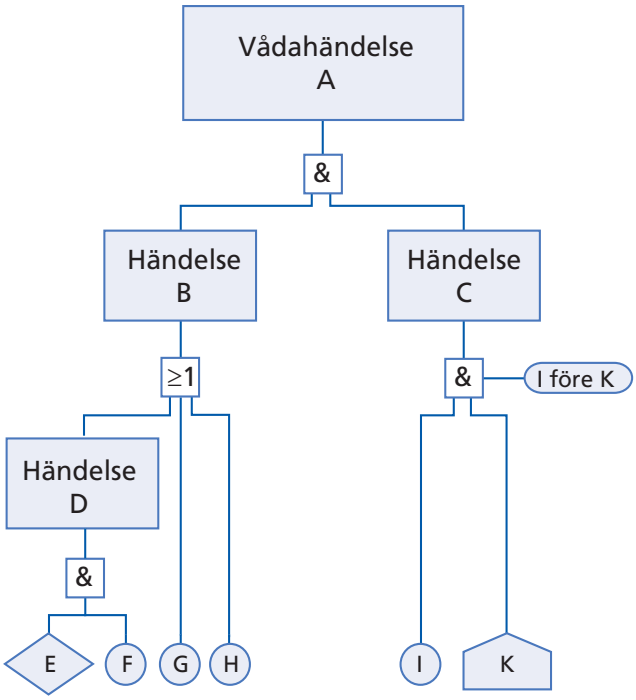


Bild 8:9 Exempel på felträdsanalys

Felträdet uttrycker orsakssambandet: A inträffar om både B och C inträffar. B inträffar om minst en av händelserna D, G eller H inträffar. D inträffar om både E och F inträffar. C inträffar om både I och K inträffar varvid I måste inträffa före K. Händelsen E kan uppdelas ytterligare. Händelsen K förväntas alltid inträffa.

8.3 Feleffektanalys (FMEA)

Vid feleffektanalys, FMEA (Fault Modes and Effects Analysis) genomförs analysarbetet induktivt (nerifrån och upp) i princip i omvänd ordning jämfört med felträdsanalys. Man utgår från komponenter eller delsystem för vilka varje felsätt analyseras med avseende på den effekt det kan åstadkomma på systemet.

Beroende av hur långt detaljutformningen av det analyserade systemet har kommit, kan felsätt i funktioner eller komponenter beaktas. För varje felsätt anges orsaken och vilken effekt det har. Ur alla tänkbara feleffekter kan sedan eventuella vådahändelser identifieras och åtgärder vidtas för att minska risken.

Även feleffektanalys kan med stor fördel utföras i preliminär form och lämplig detaljeringsgrad i tidigt skede av ett konstruktionsarbete så att riskreducerande åtgärder snabbt kan vidtas.

Analysen utförs med hjälp av formulär där i olika kolumner bland annat anges aktuell komponent och/eller funktion, möjligt felsätt, trolig felorsak, felets effekt såväl på detaljnivå som för hela systemet samt eventuellt även sannolikheten för att felet ska inträffa.

Fördelar:	Feleffektanalysen är särskilt lämplig, vid undersökning av vilka felsätt som var för sig kan orsaka en vådahändelse. Metoden är systematisk och heltäckande och resultatet blir överskådligt och lätt att förstå.
Nackdelar:	Metoden kräver genomgång av ett stort antal detaljer och felsätt, som inte direkt berör säkerheten. Analysen blir därför omfattande och tidskrävande för komplexa system. Vidare är det svårt att med metoden upptäcka effekterna av en kombination av flera samtidiga fel.

8.3.1 Kvalitativa feleffektanalyser

Analogt med kvalitativa felträd kan en riskmatris användas för bedömning av de olika felsätten. I feleffektanalysen införs en kolumn för allvarlighetsgraden, även kallad kritikaliteten. Analysmetoden betecknas då FMECA (Fault Modes, Effects and Criticality Analysis).

8.3.2 Kvantitativa feleffektanalyser

För att enklare kunna behandla resultatet av en feleffektanalys kan det vara av värde att göra dels en bedömning eller skattning av förekomsten av felsätt, dels en gradering av felsättets inverkan på systemet. Detta ger ökade möjligheter att jämföra olika konstruktionslösningar från säkerhetssynpunkt.

FMECA-formuläret kan härvidlag utökas med tre kolumner. En kolumn där felfrekvensen anges i en skala från förslagsvis A till E där A motsvarar högsta felfrekvensen. En andra kolumn där felsättets konsekvens anges i en skala I till IV där I motsvarar högsta allvarlighetsgrad (skadeklass). I den tredje kolumnen beräknas felsättets risktal (RPN= Risk Priority Number).

Det finns flera olika metoder för att beräkna risktalet. Inom ett och samma verksamhetsområde är det lämpligt att samma metod används. Den vanligaste metoden är multiplikation. Beräkning av risktalet sker genom att skalvärdena för felfrekvens (A=1, B=2, och så vidare och allvarlighet (I=1, II=2 och så vidare) multipliceras med varandra. Risktalet kommer att ge ett relativt, numeriskt värde på hur kritiskt ett visst felsätt är i förhållande till andra felsätt. På detta sätt kan olika felsätt rangordnas och prioritering av åtgärder kan göras.

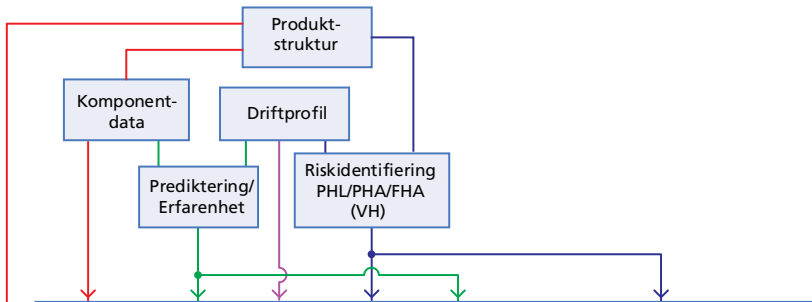
Feleffektanalysen genomförs med hjälp av formulär med kolumner, där förutsättningar och resultat förs in. Formulären kan se olika ut beroende på analysens syfte och detaljeringsgrad, ett exempel ges nedan.

Pos nr/ Benämning	Felsätt	Orsak	Fas	Feleffekt Lokalt	Feleffekt Delsystem	Feleffekt System	Fel-upptäckt	Kon-sekv	Frekv	RPN	Anmärkning
1. Lavettklyka	Glapp mellan lavettklyka och rekylmantel	Överfall ej åtdraget. För stort spel	4	Försumbar rörelse mellan lavettklyka och rekylmantel	Ökat slitage av infästningen	Minskad tillgänglighet	Pjäspersonal vid tillsyn	IV	C	12	UH-intervall minskas. Ej säkerhetskritiskt
	Infästning till rekylmantel kärvar	Överfall för litet spel etc	4	Tungt att elevera	Ökar slitage av infästningen	Minskad tillgänglighet	Pjäspersonal vid tillsyn	IV	B	8	UH-intervall minskas. Ej säkerhetskritiskt
		Materialfel	4	Rörelse mellan lavettklyka och rekylmantel	Rekylmantel lossnar	Haveri, skjutning utanför tänkt målområde	Pjäspersonal vid skjutning	I	C	3	Beräkning av hållfasthetsegenskaper, säkerhetsfaktor samt felintensitet
2. Rekylmantel	Glapp, kärvar (se pos 1)		4								
	Lossar	Tappen går av pga materielfel	4	Rörelse mellan lavettklyka och rekylmantel	Eldrör lossnar, ökar spridning	Haveri, skjutning utanför tänkt målområde	Pjäspersonal vid skjutning	II	D	8	
		Eldrörslagring kärvar	4	Ökar belastningen på rekylmantelns tapp	Eldrör lossnar, ökar spridning	Haveri, skjutning utanför tänkt målområde	Pjäspersonal vid skjutning	II	D	8	Höga rörelsekrafter
	Rekylbroms lossnar	Materialfel, defekt rekylbroms (se även pos 5 Rekylbroms)	4	Ökar belastningen på rekylmantelns tapp	Eldrör lossnar, ökar spridning	Haveri, skjutning utanför tänkt målområde	Pjäspersonal vid skjutning	II	E	10	
	Framförare lossnar	Materialfel, defekt rekylbroms (se även pos 5 Rekylbroms)	4	Utebliven framföringsfunktion	Eldrör ej åter i framfört läge	Eldavbrott	Pjäspersonal vid skjutning	IV	D	16	Ej säkerhetskritiskt

Bild 8:10 Exempel på feleffektanalys

Nedan ges ett exempel på vilka indata som behövs för att skapa en FMECA. Produkt-/systemstukturen definiera vilka delar och komponenter som systemet består av. Komponentdata definierar typ av komponent samt dess egenskaper. Vidare ger komponentunderlag för att kunna identifiera komponentens felmoder (samt felmodsfördelning) samt en prediktering av sannolikheten för att felmoden inträffar under angiven användningsfas enligt systemets driftprofil.

Produktstrukturen (systembeskrivningen) utgör underlag för att genomföra riskidentifiering (PHL, PHA, FHA) för att identifiera vådahändelser på systemnivå. Dessa vådahändelser kopplas till de identifierade effekterna av komponenterna felmoder. Vidare anges konsekvensen för systemeffekten (vådahändelsen) som exempelvis skadeklass.



Komponent	Felmod	Fas	Effekt	Sanno-likhet	S-klass I	S-klass II	S-klass III	S-klass IV
A	A1 (25%)	1	VH01	0,0025	0,1	0,2	0,3	0,4
	A2 (75%)	1	VH02	0,0075	0,0	0,0	0,3	0,7
B	B1 (50%)	1	-	0,0005	0,0	0,0	0,0	0,0
	B2 (50%)	1	VH01	0,0005	0,1	0,2	0,3	0,4
C	C1 (100%)	1	-	0,01	0,0	0,0	0,0	0,0

Bild 8:11 Exempel på underlag till feleffektanalys

8.4 Händelseträd (ETA)

Denna metod, som kan vara kvalitativ eller kvantitativ, används till att identifiera effekterna av en given händelse. Metoden används ofta för att analysera system som har skydds- och säkerhetsanordningar. Varje händelse förutsätts kunna resultera antingen i lyckat eller misslyckat resultat. Observera att sannolikheterna i trädet är betingade sannolikheter, eftersom tidigare händelse måste ha inträffat. På samma sätt som för vanliga felträd ställs frågan, vad som händer om en delhändelse inträffar eller ej. För att få en heltäckande analys måste alla starthändelser vara identifierade.

Det underlättar uppbyggnaden av ett händelseträd om det finns tillgång till en funktionsbeskrivning i form av en blockstruktur, så kallad funktionssäkerhetsschema (Reliability Block Diagram).

Följande exempel visar hur händelseträdstekniken kan tillämpas för att visa vad en grundstötning kan ge för sluthändelser. Här verkar alla delhändelserna i serie så en efterföljande händelse är betingad av att den föregående har inträffat. Inträffandesannolikheterna har noterats under ja/nej svaret.

Det bör observeras att alla händelser inte är beskrivna i exemplet, som exempel behandlas inte situationen med falsklarm.

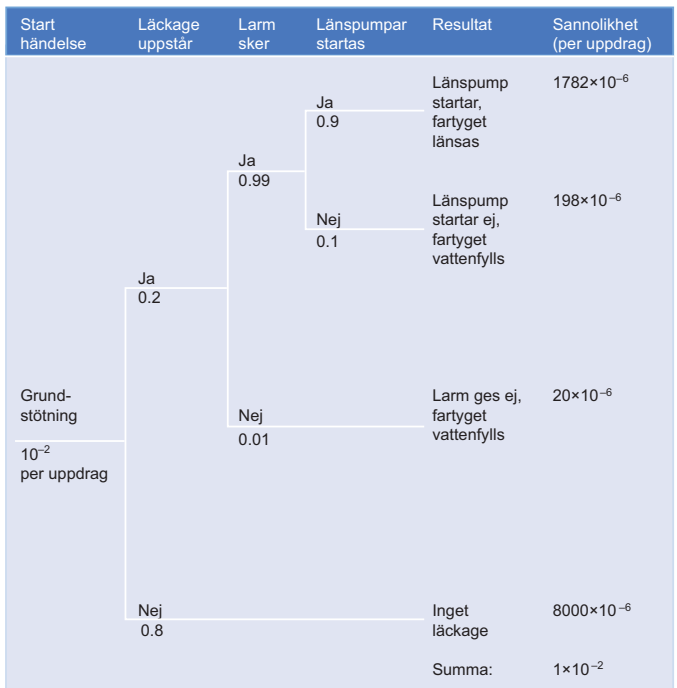


Bild 8:12 Exempel på händelseträdsanalys

8.5 Hazard and Operability (HAZOP) Study

Denna metod lämpar sig bäst för processer och operativa förlopp. Metoden är närbesläktad med feleffektanalysen (FMEA), men felmoderna har definierats och gjorts enhetliga från början. Följande principiella steg tillämpas:

- Beskriv processen eller det operativa förloppet, inklusive den mänskliga medverkan, innefattande den avsedda funktionen.
- Granska systematiskt varje del av processen eller det operativa förloppet för att utröna hur en avvikelse från avsedd funktion kan uppstå.
- Bestäm om dessa avvikelser kan leda till olyckor eller tillbud.

HAZOP genomförs lämpligen ett antal gånger under utvecklingen för att på detta sätt återföra informationen till konstruktionsansvariga successivt och därigenom erhålla ett säkrare system. Eftersom HAZOP är en relativt enkel analys kan den utföras tidigt i konstruktionsarbetet.

