Försvarsmaktens handbok
Systemsäkerhet 2011
Del 1 – Gemensam

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 tilllämpning 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
M7739-352022 H SYSTSÄK 2011 DEL 1

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

Innehåll

FÖRORD

INSTRUKTION OM FÖRSVARSMAKTENS HANDBOK SYSTEMSÄKERHET

Instruktion om Försvarsmaktens handbok systemsäkerhet 2011 *[26]* anger bland annat att:

- Försvarsmaktens arbetsordning anger att verksamhetssäkerhet ska motverka risker för olyckor och skador på personer, materiel eller miljö. Chefen för säkerhetsinspektionen beslutar om direktiv och instruktioner till verksamhetsutövare rörande verksamhetssäkerhet.
- Systemsäkerhet är en del i verksamhetssäkerheten.
- Försvarsmaktens systemsäkerhetsverksamhet syftar till att inte tillföra samhället ökade risker. Den syftar också till att systematiskt reducera riskerna vid användning till en för Försvarsmakten tolerabel nivå.

Instruktionen innehåller:

- **Handlingsregel:** Vägledande beskrivning och riktlinjer för tillämpning av denna instruktion framgår av H SystSäk.
- **Beslut:** Vid all anskaffning, modifiering, renovering och avveckling av materiel från och med 1 januari 2011 ska beslut fattas om och i vilken omfattning systemsäkerhetsverksamhet ska genomföras i enlighet med H SystSäk.

OMFATTNING

H SystSäk 2011 del 1 – Gemensam definierar grunderna för Försvarsmaktens systemsäkerhetsverksamhet genom att ange principer för grundläggande riskhantering och kravställning, ange förekommande roller, deras ansvar och uppgifter i ett livslängdsperspektiv, samt deras samverkan. Vissa organisationer/roller nämns särskilt; Ägarföreträdare (ÄF), rollhavare med konstruktionsansvar (DesignA) samt leverantör.

H SystSäk 2011 del 2 – Metoder redovisar de aktiviteter (systemsäkerhetsverktyg) som ingår i Försvarsmaktens systemsäkerhetsmetodik. I flera fall görs hänvisning till MIL-STD-882C *[46]* där aktiviteternas grundtext återfinns. Vidare anges generella systemsäkerhetskrav för utveckling, tillverkning och underhåll.

H SystSäk del 1 och 2 finns både på svenska och engelska samt är tillgängliga vid Försvarets bok- och blankettförråd (FBF).

H SystSäk CDR innehåller: H SystSäk del 1 och 2, MIL-STD-882C samt vissa stöddokument såsom risklogg, exempel och dokumentmallar. Cd-skivan ingår som bilaga i H SystSäk del 1. H SystSäk CDR kommer att uppdateras vid behov.

Läsanvisning

a. Olika rollers bedömda behov av att använda de olika delarna framgår nedan (här avses personal med systemsäkerhetsuppgifter inom angivna roller).

Roll Ex på organisation	Brukare Förband	ÄF HKV	Design A FMV, FORTV och FömedC	Leverantör Industri
Del 1 Gemensam	×	×	×	×
Del 2 Metoder		(×) Enstaka	×	×
MIL-STD-882C			×	×

b. Den som för första gången läser i H SystSäk bör för bästa utbyte av läsningen först läsa hela kapitel 1. Observera särskilt att H SystSäk inte är ett kravdokument som strikt ska följas, utan en handbok med såväl förklaringar som råd.

c. ÄF vid HKV som behöver en direkt metodanvisning vid framtagning av krav om systemsäkerhet i bland annat TTEM läser avsnitt enligt nedan, inklusive direkta hänvisningar i aktuell text. Angivna avsnitt är särskilt samskrivna som stöd vid kravställning.

Avsnitt	Innehåll
2.4 Lagar	Kopplingen mellan angiven lag/föreskrift och H SystSäk
Kapitel 5, hela	Grundläggande beskrivning av Försvarsmaktens systemsäkerhetsverksamhet. Besluts- och produktdokument för tekniskt system. Särskilda aspekter för vissa typer av tekniska system
6.5 Anskaffning	Krav som kan övervägas ställas vid anskaffning av tekniskt system av olika typer

d. Brukarrepresentanter som behöver en direkt metodanvisning för systemsäkerhetsverksamhet under användning läser *kapitel 8* och kompletterar vid behov med delar ur övriga kapitel.
e. Den som behöver en detaljerad redovisning av systemsäkerhetsaktiviteternas innehåll och generella systemsäkerhetskrav läser H SystSäk del 2 – Metoder.
f. Den som behöver en generell redovisning av systemsäkerhetsmetodikens grunder och dess tillämpning i Försvarsmakten läser allt.