Analysen omfattar följande steg:

1. Definiera analysens omfattning, vilka delprocesser eller operativa förlopp som ska omfattas.
2. Samla en grupp av personer som tillsammans utför analysen. Gruppen består lämpligen av både konstruktörer och användare/operatörer som kan bedöma effekterna av en avvikelse från den avsedda funktionen.
3. Samla all relevant dokumentation som beskriver processen eller det operativa förloppet (flödesschema, ritningar, användarmanualer, underhållsmanualer och skyddsinstruktioner).
4. Analysera varje delprocess eller operativt förlopp genom att tillämpa de fördefinierade ledorden (guide words) som leder till processpecifika avvikelser (deviations), ange möjlig orsak,

konsekvensen av avvikelsen samt erforderlig åtgärd. Följande sammanfattar arbetsgången:

4.1. Välj en delprocess eller operativt förlopp.

4.2. Ange avsedd funktion vid processen.

4.3. Tillämpa första ledordet.

4.4. Bestäm vilken avvikelse som uppstår.

4.5. Ange möjlig orsak.

4.6. Ange konsekvensen.

4.7. Ange erforderlig åtgärd.

4.8. Upprepa steg *4.3–4.7* tills inga nya avvikelser kan bestämmas.

4.9. Tillämpa nästa ledord.

4.10. Upprepa steg *4.3–4.7* tills inga nya avvikelser kan bestämmas.

4.11. Upprepa *4.9–4.10* tills alla ledord är uttömda.

Ledorden måste bestämmas för varje aktuell process eller operativt förlopp. På bilden nedan anges några fördefinierade ledord med sina definitioner.

Tabell 8:1 Ledordstabell

Ledord	Definition
Ingen/ingen	ingen funktion uppnås
Mer	en kvantitativ ökning av utresultatet
Mindre	en kvantitativ minskning av utresultatet
Såväl som	en kvalitativ ökning
Del av	en kvalitativ minskning
Omvänd	motsatt effekt
Annan/annat	något annat än avsedd funktion

Följande är ett exempel på en del av en HAZOP där endast det första ledordet ”ingen” har tillämpats.

Tabell 8:2 Exempel på HAZOP

Ledord	Avvikelse	Möjlig orsak	Konsekvens	Åtgärd
Ingen/inget	Ingen säkring	1. Felaktigt handhavande	Risk för våda-avfyring	a) Inför instruktion i manualen b) Inför avsnitt i utb-planen
		2. Spärren saknas	Som 1	a) Ändra konstruktionen

Bilaga 1 Exempel på beslutsdokument

Syfte

I detta avsnitt lämnas enkla exempel på utformning av systemsäkerhetsutlåtande, *5.27*, systemsäkerhetsgodkännande, *5.31*, säkerhetsintyg, *5.31* och centralt systemsäkerhetsbeslut, *5.33*, i texten nedan sammanfattande benämnda ”Beslutshandling”.

Omfattning av viss beslutshandling, utöver vad som framgår av här redovisade exempel, kravställs särskilt av uppdragsgivare (Försvarsmakten i kundbeställning (KB), DesignA i RFP).

Vissa grundläggande principer enligt nedan styr utformningen av beslutshandling, jämför exempel i avsnitten *Systemsäkerhetsutlåtande –Säkerhetsintyg*.

Benämning på beslutshandling är alltid ”ren” det vill säga utan epitet i form av ”tillfällig”, ”preliminär”, ”slutlig”, ”tidsbegränsad” eller motsvarande. Istället anges i rubriken på beslutshandling vilket tekniskt system som avses. Till exempel ”Systemsäkerhetsutlåtande för Eldkastare 01, försöksutförande typ E”.

Tidsbegränsningar används endast i undantagsfall då det tekniska systemet är att betrakta som färskvara. De övriga begränsningar som varje beslutshandling med nödvändighet måste innehålla avseende omfattningen av tekniskt system och dess nyttjande redovisas direkt i själva beslutshandlingen.

Det aktuella tekniska systemet definieras till sin omfattning och ingående delar/delsystem/och eventuella tillbehör (större/ säkerhetsrelaterade) för att klart redovisa vad som omfattas av genomförd systemsäkerhetsverksamhet och av beslutshandlingen.

Det tekniska systemet identifieras genom att ange benämning, beteckning, typnummer, märkning, hänvisning till tekniskt underlag där det tekniska systemet beskrivs utförligt, samt motsvarande för ingående delsystem och eventuella säkerhetsrelaterade tillbehör.

För användandet identifieras de driftsfaser, användningssätt och yttre förhållanden för vilka det tekniska systemet är avsett, samt i förekommande fall drivmedel, ammunitionstyper och motsvarande, vilka är kvalificerade för att användas tillsammans med det tekniska systemet.

I beslutshandlingen anges eventuell samfunktion med annat tekniskt system som har kvalificerats (till exempel att en viss eldkastare även är tillåten att användas från visst fordon).

I de fall till exempel DesignA har uppdragits att för visst tekniskt system ta fram ett systemsäkerhetsgodkännande, men det tekniska systemets olycksrisker inte uppfyller ställda krav, lämnas rapport i form av ett **säkerhetsmeddelande** med förslag till Försvarsmakten om lämpliga åtgärder.

Provturskommando (PTK) under SS, *5.31* innehåller ett beslutsdokument vilket benämns **säkerhetsintyg**. Intyget utfärdas av DesignA och innebär att DesignA efter granskning av alla relevanta omständigheter har funnit att det fartyg som PTK ska prova har godtagbar säkerhet. Ett exempel på säkerhetsintyg lämnas i avsnittet *Säkerhetsintyg*.

Sändlista på beslutshandling bör generellt omfatta de instanser som är berörda av beslutet. Bland annat den uppdragsgivare som ställt uppgiften avseende framtagning av beslutshandlingen. Förband och SSWG-2, *5.8* erhåller systemsäkerhetsdokumentation som bilagor till Beslut om användning (BOA).

Samtliga här redovisade exempel finns som word-filer i H SystSäk CDR.

Systemsäkerhetsutlåtande

Exempel på leverantörs systemsäkerhetsutlåtande

PETTERSSONS SMIDE AB
Simpevarp

SYSTEMSÄKERHETSUTLÅTANDE
20XX-06-15

dnr 102/-XX

Systemsäkerhetsutlåtande för eldkastare VULKANUS mod/01 med typnummer 700-953 (3 bilagor)

1 Identifiering av det tekniska systemet

1.1 Benämning

Benämning: ”Eldkastare VULKANUS”.

Modellbeteckningen: ”mod/01”.

Typnummer: ”700-953”.

1.2 Omfattning

Det tekniska systemet består av Bränsletank (artikelnummer 700-953-001), strålrör med slangpaket (artikelnummer 700-953-002) samt tre olika bränslen (artikelnummer 700-953-003--005).

1.3 Utförande

Det tekniska systemets tekniska utförande framgår av teknisk dokumentation inklusive ritningsunderlag. Den tekniska dokumentationens beteckning är ”ggggggg-vvvv-01” och ingår som bilaga 1.

Skiljaktighet, jämfört med närmast tidigare version (Eldkastare VULKANUS, försöksutgåva, typnummer 600-01) består i att tändspolen har ersatts med en nykonstruerad tändspole med motsvarande funktion men annat inre verkningssätt. Härigenom har högre funktionssäkerhet uppnåtts och olycksrisk för personskada har reducerats till tolerabel risknivå.

1.4 Märkning

Skylt med uppgifter enligt pkt 1.1 är anbringad på eldkastarens bränsletank.

1.5 Användning

Det tekniska systemet är avsett att användas för alla de driftsfaser samt under alla de yttre förhållanden som redovisas i beskrivningsbok med beteckning ”ggggggg-vvvv-02” vilken ingår som bilaga 2 här.

2 Underlag

2.1 SSPP och SAR

DesignA krav på leverantörs genomförande av systemsäkerhetsverksamhet framgår av Systemsäkerhetsplan 20XX-05-20 (Pettersson Smide AB dnr 101/-XX till vilken hänvisas i DesignA beställning). Resultat av genomförd systemsäkerhetsverksamhet är dokumenterad i Systemsäkerhetsrapport (SAR), (Pettersson Smide AB dnr 101/-XX). Under 3 nedan lämnas sammanfattningar av väsentliga delar av Systemsäkerhetsrapporten.

2.2 Systemsäkerhetskrav

De systemsäkerhetskrav som tillämpats vid systemsäkerhetsverksamheten utgörs av:

- Beställarens krav enligt punkt Systemsäkerhetskrav i anbudsförfrågan samt motsvarande punkt i vårt anbud (Pettersson Smide AB dnr 151/-08.)

- Tillämplig svensk lagstiftning samt föreskrifter från Kemikalieinspektionen, Naturvårdsverket samt Myndigheten för Samhällsskydd och beredskap, vilka samtliga har förtecknats i SAR. SAR utgör bilaga 3 till detta systemsäkerhetsutlåtande.

2.3 Klassificering av olycksrisker

Vid klassificering av olycksrisker har metodik enligt Försvarsmaktens Handbok Systemsäkerhet 2011 tillämpats.

3 Genomförd systemsäkerhetsverksamhet

3.1 Identifiering av olycksrisker med analys och provning

För identifiering av olycksrisker har Risklogg framtagits, vari har dokumenterats identifierade riskkällor och farliga tillstånd. Preliminär riskkälleanalys har genomförts. Här identifierade tänkbara vådahändelser har analyserats med hjälp av felträd respektive feleffektanalys. Resultat från samtliga analyser och prov har dokumenterats i det tekniska systemets Risklogg.

Konstruktionens känslighet mot såväl normal miljö som abnorma miljöer enligt kravspecifikation har provats vid praktisk provning.

Analys- och provningsresultat har fortlöpande utnyttjats i konstruktionsarbetet.

Härvid har samtliga enkelfel kunnat elimineras genom omkonstruktion.

Inga common cause-fel har kunnat konstateras.

3.2 Riskreducerande åtgärder

Ett stort antal riskreducerande åtgärder har vidtagits och inarbetats i konstruktionen (se förteckning i SAR).

Den viktigaste åtgärden bedöms vara införande av composit-bränsle. Bränslet (vätska) består av två stabila, relativt okänsliga komponenter som först vid blandning intar egenskaper som krävs av ett effektivt bränsle, vilket innebär att det därvid blir högkänsligt för yttre stimuli, får låg flampunkt mm. De två komponenterna förvaras i separata behållare vid kastaren och blandas först i strålröret under eldgivning.

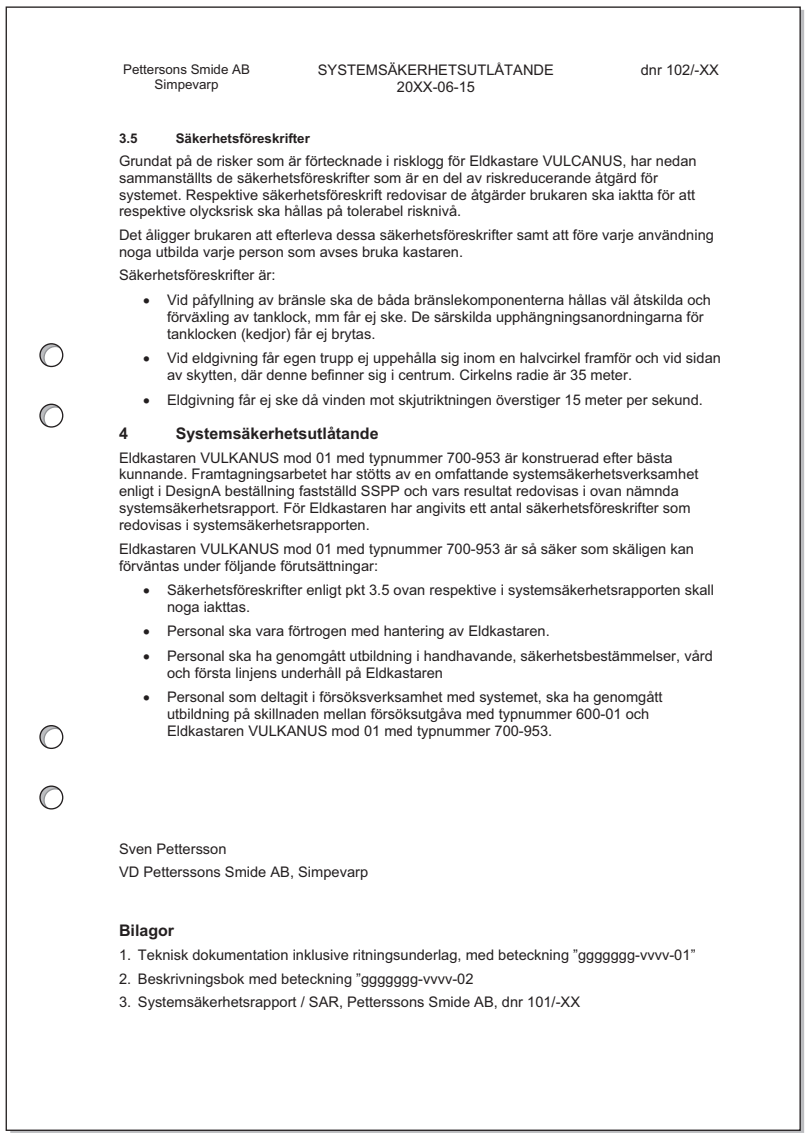
3.3 Tänkbara vådahändelser, kvarvarande risker

Förteckning över tänkbara vådahändelser är framtagen genom preliminär analys av riskkällor och farliga tillstånd och redovisas i SAR. Denna förteckning avser av Pettersson Smide AB typgodkänd produkt (enligt Typgodkännande dnr 121/-XX) och presenterar olycksrisker på systemnivå, vid växelverkan mellan delsystem samt över systemnivå genom växelverkan mellan det tekniska systemet och de fordon detta skall kunna monteras på.

För varje vådahändelse respektive farligt tillstånd har identifierats aktuella olycksrisker samt har angivits de säkerhetsbestämmelser som erfordras till förhindrande av olycka, ohälsa, sjukdom, systemförlust respektive skada på yttre miljö. Förteckning över säkerhetsbestämmelser ingår i SAR vilken utgör bilaga 3 till detta systemsäkerhetsutlåtande.

3.4 Farliga ämnen/material

Samtliga farliga ämnen/ material har identifierats genom analys jämlikt gällande lag och föreskrift samt Försvarsmaktens särskilda miljökrav enligt krav i anbudsförfrågan.



Pettersons Smide AB
Simpevarp

SYSTEMSÄKERHETSUTLÅTANDE
20XX-06-15

dnr 102/-XX

3.5 Säkerhetsföreskrifter

Grundat på de risker som är förtecknade i risklogg för Eldkastare VULCANUS, har nedan sammanställts de säkerhetsföreskrifter som är en del av riskreducerande åtgärd för systemet. Respektive säkerhetsföreskrift redovisar de åtgärder brukaren ska iaktta för att respektive olycksrisk ska hållas på tolerabel risknivå.

Det åligger brukaren att efterleva dessa säkerhetsföreskrifter samt att före varje användning noga utbilda varje person som avses bruka kastaren.

Säkerhetsföreskrifter är:

- Vid påfyllning av bränsle ska de båda bränslekomponenterna hållas väl åtskilda och förväxling av tanklock, mm får ej ske. De särskilda upphängningsanordningarna för tanklocken (kedjor) får ej brytas.
- Vid eldgivning får egen trupp ej uppehålla sig inom en halvcirkel framför och vid sidan av skytten, där denne befinner sig i centrum. Cirkelns radie är 35 meter.
- Eldgivning får ej ske då vinden mot skjutriktningen överstiger 15 meter per sekund.

4 Systemsäkerhetsutlåtande

Eldkastaren VULKANUS mod 01 med typnummer 700-953 är konstruerad efter bästa kunnande. Framtagningsarbetet har stötts av en omfattande systemsäkerhetsverksamhet enligt i DesignA beställning fastställd SSPP och vars resultat redovisas i ovan nämnda systemsäkerhetsrapport. För Eldkastaren har angivits ett antal säkerhetsföreskrifter som redovisas i systemsäkerhetsrapporten.

Eldkastaren VULKANUS mod 01 med typnummer 700-953 är så säker som skäligen kan förväntas under följande förutsättningar:

- Säkerhetsföreskrifter enligt pkt 3.5 ovan respektive i systemsäkerhetsrapporten skall noga iakttas.
- Personal ska vara förtrogen med hantering av Eldkastaren.
- Personal ska ha genomgått utbildning i handhavande, säkerhetsbestämmelser, vård och första linjens underhåll på Eldkastaren
- Personal som deltagit i försöksverksamhet med systemet, ska ha genomgått utbildning på skillnaden mellan försöksutgåva med typnummer 600-01 och Eldkastaren VULKANUS mod 01 med typnummer 700-953.

Sven Pettersson

VD Petterssons Smide AB, Simpevarp

Bilagor

1. Teknisk dokumentation inklusive ritningsunderlag, med beteckning ”gggggggg-vvvv-01”
2. Beskrivningsbok med beteckning ”gggggggg-vvvv-02
3. Systemsäkerhetsrapport / SAR, Petterssons Smide AB, dnr 101/-XX

Några kommentarer till systemsäkerhetsutlåtande

Om inga krav har ställts på tidpunkt för överlämnande av systemsäkerhetsutlåtande, *5.27*, så ska strävan vara att systemsäkerhetsutlåtandet överlämnas så tidigt som möjligt. Senast i samband med att första serieexemplar produceras bör systemsäkerhetsutlåtandet kunna överlämnas till DesignA.

Försöksmateriel hanteras på motsvarande sätt som seriemateriel. Dock att dokumentationen inte kan vara lika omfattande eller att möjliga användningsområden respektive användningsmiljöer/ abnorma miljöer inte kan/behöver vara fullständiga jämfört med seriematerielen.

Framtagning av systemsäkerhetsutlåtande för försöksmateriel fungerar närmast som en generalrepetition inför framtagningen av systemsäkerhetsutlåtande för till exemepel serieexemplaret.

Vid komplexa eller säkerhetskritiska system kommer DesignA genom sin SSWG-1, *5.8* att följa upp att systemsäkerhetsplanen följs av leverantör under utvecklings- och konstruktionsfasen.

Systemsäkerhetsgodkännande

Exempel på DesignA:s systemsäkerhetsgodkännande

ÖPPEN

Datum	FMV Dokumentbeteckning	Utgåva
2010-04-09	ÄÄFMVXXXX-1	1.0
	Ansv område/Enhet	Klassificeringsnr
		Sida
		1 (3)

Försvarsmakten/PROD

Systemsäkerhetsgodkännande av Eldkastare VULKANUS mod 01; M2101-xxxxxx (9 bilagor)

1 Identifiering av det tekniska systemet

1.1 Benämning och modellbeteckning

Det tekniska systemet benämnes ”Eldkastare VULKANUS”.

Modellbeteckningen är ”mod 01”

Det tekniska systemet har typnummer ”700-953”

Förrådsbeteckning: M2101-xxxxxx

Förrådsbenämning: Eldkastare VULKANUS mod 01.

1.2 Det tekniska systemets omfattning

Det tekniska systemet består av Bränsletank (artikelnummer 700-953-001), strålrör med slangpaket (artikelnummer 700-953-002) samt tre olika bränslen (artikelnummer 700-953-003--005).

1.3 Tekniskt utförande

Det tekniska systemets tekniska utförande som framgår av teknisk dokumentation inklusive ritningsunderlag har beteckning ”vvvvvvv-gggg-01” och ingår som bilaga 1.

Skiljaktighet, jämfört med tidigare försöksutgåva (Eldkastare VULKANUS, försöksutgåva, typnummer 600-101) består i att enhet xxxx är ersatt med en enhet med motsvarande funktion men med internt helt annorlunda verkningssätt. Härigenom har en högre funktionssäkerhet erhållits samt har olycksrisken för personskada nedbringats till kravställd nivå.

1.4 Märkning

Skylt med uppgifter enligt pkt 1.1 är anbringade på eldkastarens bränsletank.

1.5 Användning

Det tekniska system kan användas för alla de operationsfaser och under de yttre förutsättningar som redovisas i beskrivningsbok med beteckning ”vvvvvvv-gggg-02” vilken ingår som bilaga 2.

FMV Mall Upprättad handling/Utgåva nr 11.0

FMV
Försvarets materielverk
115 88 Stockholm
Besöksadress: Banérgatan 62
Tel: 08-782 40 00
Fax: 08-667 57 99
registrator@fmv.se
www.fmv.se
Org.nr: 202100-0340

ÖPPEN

Datum	FMV Dokumentbeteckning	Utgåva
2010-04-09	ÅÅFMVXXXX-1	1.0
	Ansv område/Enhet	Klassificeringsnr
		Sida 2 (3)

2 Omfattning

Detta systemsäkerhetsgodkännande omfattar följande delgodkännanden:

a) Systemsäkerhetsgodkännande för det tekniska systemet Eldkastare VULKANUS enligt bilaga 3.

b) Systemsäkerhetsgodkännande för Eldkastare VULKANUS´s installation på Stridsfordon 90 och lätt pansarbil 2000 enligt bilaga 5 och 6.

3 Underlag

Leverantörs systemsäkerhetsarbete enligt fastställd Systemsäkerhetsplan har fortlöpande följts upp och i förekommande fall omriktats av Projektledningens Systemsäkerhetsgrupp (SSWG-1).

Leverantörs Systemsäkerhetsutlåtande, inklusive säkerhetsanalyser och risklogg, har granskats och befunnits på ett korrekt sätt beskriva säkerhetsarbetet och kvarstående olycksrisker.

4 Säkerhetsbestämmelser

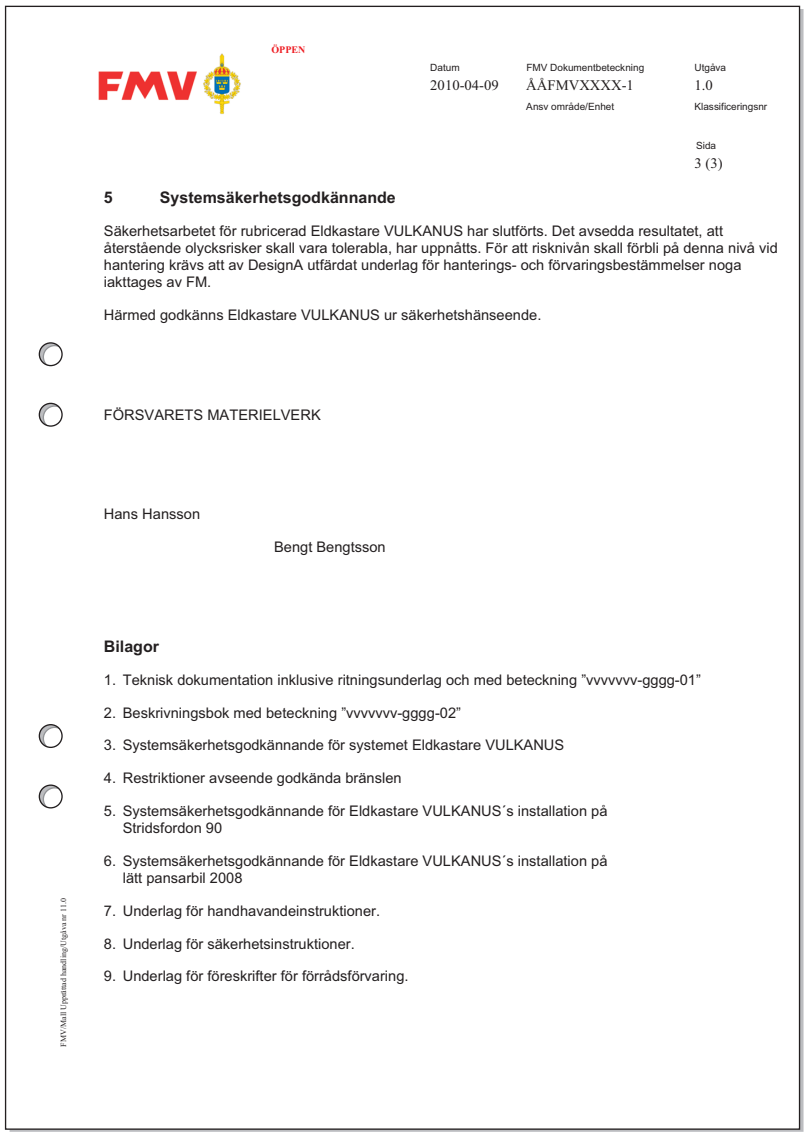
För innehållande av tolerabel risknivå erfordras ett antal säkerhetsbestämmelser. Dessa framgår av följande dokumentation:

Godkända bränslen enligt bilaga 4

Underlag för handhavandeinstruktioner enligt bilaga 7.

Underlag för säkerhetsinstruktioner enligt bilaga 8.

Underlag för föreskrifter för förrådsförvaring enligt bilaga 9.



ÖPPEN

FMV

Datum	FMV Dokumentbeteckning	Utgåva
2010-04-09	ÄÄFMVXXXX-1	1.0
	Ansv område/Enhet	Klassificeringsnr
		Sida 3 (3)

5 Systemsäkerhetsgodkännande

Säkerhetsarbetet för rubricerad Eldkastare VULKANUS har slutförts. Det avsedda resultatet, att återstående olycksrisker skall vara tolerabla, har uppnåtts. För att risknivån skall förbli på denna nivå vid hantering krävs att av DesignA utfärdat underlag för hanterings- och förvaringsbestämmelser noga iakttages av FM.

Härmed godkänns Eldkastare VULKANUS ur säkerhetshänseende.

FÖRSVARETS MATERIELVERK

Hans Hansson

Bengt Bengtsson

Bilagor

1. Teknisk dokumentation inklusive ritningsunderlag och med beteckning ”vvvvvvv-gggg-01”
2. Beskrivningsbok med beteckning ”vvvvvvv-gggg-02”
3. Systemsäkerhetsgodkännande för systemet Eldkastare VULKANUS
4. Restriktioner avseende godkända bränslen
5. Systemsäkerhetsgodkännande för Eldkastare VULKANUS´s installation på Stridsfordon 90
6. Systemsäkerhetsgodkännande för Eldkastare VULKANUS´s installation på lätt pansarbil 2008
7. Underlag för handhavandeinstruktioner.
8. Underlag för säkerhetsinstruktioner.
9. Underlag för föreskrifter för förrådsförvaring.

FMV Mall Upprättad handl/lag Utgåva ser 11.0

Några kommentarer till systemsäkerhetsgodkännande

Tidpunkt: Vilken är möjlig tidpunkt? Leverantörs systemsäkerhetsutlåtande, *5.27* kan inte erhållas före det att prototypen är utprovad och klar. Oftast inte förrän det att serietypprov är klart.