Nyheter

Ny struktur – H SystSäk 2011 omfattar, till skillnad från 1996 års utgåva, två delar samt refererar till anvisad standard för beskrivning av flera av aktiviteterna i H SystSäk del 2. För ett antal aktiviteter saknas dock beskrivning i anvisad standard. För dessa lämnas istället fullständiga beskrivningar i del 2.

Nya synsätt har etablerats bland annat genom att begreppet riskmedvetande införts. Begreppet innebär ett effektivt arbetssätt som fokuserar på användarens attityd till olycksrisker samt dennes medverkan i det ständigt pågående arbetet syftande till att det tekniska systemet fortlöpande ska innehålla ställda krav på risknivå.

Behovet av att tidigt i kravformuleringsprocessen också ställa särskilda systemsäkerhetskrav beskrivs och exempel ges på möjliga krav.

Tillfört till handboken är bland annat en utökad beskrivning av systemsäkerhetsdokumentationen.

Riskhanteringsmetodiken enligt H SystSäk 1996 har vidareutvecklats genom att varje enskild olycksrisks olika utfallsmöjligheter särskilt identifieras. Tidigare metodik beaktade endast den enskilda olycksriskens mest signifikanta del.

Beskrivning och specificerade anvisningar har tillförts för den ledning av systemsäkerhetsverksamheten som Försvarsmakten respektive DesignA utövar.

Exempel på krav som Försvarsmakten kan rikta till DesignA i TTEM respektive kundbeställning har formulerats. Dessa krav är numrerade.

En särskild CD-skiva har tagits fram. Den ingår som bilaga i del 1 av handboken.

Textutformning

Indragen blå text är citat av föreskrifter.

Hänvisningar är länkade i de elektroniska utgåvorna och markeras med kursiv stil.

Det finns tre olika former av uppräkningar i H SystSäk, numrerad, punktad och alternativlista enligt nedan.

1. Åtgärderna i den numrerade listan ska vidtas i den ordning som anges.

- Åtgärderna i den punktade listan kan genomföras i godtycklig ordning.

a. Alternativlista anger en antal tillämpliga alternativ.

Text i gula rutor är av särskild vikt.

Numrerade krav redovisas i blå rutor. Obligatoriska krav skrivs i mörkblå ruta och har fet stil för numret. Valbara krav skrivs i ljusblå ruta och har nummer i normal stil.

Tack

Vid framtagning av denna del av H SystSäk har vissa idéer, strukturer, bilder och textavsnitt hämtats från An Introduction to System Safety Management and Assurance *[3]*, framtagen av UK Ministry of Defence. Genom särskilt skriftligt beslut har MOD välvilligt ställt skriften till den svenska Försvarsmaktens förfogande.

För detta riktas ett tack till Storbritanniens Ministry of Defence.

Förbättringsförslag

Förslag om förbättringar av H SystSäk skickas till: Försvarsmaktens Högkvarter, Säkerhetsinspektionen, 107 85 Stockholm.

1 Handbokens inriktning

1.1 Bakgrund

I samband med den övergripande riskutredning som Högkvarteret (HKV) på regeringens uppdrag genomförde 1994/95, tog Överbefälhavaren (ÖB) ställning till Försvarsmaktens (FM) behov av systemsäkerhetsverksamhet.

Handbok Systemsäkerhet (H SystSäk 2011) är en vidareutveckling av tidigare utgåva (H SystSäk 1996) och innehåller Försvarsmaktens riktlinjer för genomförande av systemsäkerhetsverksamhet avseende Försvarsmaktens tekniska system.

Försvarsmakten ska enligt sin arbetsordning (ArbO) bedriva verksamhet som syftar till att minska risker hos tekniska system så att de inte orsakar skada på person, egendom eller yttre miljö.

Vapen och vapensystem är viktiga förutsättning för Försvarsmaktens verksamhet. Ny materiel anskaffas för att ge bättre effekt. Samtidigt blir materielen ofta då mer komplex varvid nya olycksrisker kan uppstå.

Låga olycksrisker uppnås genom konstruktion och andra aktiva åtgärder. Konstruktionsåtgärder utförs främst tidigt under utveckling av tekniskt system. Under vidmakthållandefasen säkerställs uppföljning och hantering såväl av kvarvarande som av nytillkomna risker.