Vad är Försvarsmaktens krav? Naturligtvis vill Försvarsmakten ha DesignA:s underlag så fort som möjligt. Försvarsmakten ska ju ta fram sin dokumentation innan materielen kan användas vid

förband. Lösningen kan vara samarbete så att underlagsdokumentationen tas fram successivt och förankras hos Försvarsmakten genom preliminär dokumentation. Härigenom får Försvarsmakten möjlighet att påbörja sitt arbete med framtagning av CSSB. Jämför nedan under försöksmateriel.

Försöksmateriel. Framtagning av system är som regel en komplex process under lång tid. Processen innehåller ofta flera moment av successiva truppförsök innan serieexemplar kan överlämnas till Försvarsmakten. Före varje överlämning till Försvarsmakten av system för truppförsök ska systemsäkerhetsgodkännande beslutas. Det är dock tillräckligt att antalet bilagor jämfört med exemplet ovan samt innehållet i dessa anpassas till den verksamhet och de förhållanden som är relevant för hur system i varje enskilt fall avses användas. Detta preciseras i systemsäkerhetsgodkännandet, *5.31*.

Centralt systemsäkerhetsbeslut

Exempel på utformning av Försvarsmaktens centrala systemsäkerhetsbeslut

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2010-04-06

HKV beteckning
14 910: XXXXX

Sida 1 (3)

Sändlista

Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning
Sven Svensson

MS 895 Centralt Systemsäkerhetsbeslut för det tekniska systemet Eldkastare VULKANUS, mod 01, M2101-xxxxxx (3 bilagor)

1 Identifiering av det tekniska systemet

1.1 Benämning och modellbeteckning

Det tekniska systemet benämnes ”Eldkastare VULKANUS”.
Modellbeteckningen är ”mod 01”
Det tekniska systemet har typnummer ”700-953”
Förrådsbeteckning: M2101-xxxxxx
Förrådsbenämning: Eldkastare VULKANUS mod 01.

1.2 Det tekniska systemets omfattning

Det tekniska systemet består av Bränsletank (artikelnummer 700-953-001), strålrör med slangpaket (artikelnummer 700-953-002) samt tre olika bränslen (artikelnummer 700-953-003--005).

1.3 Det tekniska systemets utförande

Det tekniska systemets tekniska utförande som framgår av teknisk dokumentation inklusive ritningsunderlag har beteckning ”vvvvvvv-gggg-01” och ingår som bilaga 1.

Skiljaktighet, jämfört med tidigare försöksutgåva (Eldkastare VULKANUS, försöksutgåva, typnummer 600-101) består i att enhet xxxx är ersatt med en enhet med motsvarande funktion men med internt helt annorlunda verkningssätt. Härigenom har en högre funktionssäkerhet erhållits samt olycksrisken för personskada har nedbringats till en tolerabel nivå.

(PAS)

Postadress	Besöksadress	Telefon	Telefax	E-post, Internet
107 85 STOCKHOLM	Lidingövägen 24	08-788 75 00	08-788 77 78	exp-hkv@mil.se www.hkv.mil.se

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2010-04-06

HKV beteckning
14 910: XXXXX

1.4 Märkning

Skylt med uppgifter enligt pkt 1.1 är anbringade på eldkastarens bränsletank.

För att möjliggöra materiel- och skaderapportering med handhållen fältutrustning (mikro-dataterminal) är samtliga delar märkta med streckkod.

1.5 Användning

Det tekniska systemet kan användas för alla de driftsfaser och yttre förutsättningar som Reglemente för eldkastare VULKANUS mod 01 med diarienummer vvvvvvvvvvvvv-lllllll anger.

2 Bakgrund

DesignA har med skrivelse Avdelning 14 910:XXXX beslutat om säkerhetsgodkännande för systemet Eldkastare VULKANUS mod 01, M2101-xxxxxx. DesignA har därvid även överlämnat restriktioner för användning samt underlag för FM utarbetande av instruktioner och Säkerhetsbestämmelser för hantering.

3 SSWG-2

Arbetsgrupp Systemsäkerhet (SSWG-2) samt uppgifter för denna är beslutad. Arbetsgruppens uppgifter och bemanning framgår av bilaga 2

4 Restriktioner och kompletterande säkerhetsbestämmelser

Restriktion: Eldkastaren får endast användas med vatten som ammunition intill dess att godkänd ammunition har fastställts.

Kompletterande säkerhetsbestämmelse: Vid skjutning med vatten är minsta skjutavstånd mot person 15 meter.

5 Samråd

C MARKI har tecknat samråd.

6 Centralt systemsäkerhetsbeslut

Chefen för PROD Armé beslutar härmed om Central systemsäkerhetsbeslut för eldkastare VULKANUS mod 01 som underlag för FM Beslut om användning.

Härvid skall tillämpas de instruktioner för det tekniska systemet och ingående delsystem som framgår av materielbeskrivningar (motsv.), reglementen och instruktioner. Nu gällande publikationer förtecknas i bilaga 3.

FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2010-04-06

HKV beteckning
14 910: XXXXX

Sida 3 (3)

Det tekniska systemet kan användas buret av person, det kan monteras på stridsfordon 90 respektive lätt pansarbil 2000.

Det tekniska utförandet/versionen är härmed fastställt och får ej ändras utan nytt Central systemsäkerhetsbeslut av Chefen för PROD Armé. Det tekniska utförandet framgår av bilaga 1.

Beslut avseende ovanstående instruktioner i säkerhetsinstruktionen har fattats med stöd av FM ArbO.

Carl Carlsson
Enhetschef

Sven Svensson
MSA

Bilagor

1. DesignA systemsäkerhetsgodkännande.
2. Arbetsgrupp Systemsäkerhet, (SSWG-2) uppgifter och företrädare.
2. Gällande publikationer

Sändlista:
PROD
FMV

För kännedom inom HKV
SÄKINSP
GL
LEDS
INS

Några kommentarer till centralt systemsäkerhetsbeslut

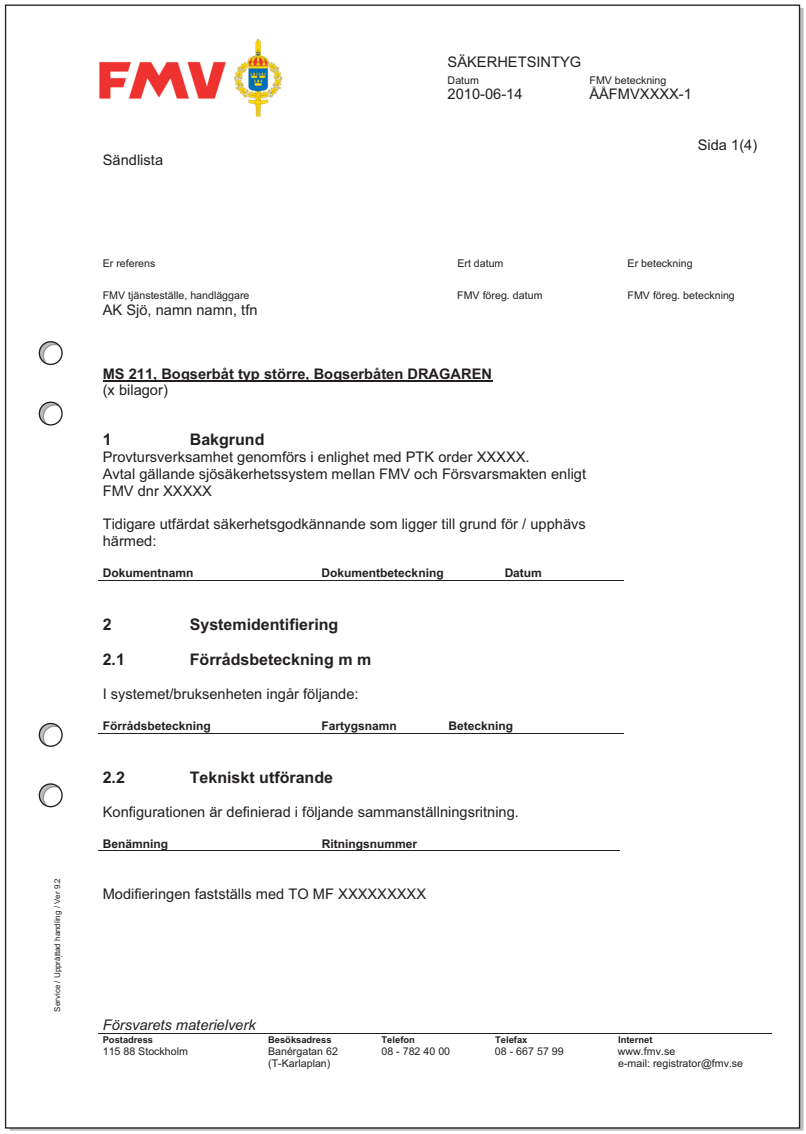
Tidpunkt: Vilken är möjlig tidpunkt? Leverantörs systemsäkerhetsutlåtande, *5.27* kan inte komma innan det att prototypen är utprovad och klar. Oftast inte förrän att serietypprov är klart. Först därefter kan DesignA:s systemsäkerhetsgodkännande, *5.31*

Försvarsmaktens krav. Naturligtvis vill Försvarsmakten ha DesignA:s underlag så fort som möjligt. Försvarsmakten ska ju ta fram sin dokumentation och centralt systemsäkerhetsbeslut, *5.33* innan materielen kan användas vid förband. Lösningen kan vara samarbete så att underlagsdokumentationen tas fram successivt och remissarbete/förankring hos Försvarsmakten med preliminär dokumentation görs innan DesignA:s säkerhetsgodkännande beslutas. Härigenom får Försvarsmakten möjlighet att påbörja arbetet med framtagning av dokumentation enligt punkt 4 och 6 i exemplet. Jämför nedan under försöksmateriel.

Försöksmateriel. Framtagning av system är som regel en komplex process under lång tid. Processen innehåller ofta flera moment av successiva truppförsök innan serieexemplar kan erhållas. Före varje truppförsök (serie av försök) med viss ”försöksutgåva” av system ska centralt systemsäkerhetsbeslut, *5.33* fattas. Det är dock tillräckligt att underlaget enligt 3 och 4 i exemplet ovan begränsas till den verksamhet och de förhållanden under vilka system i varje enskilt fall avses användas.

Säkerhetsintyg

Exempel på utformning av DesignA:s säkerhetsintyg



SÄKERHETSINTYG
Datum 2010-06-14
FMV beteckning ÄÄFMVXXXX-1

Sida 1(4)

Sändlista

Er referens | Ert datum | Er beteckning

FMV tjänsteställe, handläggare
AK Sjö, namn namn, tfn
FMV föreg. datum | FMV föreg. beteckning

MS 211, Bogserbåt typ större, Bogserbåten DRAGAREN
(x bilagor)

1 Bakgrund

Provtursverksamhet genomförs i enlighet med PTK order XXXXX.
Avtal gällande sjösäkerhetssystem mellan FMV och Försvarsmakten enligt FMV dnr XXXXX

Tidigare utfärdat säkerhetsgodkännande som ligger till grund för / upphävs härmed:

Dokumentnamn	Dokumentbeteckning	Datum

2 Systemidentifiering

2.1 Förrådsbeteckning m m

I systemet/bruksenheten ingår följande:

Förrådsbeteckning	Fartygsnamn	Beteckning

2.2 Tekniskt utförande

Konfigurationen är definierad i följande sammanställningsritning.

Benämning	Ritningsnummer

Modifieringen fastställs med TO MF XXXXXXXXX

Service / Upprättad handling / Ver 6.2

Försvarets materielverk

Postadress	Besöksadress	Telefon	Telefax	Internet
115 88 Stockholm	Banérgatan 62 (T-Karlaplan)	08 - 782 40 00	08 - 667 57 99	www.fmv.se e-mail: registrator@fmv.se

2.3 Märkning, spårbarhet m m

Samtliga enheter har tilldelats militär beteckning enligt följande:

Förrådsbenämning	Förrådsbeteckning	Beteckning

2.4 Underlag / Publikationer

Följande publikationer är tillämpliga vid användning, vård och underhåll av systemet:

Förrådsbenämning	Förrådsbeteckning	Anmärkning

2.5 Omfattning av systemsäkerhetsarbetet

Systemsäkerhetsverksamheten samt detta säkerhetsgodkännande omfattar genomförda nyinstallationer samt modifieringar och deras integration i befintligt system.

2.6 Gränsytor till andra system/bruksenheter

Dokumentnamn	Dokumentbeteckning	Datum

3 Användningsområde

Provtursorder och provföreskrifter framgår av XXXX

Användningsområdet för systemet definieras i YYYY

4 Beskrivning av genomfört systemsäkerhetsarbete

4.1 Allmänt

Leverantörens systemsäkerhetsarbete har fortlöpande följts och befunnits vara tillfredsställande. Utfärdat säkerhetsutlåtande har granskats och befunnits på ett korrekt sätt beskriva genomfört säkerhetsarbete och återstående risker.

4.2 Registreringsbesiktning/Certifiering

4.3 Delgodkännanden, värdighetsgodkännanden m m

SÄKERHETSINTYG

Datum 2010-06-14

FMV beteckning ÄÄFMVXXXX-1

5 Kravuppfyllnad

Bedömning av tolerabel risknivå har skett enligt systemsäkerhetskrav i HKV skrivelse XXXX / TTEM YYY.

Tolerabel risknivå har, med iakttagande av angivna restriktioner, uppnåtts för alla risker.

6 Restriktioner

För innehållande av tolerabel risknivå skall…….

Före nyttjande skall fartyget ha godkänd sjövärdighetsbesiktning av Marinens fartygsinspektion.

7 Säkerhetsintyg

Säkerhetsarbetet är slutfört. I de fall detta arbete fortskrider syftar det till att avlägsna restriktioner enligt avsnitt 6 ovan.

I säkerhetsutlåtande ”angivna åtgärder” för att bringa risker till tolerabel nivå, har implementerats. Konstruktiva åtgärder är genomförda, handhavande och underhållspublikationer har uppdaterats och varningsskyltar satts upp enligt ”angivna åtgärder” i säkerhetsutlåtandet.

För att bibehålla risknivån krävs att hanterings- och handhavande-bestämmelser, materielvårdsföreskrifter samt restriktioner enligt ovan följs.

Militära sjösäkerhetsinspektionen har tecknat samråd på detta Säkerhetsintyg.

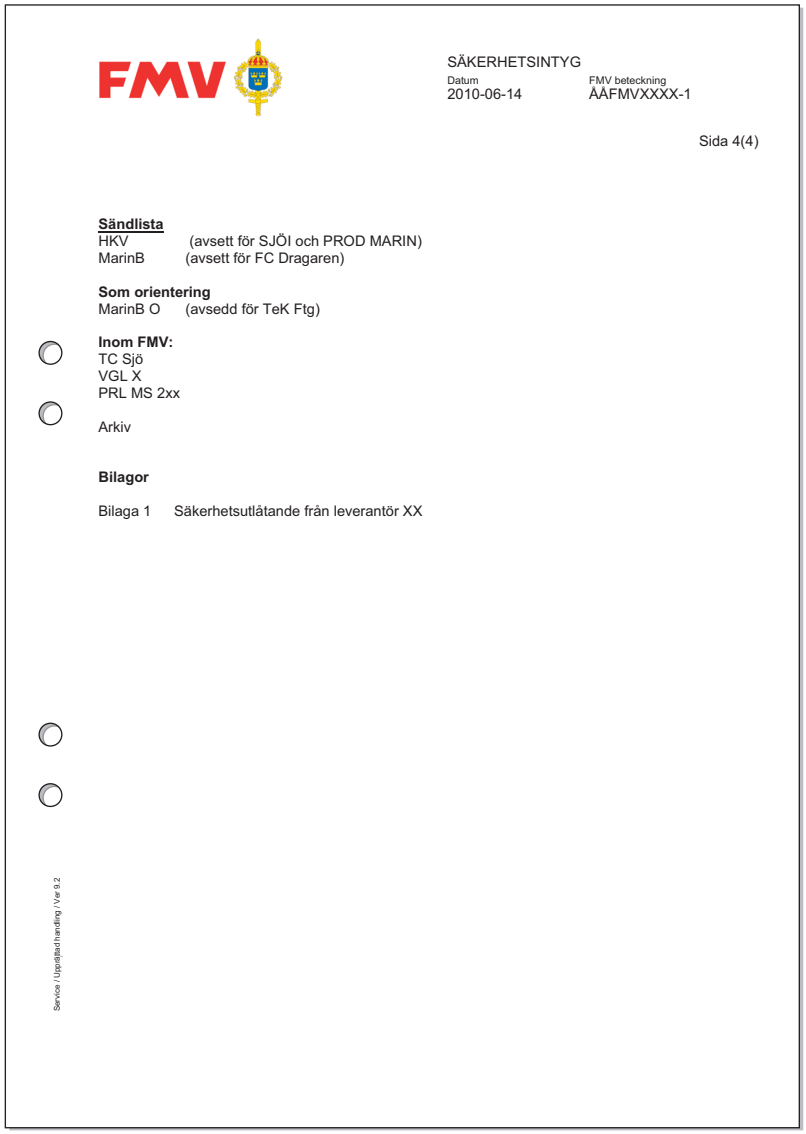
Härmed godkänns bogserbåten Dragaren ur säkerhetshänseende.

Beslut i detta ärende har fattats av X nn. Föredragande har varit PRL MS 2XX nn, och i den slutliga beredningen har PRL nn och PRL nn deltagit.

FÖRSVARETS MATERIELVERK

nn
VGL x

nn
PRL MS 2xx



FMV

SÄKERHETSINTYG

Datum 2010-06-14

FMV beteckning ÄÄFMVXXXX-1

Sida 4(4)

Sändlista
HKV (avsett för SJÖI och PROD MARIN)
MarinB (avsett för FC Dragaren)

Som orientering
MarinB O (avsedd för TeK Ftg)

Inom FMV:
TC Sjö
VGL X
PRL MS 2xx

Arkiv

Bilagor

Bilaga 1 Säkerhetsutlåtande från leverantör XX

Service / Upphandlingshandling / Ver 9.2

Några kommentarer till säkerhetsintyg

Tidpunkt: Om inga andra krav har ställts i detta avseende överlämnas Säkerhetsintyget, *5.31* till Försvarsmakten innan PTK börjar använda fartyget för sjögående verksamhet.

Definitioner

För att underlätta förståelsen av i handboken använda begrepp och akronymer lämnas nedanstående ordförklaringar. Svensk standard SS 441 05 05, MIL-STD-882C samt facklitteratur inom systemsäkerhetsområdet, har utgjort underlaget för flertalet av dessa förklaringar. Det bör observeras att några termer har något skilda definitioner i olika standarder. Det föreligger exempelvis skillnader mellan svensk standard och amerikansk militär standard.

Ett antal definitioner är handbokens egna.

Begrepp	Förklaring
ALARP	As low as reasonable practicable, så låg som praktiskt och rimligt möjligt (avser en viss risk). Ett begrepp som används i brittisk lagstiftning, innebär att åtgärder för att minska en viss risk ska fortsättas så länge som insatsen ger märkbar effekt på risken till rimlig kostnad.
Allvarlig personskada *Serious injury*	Skada med bestående förlust av kroppsfunktion/kroppsdel.
Allvarligt fel *Serious defect*	Avvikelse från givna fordringar i fråga om viss egenskap och som därmed kan leda till ett osäkert tillstånd.
Ammunition *Ammunition*	Materiel/tekniskt system avsett för skadeverkan, rök- eller lysverkan, sprängning, minering, minröjning samt materiel/ tekniskt system som vid utbildning ersätter denna. Materielen/det tekniska systemet kan innehålla explosivämnen eller andra kemikalier.
Anläggning *Facility*	För viss funktion eller verksamhet iordningställt markområde, byggnad eller utrymme jämte för funktionen eller verksamheten erforderliga installationer, till exempel befästning, kasernetablissement, basområde, förbindelser med mera. Med anläggning avses även de truppbefästningar som behövs för att lösa uppgiften. Till anläggning hänförs även anläggningsbundna förnödenheter.
Användningsmiljö *Operational environment*	Faktisk omgivning till visst tekniskt system. Kan utgöras av andra tekniska system, strömförsörjning (spänning, frekvens, strömstyrka), vatten, avlopp, kemiska förhållanden, drivmedelsförsörjning, reparationsmöjligheter, flygtrafikledning med mera.

Begrepp	Förklaring
Aversionsfaktor *Aversion factor*	Innebär här att allvarlig olycka tolereras i lägre utsträckning än motsvarande olycka som resulterar i lindriga skador.
Barriär *Barrier*	Skyddsanordning (till exempel plåtskiva framför snurrande hjul, axlar, kedjor, strömförande skenor) men även i form av mjuka delar med direkt skyddsfunktion. Även personlig skyddsutrustning kan ses som del av barriär.
Begränsat tolerabel (BT) *Limited tolerable*	En viss risknivå. I RFP specificeras vem som får stänga en risk på denna nivå.
Beslutsdokument för systemsäkerhet *Decision document for system safety*	Samlande begrepp som används i handboken för följande tre beslutsdokument: • Systemsäkerhetsutlåtande, SCA (Safety Compliance Assessment). • Systemsäkerhetsgodkännande, SS (Safety Statement). • Centralt systemsäkerhetsbeslut, CSSB.
Bidragande orsaker *Contributing causes*	För att en riskkällas skadliga egenskaper ska aktiveras kan en viss mekanism erfordras. (Se *Utlösande faktor*)
Central verksamhetsutövare *Central operator*	Chefen för Försvarsmaktens ledningsstab, produktionschefen och insatschefen är centrala verksamhetsutövare.
CIP-konventionen *C.I.P. convention*	CIP-konventionen säkerställer att varje civilt skjutvapen och all civil ammunition som säljs i deltagarländerna, är säker för användaren. CIP-konventionen omfattar 14 stater (Sverige är inte medlem). The Commission Internationale Permanente pour l'Epreuve des Armes à Feu Portatives .
CIP-stämpel *C.I.P. proof mark*	**Civila skjutvapen** Tillverkare och importör av skjutvapen i stat som är medlem av CIP är tvingad att begära hos ett godkänt testorgan, att utföra provning av alla skjutvapen de tillverkar respektive importerar. Efter utförd och godkänd provning åsätts provade vapendelar CIP- märkning. **Ammunition** CIP-konventionen tvingar tillverkare respektive importör av ammunition som ska säljas i ett CIP-land att kontinuerligt under tillverkning prova ammunitionen enligt CIP-specifikationer. Sådan ammunition ska förses med CIP-märkning.

Begrepp	Förklaring
Civil ammunition *Civil ammunition*	Civil handvapenammunition som förekommer i handeln (COTS) och är försedd med CIP-stämpel (ersätter CE-märkning).
Civilt handvapen *Civilian handgun*	Civilt handvapen som förekommer i handeln (COTS) och är försett med CIP-stämpel (ersätter CE-märkning).
Designansvarig (DesignA) *Responsible for design (DesignA)*	Rollhavare med Tekniskt designansvar (se tekniskt designansvar) Exempel på DesignA är statlig myndighet, utländsk myndighet, leverantör med OPS-avtal med Försvarsmakten
Deterministisk riskanalys *Deterministic risk analysis*	Deterministisk riskanalys utgår från vilka risker som fysiskt sett anses kunna inträffa. Härvid kan väljas endera värsta tänkbara skadehändelse eller dimensionerande skadehändelse (jämför probabilistisk riskanalys).
EASA	Europeiska flygsäkerhetsbyrån (EASA) har genom en EG förordning övertagit de europeiska nationella myndighetsuppgifterna att typgodkänna flygmateriel för den öppna europeiska gemensamma marknaden.
Enhet *Item*	Benämning för varje delsystem, apparat, komponent, detalj eller annat som kan betraktas separat.
Enkelfelkriteriet *Single Failure Criterion, Single Event Criterion*	Fel eller händelse som ensamt kan leda till vådahändelse.
Expertsystem *Expert system*	Se *Neurala nätverk*.
F-kod *F-code*	Förvaringskod enligt IFTEX. Utgör grund för hur Försvarsmaktens ammunition får lov att förvaras.
Fara *Danger/Hazard*	Ett tillstånd som är en förutsättning för en olycka, innefattar både riskkälla och farligt tillstånd.
Farligt tillstånd *Hazardous condition*	En fysisk situation som kan leda till en olycka.
Fel *Defect*	Avvikelse från givna krav i fråga om viss egenskap.
Fel *Failure*	Upphörande av en enhets förmåga att utföra krävd funktion.

Begrepp	Förklaring
Feleffekt, felkonsekvens *Fault effect, Fault consequence*	Det resultat som blir direkt eller indirekt följd av att fel inträffar.
Felfrekvens *Failure probability density*	Felfrekvensfunktionens värde vid en angiven tidpunkt.
Felorsak *Failure cause*	Omständighet som lett till feluppkomst.
Felsannolikhet *Probability of failure*	Sannolikhet för ett eller flera fel under angivet tidsintervall.
Felsäker *Fail safe*	Egenskap hos en enhet sådan att dess fel inte blir farliga fel. En fail-safe konstruktion är sådan att vid fel i konstruktionen så hamnar systemet i ett säkert tillstånd.
Felsätt, felmod *Fault mode*	Ett av de möjliga feltillstånden hos en enhet.
Försumbar skada *Negligible damage*	Skadeutfall som är bagatellartat och av mindre omfattning. Åtgärdas med ”plåster och några dagars vila”.
Försök *Trial/Experiment*	Med försök avses verksamhet för taktisk värdering av materiel/system/produkt, vilket avser att visa att ett tekniskt system är taktiskt lämpligt och kan hanteras på avsett sätt. (Jämför *Provning*.)
Godkända processer (RML) *Approved processes*	Varje auktorisation som utfärdas baseras på ett ändamålsenligt verksamhetsledningssystem. I verksamhetsledningssystem ingår att definiera de processer som bland annat är kritiska för kvaliteten på de produkter och tjänster som levereras. Dessa processer ska således godkännas av luftfartmyndigheter.
Granskning *Design review*	Syftar till att på ett kvalitetssäkrat och spårbart sätt granska främst teknisk dokumentation.
Gränsyta, gränssnitt *Interface*	Utformningen av en logisk eller fysisk gräns/ förbindelse mellan olika funktioner, objekt, delsystem eller system.
Hantering *Handling*	Med hantering avses tillverkning, bearbetning, behandling, förpackning, förvaring, transport, användning, omhändertagande, förstöring, saluförande, underhåll, överlåtelse och därmed jämförliga förfaranden. (Definitionen är hämtad från lag om brandfarliga och explosiva varor.)