1.2 Syfte

Svenska lagar och författningar reglerar vilka säkerhetsegenskaper olika typer av förnödenheter, arbetslokaler, utrustningar med mera ska ha för att få marknadsföras respektive användas. Ett antal av dessa lagar/föreskrifter lämnar undantag för militär materiel respektive militär användning. Vilka dessa författningar är förändras fortlöpande.

Oaktat dessa undantag gäller Arbetsmiljölagen (AML) *[5]* som bland annat beskriver arbetsgivaransvar med att ”Arbetsgivaren ska vidtaga alla de åtgärder som behövs för att förebygga att arbetstagaren utsätts för ohälsa eller olycksfall”.

Instruktion om Försvarsmaktens handbok Systemsäkerhet 2011 *[26]* anger att handboken är Försvarsmaktens vägledande beskrivning och riktlinjer för genomförande av systemsäkerhetsverksamhet vid anskaffning, modifiering, renovering och avveckling av tekniska system.

H SystSäk har skapats av Försvarsmakten för att täcka den lucka som uppkommer genom ovanstående beskrivna undantag. H SystSäk utgör därmed Försvarsmaktens metodik för att möjliggöra framtagning av säker materiel/säkra tekniska system för Försvarsmakten och som ska vara säker vid alla de verksamheter där Försvarsmakten kan komma att hantera materielen/det tekniska systemet, såsom vid användning, utbildning, förvaring, transport, underhåll samt avveckling.

H SystSäk:

- beskriver ansvar och rollspel för hantering av risker under anskaffning och användning av militär materiel/tekniska system
- beskriver Försvarsmaktens systemsäkerhetsmetodik som ska användas för att säkerställa att risker i Försvarsmaktens materiel/tekniska system *är och förblir så låga att de uppfyller ställda krav på tolerabel risknivå* under livslängden
- utgör grunddokument vid framtagning av säkerhetsrelaterade designregler för specifikt teknikområde hos DesignA (*avsnitt 3.8*).

1.3 Tillämpning

Försvarsmakten reglerar omfattningen av den systemsäkerhetsverksamhet som ska bedrivas vid FMV, FORTV, FOI och FRA. Detta sker generellt i samordningsavtal med respektive myndighet.

Verksamheten vid FömedC och FMLOG regleras av Försvarsmaktens HKV.

Försvarsmakten reglerar genom offertförfrågan och beställning systemsäkerhetsverksamheten vid OPS-partner respektive DesignA.

Instruktion om Försvarsmaktens Handbok Systemsäkerhet 2011 *[26]* anger att vid all anskaffning, modifiering, renovering och avveckling av materiel från 1 januari 2011 ska beslut tas om och i vilken omfattning systemsäkerhetsverksamhet ska genomföras i enlighet med H SystSäk.

H SystSäk är framtagen för att kunna användas vid alla de tillfällen/faser när tekniskt systems systemsäkerhetsegenskaper avses påverkas, vilket främst sker vid studier, kravställning, utveckling, tillverkning, anskaffning, provning, granskning, vidmakthållande och vid avveckling. Handboken beskriver och ger specificerade anvisningar för Försvarsmaktens och DesignA:s ledning av systemsäkerhetsverksamhet.

Handboken kan tillämpas på tekniskt system eller tekniskt delsystem på valfri nivå, det vill säga även på enstaka teknisk produkt.

Försvarsmaktens systemsäkerhetskrav för visst tekniskt system anges i TTEM respektive kundbeställning (KB) till DesignA. Detta beskrivs närmare i *avsnitt 6.5*.

DesignA:s krav på systemsäkerhetsverksamhet i RFP grundas på krav i TTEM samt *kapitel 7*. Vid val och anpassning (Tailoring) av de aktiviteter ur del 2 som avses åläggas leverantör, tilllämpas *H SystSäk del 2, kapitel 3*.

Anläggningar ingår inte i definitionen av tekniskt system utan utgör den miljö där det tekniska systemet installeras och brukas. Anläggning kan förutom skydd även tillhandahålla vissa anläggningstekniska basresurser som el, kraft, värme, kyla, ventilation, vatten och avlopp. Framtagning av denna typ av resurser hanteras genom beställning från Försvarsmakten till FORTV.

1.4 Krav

1.4.1 Innebörd

Försvarsmakten är som beställare även kravställare. Handbokens krav fördelar sig på obligatoriska respektive valbara krav. Begreppen obligatorisk/valbar utgör anvisning för beställaren vid kravställning i KB/TTEM. Motsvarande gäller då DesignA ställer krav i anbudsförfrågan (RFP).

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. Det kan dock finnas sådana förutsättningar som medför att visst obligatoriskt krav inte är tillämpbart i viss beställning.