Begrepp	Förklaring
Individuell risk *Individual risk*	Frekvensen som en individ kan förväntas att utsättas för av en given nivå av skada orsakad av specificerade faror (IchemE, Institution of Chemical Engineers). Den är vanligtvis beräknad för en genomsnittsperson i gruppen.
Inkrementell utveckling *Incremental development*	Först byggs de centrala delarna av systemet. Det säkerställs att dessa fungerar som kravställt. Sedan läggs fler funktioner till och kontrolleras på samma sätt. När alla krävda funktioner är på plats är systemet färdigt.
Konfigurationsbeslut *Configuration decision*	Produktdokument som fastställer tekniskt systems omfattning och konfiguration.
Konsekvens *Effect/Damage*	Konsekvensen av en olycka utgörs av eventuell skada på person, egendom och yttre miljö.
Krigsskadereparation *Battle damage repair*	Metod för avhjälpande underhåll syftande till att efter skada snabbt återställa tekniskt systems krigsanvändbarhet. Krigsskadereparation utförs endast under krig eller krigsliknande förhållanden. Reparationen bör vara acceptabel från systemsäkerhetssynpunkt (Jämför STANAG 2418).
Kritiska delar *Critical items*	En del, sammansättning, installation eller produktionsprocess med en eller flera egenskaper, som om denna inte överensstämmer med sina krav, resulterar i ett osäkert tillstånd.
Kritiska egenskaper *Critical characteristics*	En egenskap, (tolerans, ytfinhet, material, tillverkning, sammansättning) hos en produkt, material eller process, som om denna inte överensstämmer med sina krav, kan resultera i ett fel hos en kritisk del.
Kritiskt fel *Critical defect*	Avvikelse från givna fordringar i fråga om viss egenskap och som därmed direkt kan leda till ett osäkert tillstånd.
Kundbeställning (KB) *Customer order*	Beställning av vara eller tjänst från Försvarsmakten till DesignA. Innehåller beslut om pengar och specifikation av vad som ska levereras, tidsförhållanden med mera. Om beställningen avser tekniskt system ingår (referens till) TTEM/TEMU.
Kvalificering *Qualification*	Verifiering av en produkts egenskaper.
Livslängd *Life time, Service life*	Total tid från det att ett system skapas till och med dess avveckling.

Begrepp	Förklaring
Materielsystem *Materiel system*	Se *Tekniskt system*.
Materielkontoret (MaK) *Systems Office*	Är ÄFR för all materiel som inget TeK ansvarar för bland annat samtliga standardfordon (COTS). MaK är organisatoriskt en del av FMLOG.
Militär ammunition *Military ammunition*	Ammunition som oavsett ursprung avses för att genomföra militär verksamhet.
Militär materiel *Military equipment*	Tekniskt system som särskilt har konstruerats och tillverkats (även genom integration) för att genomföra militär verksamhet.
Militär olycksrisk *Military accident risk*	Risk för skada under strid förorsakad av brister i materielens utförande och funktion. Särskilt avgörande är den fördel fienden kan få av detta i en stridssituation.
Militärt ändamål *Military purpose*	Verksamhet syftande till att förbereda och genomföra organiserad, väpnad strid.
Mindre allvarlig personskada *Less serious injury*	Skada som person blir återställd ifrån efter sjukhusvård (till exempel benbrott).
Neurala nätverk *Neural networks*	Teknik för att skapa expertsystem. Avser algoritmer för informationsbehandling som försöker efterlikna funktionen i nervcell och hjärna.
Obligatoriskt krav *Mandatory requirement*	Krav som har avgörande betydelse för systemsäkerheten. Kommentar: Om ett obligatorisk krav inte kan uppfyllas av exempelvis taktiska skäl eller kostnadsskäl, kan en avvikelse accepteras om det kan visas att acceptabel säkerhet fortfarande kan erhållas.
Olycka/olyckshändelse *Accident, Mishap*	Inträffar då någon/något exponeras för vådahändelse eller farligt tillstånd och därvid skadas (skada på person, egendom eller yttre miljö). Olycka är alltid oplanerad, ej resultat av till exempel fientlig handling. Mishap används endast i USA.

Begrepp	Förklaring
Olycksrisk *Accident risk*	Avser risk för skada på människa, egendom och/eller yttre miljö. Uttrycks som funktion av sannolikheten för att olycka inträffar och dess konsekvens (konsekvensen vanligen fördelad på de fyra skadeklasserna för människa respektive ekonomi. Fördelas om möjligt på delrisker för de fyra skadeklasserna.
Personsäkerhet *Personal safety*	Egenskapen hos ett system att inte orsaka oacceptabel personskada.
Proaktiv *Proactive*	Förutseende och förebyggande.
Probabilistisk riskanalys *Probabilistic risk analysis*	Probabilistiska riskanalysmetoder utgår från att såväl sannolikheter för att olyckshändelser ska inträffa, som de konsekvenser dessa ger upphov till, är av betydelse för bedömning av risknivån. (Jämför *Deterministisk riskanalys*).
Produkt *Product*	Med produkt förstås här främst sådan vara som ”säljs över disk”/är kommersiellt tillgänglig (COTS) och säkerhetsmässigt är konstruerad för att uppfylla produktsäkerhets- och produktansvarslagarna samt tillämpliga EU-direktiv.
Produktsäkerhet *Product safety*	Egenskapen hos en produkt att inte kunna orsaka skada på person, egendom eller yttre miljö.
Provning *Testing*	Med provning avses teknisk verifiering och validering. Provning utgör tillsammans med granskning den kvalificeringsverksamhet som syftar till att verifiera ställda tekniska krav och förväntningar, till exempel visa att ett eldrör kan motstå det tryck avsedd ammunition skapar. Vid provning kan förekomma vida större risker än vad säkerhetsgodkänd materiel får lov att innehålla. (Jämför *Försök*.)
Reaktiv *Reactive*	Att i efterhand vidta åtgärd för att söka förhindra en upprepning av till exempel en olycka.
Restriktion *Restriction*	Tillfällig inskränkning i tekniskt systems tillåtna brukande för att temporärt hantera viss risk och därigenom innehålla ställda krav på systemsäkerhet.
Risk *Risk*	Se *Olycksrisk*.

Begrepp	Förklaring
Riskanalys *Risk analysis*	En systematisk användning av tillgänglig information för att identifiera olycksrisker för person, egendom och yttre miljö.
Riskkälla *Hazard*	Något som kan leda till skada på person, egendom eller yttre miljö.
Risklogg *Risk log*	Dokument för dokumentation av visst tekniskt systems samtliga risker. Avser ersätta tidigare dokument PHL, riskkällelista och risklista.
Riskmatris *Risk matrix*	Tvådimensionell graf som används för att åskådliggöra samband mellan sannolikhet och konsekvens. Kan graderas samt förses med gränser som visar acceptanskriterier.
Riskreducerande åtgärd *Risk reduction activity*	Eliminera riskkällor. Konstruera bort risken. Införa skyddsanordningar (benämns även barriär). Införa aktiv varningsutrustning (till exempel ljud/ljussignaler). Införa restriktioner/utbildning/ instruktioner/varningsskyltar.
Samhällsrisk *Societal risk*	Relationen mellan frekvens och antalet människor som drabbas av en specificerad nivå av skada i en given folkmängd exponerad för specificerad risk (IchemE, Institution of Chemical Engineers). Den beräknar därför hur många människor som är omfattade av en olycka.
Skada *Harm*	Skada på person, egendom eller yttre miljö. Med begreppet skada avses i H SystSäk alla möjliga utfall.
Skadeklass *Hazard severity category*	För personskada: Dödsfall, allvarlig personskada, mindre allvarlig personskada och försumbar skada. För ekonomisk skada: Jämförbart med total systemförlust, betydande förlust, begränsad förlust, liten förlust. Detaljer framgår av *H SystSäk del 1, avsnitt 4.2.3*.
Styrande verksamhet *Managing activity*	Uttrycket refererar ofta till en anskaffande instans såsom Försvarsmakten och DesignA, men kan även inkludera leverantörer eller underleverantörer som kräver en aktivitet av sin underleverantör
Stängning av risk *Risk acceptance*	För vardera av ett tekniskt systems olycksrisker, fattas acceptansbeslut. Vid acceptansbeslut jämförs olycksriskens värde, hämtat ur det tekniska systemets risklogg, med kravställt riskvärde.
System *System*	Se *Tekniskt system*.

Begrepp	Förklaring
System av system *System of systems*	Förmåga som skapas genom användning av befintliga tekniska system och produkter på nytt sätt, eventuellt tillsammans med nytillförd materiel.
Systematiska fel *Systematic errors*	Ett fel som alltid inträffar vid viss användning av system och som ger samma felutfall varje gång. Orsaken kan till exempel vara logiskt fel i programvara som ger samma felutfall vid exekvering, eller fysiskt fel hos en ”batch” komponenter som ger samma felutfall då komponenterna exponeras/används (batch = grupp av komponenter tillverkade i en följd/med samma maskininställning, av samma insatsvaror/råvaror, med mera).
Systemrisk *System hazard*	Olycksrisk på övergripande systemnivå, som oavsiktligt kan förorsakas av systemets krävda förmåga. Framgår ofta som svar på frågan: Givet systemförmågan, vad får inte denna ställa till med/vad får inte hända?
Systemsäkerhet *System safety*	Egenskapen hos ett tekniskt system att inte oavsiktligt orsaka skada på person, egendom eller yttre miljö. (Person; död, fysisk skada eller sjukdom. Egendom; skada på alternativt förlust av egendom eller utrustning. Yttre miljö; ”ytlig” skada som helt eller delvis kan saneras respektive permanent skada, till exempel utrotning av djurart).
Systemsäkerhetsanalys *Safety analysis*	Samlingsterm för de delar av systemsäkerhetsverksamheten som innebär dels systematisk kartläggning av möjliga vådahändelser och orsaker till dessa, dels kvalitativ eller kvantitativ utvärdering av riskerna hos tekniskt system.
Systemsäkerhetsbeslut *System safety decisions*	Systemsäkerhetsbeslut är en samlande benämning, som i denna handbok omfattar: • systemsäkerhetsutlåtande • systemsäkerhetsgodkännande • centralt systemsäkerhetsbeslut.

Begrepp	Förklaring
Systemsäkerhets-dokumentation *System safety documentation*	Med fullständig systemsäkerhetsdokumentation för visst tekniskt system avses: • Från leverantör Riskdokumentation inklusive risklogg med riskbeslut för varje enskild risk Systemsäkerhetsrapport med analysresultat (från utförda analysaktiviteter såsom PHL, PHA, SHA med flera) Systemsäkerhetsutlåtande • Från DesignA Systemsäkerhetsgodkännande (Allt ovanstående material från leverantör utgör underlag) • Inom Försvarsmakten Centralt systemsäkerhetsbeslut För att sammankoppla riskdokumentation och systemsäkerhetsbeslut för visst tekniskt system krävs ett beslut om gällande konfiguration av det tekniska systemet. Med systemsäkerhetsbeslut förstås i denna handbok: systemsäkerhetsutlåtande, systemsäkerhetsgodkännande och centralt systemsäkerhetsbeslut.
Säkerhetsintyg *Safety certificate*	Utfärdas av DesignA och är en form av systemsäkerhetsgodkännande. Säkerhetsintyget innebär att DesignA granskat alla relevanta omständigheter och har funnit att det fartyg som ett PTK ska prova har godtagbar säkerhet. Säkerhetsintyget överlämnas till Försvarsmaktens Sjösäkerhetsinspektion som efter godkännande överlämnar detta till PTK.
Systemsäkerhets-krav *System safety requirement*	Försvarsmaktens krav på DesignA omfattar dels verksamhetsåtaganden och tekniska krav på det tekniska systemets systemsäkerhetsegenskaper. Jämför *avsnitt 5.3*.
Säkerhetsmeddelande *Safety message*	Rapport som lämnas i det speciella fall att DesignA har uppdragits att för visst tekniskt system utfärda ett systemsäkerhetsgodkännande, men där det tekniska systemet i fråga konstateras ej ha acceptabel säkerhetsnivå.
Systemsäkerhets-verksamhet *System Safety Activities*	Det totala arbete som bedrivs för ett visst tekniskt system under studier, utveckling, anskaffning/upphandling respektive renovering och modifiering), produktion, drift (inklusive teknisk anpassning), vidmakthållande och avveckling, i syfte att identifiera och kvantifiera risker, eliminera dessa eller reducera dem enligt ställda krav.
Säkerhet *Safety*	Frånvaro av olycksrisk som kan leda till oavsiktlig skada.

Begrepp	Förklaring
Säkerhet *Security*	Frånvaro av förhållanden som innebär spionerі, sabotage, terrorism och andra brott mot rikets säkerhet.
Säkerhetsbrist *Safety defect*	En produkt har en säkerhetsbrist om den inte är så säker som skäligen kan förväntas.
Säkerhetsledning *Safety management*	En tillämpad form av kvalitetsstyrning och definieras som alla åtgärder som syftar till att påverka säkerheten på ett verksamhetsställe.
Teknisk anpassning *Technical adaptation*	Att tillfälligt förändra/anpassa tekniskt systems konstruktion och/eller funktion med anledning av störning, förändrad hotbild eller miljö. Också vid förändrade operativa, taktiska eller stridstekniska krav. Tillämpas endast under direkta stridsförhållanden (krig, kris, internationell insats). Ändringen är av tillfällig art, och materielen ska då så erfordras kunna återställas till ursprungligt skick.
Tekniskt designansvar *Technical design responsibility*	Tekniskt designansvar innebär att för tekniskt system fastställa teknisk struktur och konstruktion, samt att fastställa vilken integration av tekniska system/delsystem, apparater och komponenter som omfattas av viss tillåten konfiguration (inklusive underhållslösningar) och att säkerställa att denna uppfyller lagkrav, fastställda målsättningar och övriga krav avseende prestanda, funktion, informations- och systemsäkerhet under det tekniska systemets livslängd. Tekniskt designansvar, inklusive teknisk systemledning, innehas normalt av DesignA för alla nivåer av tekniska system som DesignA har levererat till Försvarsmakten. Tekniskt designansvar är kopplat till typ av tekniskt system. Industri och leverantör har ett produktansvar och kan ha ett tekniskt designansvar inför anskaffande organisation, men det är alltid anskaffande organisation som är tekniskt designansvarig.
Teknikkontor, (TeK) *Technical Office*	Ägarföreträdarens representant (ÄFR) för specifik materiel.
Teknisk order (TO) *Technical order*	Materielpublikation som utges av Försvarets materielverk på uppdrag av Försvarsmakten. Genom teknisk order regleras drift, underhåll, vård och modifiering av förnödenheter.

Begrepp	Förklaring
Teknisk standardorder *Technical standard order*	Teknisk standardorder utfärdas av luftfartsmyndighet och utgör en standard som specificerar minimiegenskaper för en artikel.
Tekniskt system *Technical system*	Ett system definieras enligt ISO/IEC 15288 som ”En sammansättning av samverkande element organiserade att uppnå ett eller flera uttalade syften”. Med system förstås i H SystSäk alltid just Tekniskt system. Med tekniskt system förstås även sådant system som har skapats genom integration av tekniska system, delar ur sådana och/eller andra produkter. Ammunition är alltid ett eget tekniskt system.
Tillbud *Incident*	Vådahändelse som inte leder till olycksfall eftersom ingenting exponeras vid vådahändelsen.
Tillfällig reparation *Expedient repair*	Metod för icke permanent avhjälpande underhåll av drift- och/eller stridsskada omfattande okonventionella reparationsmetoder och/eller alternativ reservmaterielförsörjning. Reparationen ska vara acceptabel från systemsäkerhetssynpunkt
Tolerabel (T) *Tolerable*	En viss angiven risknivå.
Utlösande faktor *Trigger*	För att en riskkällas skadliga egenskaper ska aktiveras kan en viss mekanism erfordras. I vissa fall kan även utlösande faktor erfordras för att åstadkomma en vådahändelse. (Jämför *Bidragande orsaker*)
Valbart krav *Optional requirment*	Urvalet av de valbara krav som ska genomföras för tekniskt system anpassas av beställaren efter systemets komplexitet. Jämför Obligatoriskt krav
Validering *Validation*	Sätt att visa att kraven är korrekta, det vill säga att systemet kommer att fungera på avsett sätt i sin operativa miljö om kraven uppfyllts.
Verifiering *Verification*	Konfirmering genom framtagning och undersökning av objektiva bevis för att specificerade krav uppfyllts.
Verksamhetssäkerhet *Operational safety*	Försvarsmaktens verksamhetssäkerhet avser Försvarsmaktens förmåga att hantera risker vid all verksamhet så att författningsenliga krav på arbetsmiljö och säkerhet för Försvarsmaktens personal samt kraven på säkerhet för tredje man, yttre miljö och egendom uppfylls.

Begrepp	Förklaring
Vådahändelse *Hazardous event*	Händelse som inträffat av våda, det vill säga utan uppsåt, oplanerat och som kan resultera i olycka eller tillbud om någon eller något exponeras.
Yttre miljö *Environment*	Omgivningar där en organisation verkar, vilket inkluderar luft, vatten, mark, naturresurser, flora, fauna och människor samt samspelet mellan dessa.
Ägarföreträdare (ÄF) *Owner representative*	Ägarföreträdaren har inför regeringen ansvar för förnödenheternas status, sekretess, befintlighet och redovisning. FMV är ägarföreträdare för materiel före leverans till Försvarsmakten. Försvarsmakten är ägarföreträdare från det att leverans av förnödenheterna till Försvarsmakten godkänts, tills det att förnödenheterna avgångsredovisas ur Försvarsmaktens förnödenhetsbestånd. Detta avser även anläggningstillgångar placerade vid industrin och FMV.
Ägareföreträdarens Representant (ÄFR) *The owner respresentative's representative*	För de flesta tekniska system finns Ägareföreträdarens representant, ÄFR, utsedda i form av Teknikkontor och Materielkontor. Dessa agerar som ägare till materielen under drift, vidmakthållande och avveckling. ÄFR ansvarar för att representera ÄF vad gäller drift- och ekonomistyrning, uppföljning och analys, konfigurationsläge, modifieringar och TO-verksamhet samt tekniskt systemstöd och teknisk utveckling. FMV är ägarföreträdares representant för förnödenheter som huvudsakligen anskaffats för och används i FMV:s provningsverksamhet. För förnödenheter som inte entydigt kan hänföras till någon av ovanstående verksamheter ska ägarföreträdandets representant regleras i respektive beställning.

Akronymer/förkortningar

Komplett förteckning över de akronymer och förkortningar som återfinns i H SystSäk.

Akronym/Förkortning	Förklaring
ADR	Accord Européen Relatif au Transport International des Marchandises Dangereuses par Route European Agreement Concerning the International Carriage of Dangerous Goods by Road
AE	Architect and Engineering Firm
ALARP	As low as reasonable practicable, så låg som praktiskt och rimligt möjligt (avser viss olycksrisk)
AML	Arbetsmiljölagen
AV	Arbetsmiljöverket
BOA	Beslut om användning
BT	Begränsat tolerabel risknivå
BVKF	Försvarsmaktens instruktion för åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor m m
CAA	Civil Aviation Authority, Storbritanien
CDRL	Contract Data Requirement List
CE	CE-märkning (EC mark of conformity), Communauté Européenne
CFR	Code of Federal Regulations
CI	Critical Item
CIL	Critical Item List
CIP	The Commission Internationale Permanente pour l'Epreuve des Armes à Feu Portatives (Permanent International Commission for Firearms Testing - commonly abbreviated as C.I.P. or CIP)
CM	Configuration Management
COSHH	Control of Substances and Hazardous to Health
COTS	Hyllvara, färdig produkt (Commercial off the Shelf)
CSP	Certified Safety Professional
CSSB	Centralt systemsäkerhetsbeslut

Akronym/Förkortning	Förklaring
DAL	Development Assurance Level
Def-Stan	Defence Standard (Storbritannien)
DesignA	Konstruktionsansvarig organisation (bland annat FömedC, FMLOG, FMV, FORTV, OPS-partner)
DGA	Délégation Générale pour l'Armement, Franska militära luftfartsmyndigheten
DID	Data Item Description, dokumentinstruktioner som anger innehåll och omfattning i rapporter
DLA	Defense Logistics Agency
DoD	Department of Defense (USA)
DoDI	DOD Instruction
DOD-STD	Department of Defense Standard
DOT	Department of Transportation (USA)
EASA	Europeiska flygsäkerhetsbyrån. EASA har genom en EG förordning övertagit de europeiska nationella myndighetsuppgifterna att typgodkänna flygmateriel för den öppna europeiska gemensamma marknaden
ECP	Engineering Change Proposal
ECPSSR	Engineering Change Proposal System Safety Report
EHA	Riskanalys för yttre miljö (Environmental Hazard Analysis)
EHC	Explosive Hazard Classification and Characteristics Data
EOD	Explosive Ordnance Disposal
ESOH	Environmental, Safety and Occupational Health
ET	Ej tolerabel risknivå
ETA	Händelseträdsanalys (Event Tree Analysis)
FAA	Federal Aviation Authority
FC	Funktionscentrum
FHA	Funktionell riskanalys (Functional Hazard Assesment)
FLYGI	Militära flyginspektionen
FM	Försvarsmakten

Akronym/Förkortning	Förklaring
FM ArbO	Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FFS 2009:2 med ändring FFS 2009:3)
FMEA	Feleffektanalys (Fault Modes and Effects Analysis)
FMECA	Feleffekt- och kritikalitetsanalys (Fault Modes Effects and Criticality Analysis)
FMUK	Försvarsmaktens undersökningskommission
FMV	Försvarets materielverk
FOI	Totalförsvarets forskningsinstitut
FORTV	Fortifikationsverket
FRA	Försvarets radioanstalt
FRACAS	Felrapporteringssystem (Failure Reporting, Analysis and Corrective Action)
FSD	Försvarsstandard
FSI	Försvarsmaktens Flygsäkerhetsinspektör
FTA	Felträdsanalys (Fault Tree Analysis)
FömedC	Försvarsmedicincentrum
G	Generellt tillämpbart
GC	Generellt tillämpbart vid konstruktionsändring
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GOTS	Hyllvara, färdig produkt utvecklad åt staten (Governmental off the Shelf)
H FordonSäk	Handbok Fordonssäkerhet
H Mål	Handbok för Försvarsmaktens framtagning av målsättningar för förband, förnödenheter och anläggningar för krigsorganisationens behov
H VAS	Handbok Vapen och Ammunitionssäkerhet
HAZOP	Hazard and Operability Study
HHA	Hälsoriskanalys (Health Hazard Assessment)
HHAR	Health Hazard Assessment Report
HKV	Högkvarteret
HMI	Användargränssnitt (Human Machine Interface)
HRI	Hazard Risk Index

Akronym/Förkortning	Förklaring
HTM	Halvtidsmodifiering
HTRR	Hazard Tracking and Risk Resolution
IEC	International Electrotechnical Commission
IFTEX	Försvarsmaktens instruktion för förvaring och transport av ammunition och övriga explosiva varor
ILS	Integrated Logistic Support
IMSC	Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms
IRS	Interface Requirements Specifications
ISO	Internationella standardiseringsorganisationen
ISSPP	Integrated System Safety Program Plan
JSP	Joint Service Publication
LKA	Lågkänslig ammunition
MA	Managing activity
MaK	Materielkontoret
MB	Miljöbalken
MCS	Minimal Cut Set
MFI	Militära fartygsinspektionen
MIFOR	Militära fordonsregistret
MIL-STD	Amerikansk militär standard (Military Standard)
MOTS	Militär hyllvara, färdig produkt utvecklad åt försvaret (Military off the Shelf)
MPD	Materielproduktdeklaration
MRAR	Mishap Risk Assessment Report
MS	Materielsystem
MSA	Materielsystemansvarig i Försvarsmaktens HKV
MSB	Myndigheten för samhällsskydd och beredskap
MSI	Materielsystemintyg
MTC	Materieltypcertifikat
N/A	Ej tillämpligt (Not Applicable)
NDI	Non-developmental Item
O&SHA	Säkerhetsanalys för användning och underhåll (Operating and Support Hazard Analysis)

Akronym/Förkortning	Förklaring
OHHA	Operating and Health Hazard Analysis
OPR	Office of Primary Responsibility
OPS	Offentlig privat samverkan /PPP Private-Public Partnership
OSHA	Occupational Safety and Health Administration
PAL	Produktansvarslagen
PE	Professional Engineer
PESHE	Programmatic environment, safety, and occupational health evaluation
PHA	Inledande undersökning av riskkällor och farliga tillstånd (Preliminary Hazard Analysis)
PHL	Inledande identifiering av riskkällor och farliga tillstånd (Preliminary Hazard List)
PHST	Förslag till hanterings- och förvaringsbestämmelser (Package Storage and Handling Requirements)
PL	Produktledare
PM	Program Manager
PRL	Projektledare
PTEMU	Preliminär Teknisk-Ekonomisk Målsättning för Utbildningsmateriel
PTK	Provturskommando
PTR	Program Trouble Reports
PTTEM	Preliminär Taktisk-Teknisk-Ekonomisk Målsättning
RADS	Riskanalys inför avveckling av system (Risk Assessment at Disposal of System)
REMO	Renovering – modifiering
RENO	Renovering
RFP	Kravställning vid anbudsförfrågan (Request for Proposal)
RML	Regler för militär luftfart
RML V-5J	Regler för militär luftfart, Underavdelning J - auktoriserade designorganisationer - nivå 2
RML V-5JA	Regler för militär luftfart, Underavdelning J - auktoriserade designorganisationer - nivå 3

Akronym/Förkortning	Förklaring
RML V-5B	Regler för militär luftfart, Underavdelning B - Materielsystemintyg och militärt typcertifikat
RML V-5G	Regler för militär luftfart, Underavdelning G - Auktoriserade produktionsorganisationer
RMS	Regler för militär sjöfart
S	Selektivt tillämpbart
SAR	Säkerhetsrapport (Safety Assessment Report)
SCA	Systemsäkerhetsutlåtande (Safety Compliance Assessment)
SCCSC	Safety Critical Computer Software Components
SCF	Safety Critical Functions
SCG	Storage Compatibility Group
SCN	Specification Change Notices
SDB	Säkerhetsdatablad
SDR	System Design Review
SHA	Säkerhetsanalys för system (System Hazard Analysis)
SHRI	Software Hazard Risk Index
SI	Säkerhetsföreskrifter (Safety Instructions)
SIL	Safety Integrity Level
SJÖI	Militära sjösäkerhetsinspektionen
SOW	Verksamhetsåtaganden (Statement of Work)
SPR	Software Problem Reports
SR	Systemsäkerhetsgenomgång, Safety Review.
SRCA	Säkerhetskravsanalys (Safety Requirements/Criteria Analysis)
SRR	System Requirements Review
SS	Systemsäkerhetsgodkännande (Safety Statement)
SS	Svensk standard
SSE	Systemsäkerhetsvärdering (System Safety Evaluation)
SSHA	Säkerhetsanalys för delsystem (Sub System Hazard Analysis)
SSI	Safety Significant Item
SSMP	System Safety Management Plan

Akronym/Förkortning	Förklaring
SSP	Systemsäkerhetsprogram (System Safety Program)
SSPP	Systemsäkerhetsplan (System Safety Program Plan)
SSPPR	System Safety Program Progress Report
SSPR	Systemsäkerhetsgranskning (System Safety Program Review/Audits)
SSPS	Rapport över systemsäkerhetsarbetet (System Safety Progress Summary)
SSR	Software Specification Review
SSS	System/Segment Specification
SSWG	Arbetsgrupp för systemsäkerhet (System Safety Working Group) Ibland kallade SSWG-1 respektive SSWG-2
SV	Säkerhetsverifiering (Safety Verification)
SäkI	Försvarsmaktens säkerhetsinstruktion för vapen och ammunition med mera
SäkI G	Försvarsmaktens säkerhetsinstruktion för vapen och ammunition med mera – Gemensam del
SÄKINSP	Försvarsmaktens säkerhetsinspektion
T	Tolerabel risknivå
TA	Teknisk anvisning
TC	Truppslagscentrum
TeK	Teknikkontor
TEMU	Teknisk-Ekonomisk-Målsättning för Utbildningsmateriel
TjF	Tjänsteföreskrift för FMV
TO	Teknisk order
TOEM	Taktisk, organisatorisk, ekonomisk målsättning
Tso	Teknisk standard order
TSR	Användarmanualer och utbildning (Test and Safety Regulations)
TTEM	Taktisk-Teknisk-Ekonomisk Målsättning
UAV	Unmanned Aerial Vehicle
UhF	Handbok underhållstjänst i fred
UK	United Kingdom

Akronym/Förkortning	Förklaring
US	United States
UTEMU	Utkast till Teknisk-Ekonomisk Målsättning för Utbildningsmateriel
UTTEM	Utkast till Taktisk-Teknisk-Ekonomisk Målsättning
V&V	Verifiering och Validering
VD	Verkställande direktör
WBS	Work Breakdown Structure
WEEE	Waste Electrical and Electronic Equipment
VFM	Verksamhetsordning för Försvarsmakten
WSESRB	Weapon System Explosive Safety Review Board
ÄF	Ägarföreträdare
ÄFR	Ägarföreträdarens representant
ÖB	Överbefälhavaren

Referenser

Följande dokument utgör källdokument till handbokens båda delar. Angivna dokumentbeteckningar med mera är de som var aktuella vid handbokens färdigställande. I det fall att viss referens behöver tillämpas rekommenderas att förekomsten av senare utgåva kontrolleras.

Ref nr	Titel
1	ADR, Myndigheten för samhällsskydd och beredskaps föreskrifter om transport av farligt gods på väg och i terräng; MSBFS 2009:2. Bokstaven ”S” efter ADR betecknar att föreskrifterna innehåller den svenska versionen av bilagorna A och B till den europeiska överenskommelsen om internationell transport av farligt gods på väg (ADR), kompletterade med bestämmelser som endast gäller för nationella transporter i Sverige.
2	Arbetsmiljölag, SFS 1977:1160.
3	Avfall som utgörs av eller innehåller elektriska eller elektroniska produkter, 2002/96/EG, WEEE.
4	Certification Considerations for Highly-Integrated or Complex Aircraft Systems, SAE ARP4754.
5	Defence Standard 00-56 issue 2, part 2, 13:th Dec 1996.
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	Europaparlamentets och rådets förordning, EG nr 1907/2006 (REACH).
14	FMV Handbok HMI, 14 910:753/2009.

Ref nr	Titel
15	FMV Återvinningsmanual, 32822/2008 version 2.0.
16	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508.
17	Förordning (2007:936) om folkrättslig granskning av vapenprojekt.
18	Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk, 2001. 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.
20	Försvarsmaktens instruktion för åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor mm, BVKF.
21	Handbok Fordonssäkerhet 2000 års utgåva, M7762-000511, H FordonsSäk.
22	Handbok för Försvarsmaktens förnödenhetsavveckling, M7751-704081, H Förnavv.
23	Handbok för Försvarsmaktens målsättningsarbete (H Mål), 2006.
24	Handbok för Vapen- och Ammunitionssäkerhet, M7762-000212, H VAS.
25	Handbok Miljö för Försvarsmakten, M7740-784501, H Miljö.
27	ITAA Standard, Standard Best Practices for System Safety Program Development and Execution, GEIA-STD-0010, October 2008.
28	Kemikalieinspektionen Prioriteringsguiden (PRIO), *www.kemi.se*.
29	Ledningssystem för kvalitet - Krav, SS-EN ISO 9001:2008.
30	Military Airworthiness Regulations, JSP523.
31	Miljöbalken, SFS 1998:808.
32	Miljöledningssystem - Krav och vägledning, SS-EN ISO 14001:2004.
33	MOD Sustainable Development and Environmental Manual, JSP418.
34	Ordnance, Munitions and Explosives Safety Manual, JSP520.
35	Procedures for Land Systems Equipment Safety Assurance, JSP454.
36	Produktansvarslagen, SFS 1992:18.

Ref nr	Titel
37	Safety Assessment Procedure Guidelines and Methods, SAE ARP 4761.
38	SEES Handbok Miljötålighetsteknik.
39	Ship Safety Management, JSP430.
40	Software Consideration in Airborne Systems and Equipment Certification, RTCA DO-178B, 1992.
41	Svensk Standard, SS 2222.
42	Säkerhetsinstruktion för vapen och ammunition med mera, Gemensam del, SäkI G.
43	UK Def-Stan 00-56 issue 3.
44	US WSESRB Hazard Analysis Guide list.

Bildförteckning

Bild 1:1 Systemsäkerhetsaktiviteter 11
Bild 3:1 Systemsäkerhetsaktiviteternas samband 24
Bild 5:1 System Safety Program (SSP) för Försvarsmakten 45
Bild 5:2 System Safety Program (SSP) för DesignA 45
Bild 5:3 Systemsäkerhetsvärdering (SSE) 48
Bild 5:4 Systemsäkerhetskrav i TTEM 50
Bild 5:5 Kravställning vid anbudsförfrågan (RFP) 56
Bild 5:6 System Safety Program Plan (SSPP) 59
Bild 5:7 Integration/Management of Subcontractors (IMSC 61
Bild 5:8 System Safety Program Reviews/Audits (SSPR) 63
Bild 5:9 System Safety Working Group (SSWG) 65
Bild 5:10 Hazard Tracking and Risk Resolution (HTRR) 67
Bild 5:11 System Safety Progress Summary (SSPS) 69
Bild 5:12 Safety Critical Functions (SCF) 75
Bild 5:13 Preliminary Hazard List (PHL) 77
Bild 5:14 Preliminary Hazard Analysis (PHA) 79
Bild 5:15 Safety Requirements/Criteria Analysis (SRCA) 81
Bild 5:16 Subsystem Hazard Analysis (SSHA) 83
Bild 5:17 System Hazard Analysis (SHA) 86
Bild 5:18 Operating and Support Hazard Analysis (O&SHA) 89
Bild 5:19 Health Hazard Assessment (HHA) 92
Bild 5:20 Miljörelaterade aktiviteter 96
Bild 5:21 Riskanalys för yttre miljö (EHA) 97
Bild 5:22 Functional Hazard Assessment (FHA) 101
Bild 5:23 Safety Assessment Report (SAR) 105
Bild 5:24 Safety Review (SR) 108
Bild 5:25 Safety Verification (SV) 110
Bild 5:26 Säkerhetsföreskrifter (SI) 113
Bild 5:27 Systemsäkerhetsutlåtande (SCA) 117
Bild 5:28 Felrapporteringssystem (FRACAS) 121
Bild 5:29 Systemsäkerhetsgodkännande (SS) 128
Bild 5:30 Användarmanualer och utbildning (TSR) 132
Bild 5:31 Centralt systemsäkerhetsbeslut (CSSB) 134
Bild 5:32 Riskanalys inför avveckling av system (RADS) 138
Bild 8:1 Säkerhetsanalys 149
Bild 8:2 Koppling av aktivitet till metod 150
Bild 8:3 Felträdssymboler 151
Bild 8:4 Antalet &-villkor 153
Bild 8:5 Felträd med olika antal &-villkor 153
Bild 8:6 Beräkningar av felträdssannolikheter 154
Bild 8:7 Påkännings-tålighets-metoden 154
Bild 8:8 Exempel på lösning med boolesk algebra 155
Bild 8:9 Exempel på felträdsanalys 156
Bild 8:10 Exempel på feleffektanalys 159
Bild 8:11 Exempel på underlag till feleffektanalys 160
Bild 8:12 Exempel på händelseträdsanalys 161

Tabellförteckning

Tabell 2:1 Kravlista 15
Tabell 2:2 Kravlista 17
Tabell 2:3 Kravlista 18
Tabell 2:4 Kravlista 18
Tabell 3:1 Kravlista 19
Tabell 3:2 Tillämpningar 27
Tabell 4:1 Aktiviteter 41
Tabell 5:1 Värderingsmatris 47
Tabell 8:1 Ledordstabell 163
Tabell 8:2 Exempel på HAZOP 164

Projektledare
Ragnar Ekholm, FMV

Ämnesexperter
Arne Börtemark, FMV (Del 1 och 2)
Ragnar Ekholm, FMV (Del 1 och 2)
Pär-Anders Wallentin, Saab Bofors Dynamics AB (Del 2)
Lars Lange, FMV (Del 2)

Illustrationer och omslag
Leif Sundberg, Sörman Information AB
Mats Lundgren, Sörman Information AB

Original
Mats Lundgren, Sörman Information AB

Digital utgåva
Mats Lundgren, Sörman Information AB

Foton till omslag
Katsuhiko Tokunaga, SAAB
Peter Nilsson, Kockums
Sörman Information AB

1 Kravställning
1.1 Grunder ... 11
1.2 Kravnumrering ... 12
1.3 Innebörd av kravnivå ... 13
2 Materielkrav
2.1 Konstruktion ... 15
2.2 Tillverkning ... 17
2.3 Underhåll ... 18
2.4 Avveckling ... 18
3 Systemsäkerhetsaktiviteter
3.1 Krav på aktiviteter för systemsäkerhetsverksamheten ... 19
3.2 Val av aktiviteter (Tailoring) ... 21
4 H SystSäk och MIL-STD-882C
4.1 Allmän tolkning och vägledning till MIL-STD-882C ... 37
4.2 Generell beskrivning av aktiviteter i H SystSäk ... 39
4.3 Översikt över samtliga systemsäkerhetsaktiviteter ... 41
5 Beskrivning av aktiviteter
5.1 System Safety Program (SSP) – Task 101 ... 43
5.2 Systemsäkerhetsvärdering (SSE) – S10 ... 46
5.3 Systemsäkerhetskrav i TTEM (TTEM) – S11 ... 49
5.4 Kravställning vid anbudsförfrågan (RFP) – S12 ... 51
5.5 System Safety Program Plan (SSPP) – Task 102 ... 58
5.6 Integration/Management of Subcontractors (IMSC) – Task 103 ... 60
5.7 System Safety Program Reviews/Audits (SSPR) – Task 104 ... 62
5.8 System Safety Working Group (SSWG) – Task 105 ... 64
5.9 Hazard Tracking and Risk Resolution (HTRR) – Task 106 ... 66
5.10 System Safety Progress Summary (SSPS) – Task 107 ... 68
5.11 Safety Critical Functions (SCF) – S13 ... 70
5.12 Preliminary Hazard List (PHL) – Task 201 ... 76
5.13 Preliminary Hazard Analysis (PHA) – Task 202 ... 78
5.14 Safety Requirements/Criteria Analysis (SRCA) – Task 203 ... 80
5.15 Subsystem Hazard Analysis (SSHA) – Task 204 ... 82
5.16 System Hazard Analysis (SHA) – Task 205 ... 84
5.17 Operating and Support Hazard Analysis (O&SHA) – Task 206 ... 87
5.18 Health Hazard Assessment (HHA) – Task 207 ... 90
5.19 Riskanalys för yttre miljö (EHA) – S21 ... 93
5.20 Functional Hazard Assessment (FHA) – S22 ... 98
5.21 Safety Assessment Report (SAR) – Task 301 ... 104
5.22 Test and Evaluation Safety – Task 302 ... 106
5.23 Safety Review (SR) – Task 303 ... 106
5.24 Safety Verification (SV) – Task 401 ... 109
5.25 Säkerhetsföreskrifter (SI) – S41 ... 111
5.26 Safety Compliance Assessment – Task 402 ... 114
5.27 Systemsäkerhetsutlåtande (SCA) – S42 ... 114
5.28 Felrapporteringssystem (FRACAS) – S43 ... 118
5.29 Explosive Hazard Classification and Characteristics – Task 403 ... 122
5.30 Explosive Ordnance Disposal Source Data – Task 404 ... 122
5.31 Systemsäkerhetsgodkännande (SS) – S51 ... 122
5.32 Användarmanualer och utbildning (TSR) – S52 ... 129
5.33 Centralt systemsäkerhetsbeslut (CSSB) – S53 ... 133
5.34 Riskanalys inför avveckling av system (RADS) – S61 ... 135

6 Programvarusäkerhet
6.1 Allmänt ... 139
6.2 Programvaruegenskaper ... 139
6.3 Säkerhetskrav på programvara ... 142
6.4 Verifiering av programvara ... 144
7 Checklista för materielkrav och aktiviteter
8 Systemsäkerhetsanalyser
8.1 Principer för systemsäkerhetsanalyser ... 149
8.2 Felträdsanalys (FTA) ... 151
8.3 Feleffektanalys (FMEA) ... 156
8.4 Händelseträd (ETA) ... 160
8.5 Hazard and Operability (HAZOP) Study ... 162
Bilaga 1 Exempel på beslutsdokument ... 165
Definitioner ... 183
Akronymer/förkortningar ... 197
Referenser ... 205