Urvalet av krav som ska ställas för tekniskt system anpassas av beställaren efter systemets komplexitet.

1.4.2 Numrering

H SystSäk krav är numrerade enligt följande princip.

Begynnelsesiffra för visst krav anger varifrån kravet härstammar, till exempel 2 anger att kravet kommer från H SystSäk del 1.

De följande siffrorna anger avsnitt, till exempel 632 som anger att kravet kommer från kapitel 6 avsnitt 3.2. Slutligen har varje krav ett löpnummer som gäller inom respektive avsnitt. Till exempel anger 2.632.01 det första kravet i kapitel 6 avsnitt 3.2 i H SystSäk del 1.

Följande begynnelsesiffror är fördelade till befintliga handböcker/designregler (för upplysning om hierarki och relation mellan dessa dokument se *avsnitt 2.4*)

0	H SystSäk 2011 del 2
1	H VAS (FMV Handbok för Vapen- och Ammunitionssäkerhet) *[11]*
2	H SystSäk 2011 del 1
3	H FordonSäk (FMV Handbok Fordonssäkerhet) *[10]*
6	H ProgSäk (FM handbok för programvara i säkerhetskritiska tillämpningar) *[20]*

1.5 Anpassning

H SystSäk del 1 syftar primärt till att informera om fakta, ge bakgrund och fördjupningar (främst om olycksrisk) samt att direkt ge stöd till vissa utpekade roller. Stödet utgörs av beskrivning av den systemsäkerhetsverksamhet som är lämplig att genomföra samt redovisning av ett antal formulerade krav, varav några anses vara obligatoriska (utmärkta med kravnummer i fet stil och på mörkblå botten). Övriga krav är valbara.

H SystSäk del 2 innehåller detaljerad beskrivning av alla de aktiviteter som utgör systemsäkerhetsverksamhetens ”verktyg”. Också del 2 innehåller ett antal krav, uppdelade i obligatoriska respektive valbara och numrerade på samma sätt som ovan.

H SystSäk ska inte uppfattas som ett kravdokument som ska tilllämpas bokstavligen, utan som en handbok som beskriver metoderna. Vilka aktiviteter, dokument med mera upptagna i handboken som ska användas i den enskilda anskaffningen måste alltid anpassas efter aktuellt tekniskt systems art, komplexitet och bedömda riskinnehåll.

Om det vid tillämpning av systemsäkerhetsmetodiken enligt denna handbok uppstår konflikt med regelverk som till exempel reglerar mark-, sjö- och flygsäkerhet, så äger de reglerna företräde och *förhållandet ska omgående anmälas med skrivelse till Försvarsmaktens HKV SÄKINSP*.

2 Grunder

2.1 Säkerhet

Försvarsmakten arbetar med risker på både kort och lång sikt. För att skapa förståelse för grunder och sammanhang ges nedan en kort översikt av förhållandet säkerhet och risk. Texten i *avsnitt 2.1–2.3* är till delar hämtad från An Introduction to System Safety Management and Assurance *[3]*.

Människans självbevarelsedrift leder naturligt till en ständig strävan att försöka undvika skada och förlust oavsett orsak – översvämning, flygplanskrasch, exponering för miljögifter, olycka i arbetet, ekonomisk förlust i affärsverksamhet, stöld, brand, försening med mera. Likväl är fullständig säkerhet sällsynt eftersom nästan all verksamhet har risker. Att tolerera vissa risker är dock en förutsättning för att kunna få ekonomiska eller andra fördelar, spänning eller annat. Avvägning mellan upplevd fördel och tolererad risk är den form av riskkontroll som är en del av det mänskliga livet och just kan benämnas självbevarelsedrift.

Termen risk används i många sammanhang, och relaterar allmänt till viss *konsekvens* (oönskat alternativ/resultat) och *sannolikhet* för att konsekvensen ska inträffa. Det förekommer en rad olika riskbegrepp och de vanligaste är:

- **Affärsrisk** såsom finansiell risk av att tillräckligt kassaflöde saknas eller risk att bli stämd för lagbrott
- **Försäkringsrisk** såsom risk för stöld, skada på egendom eller oväntade medicinska räkningar på semestern
- **Investeringsrisk** såsom risk att förlora kapital genom att investera i aktier, vars värde faller under investeringsnivån
- **Projektrisk** såsom risk för försening, risk att överskrida budget eller teknisk risk att inte uppnå erforderlig prestanda. Även olycksrisk (se nedan) som visar sig omöjlig eller mycket kostsam att hantera utgör projektrisk
- **Olycksrisk** som avser risk för skada på människa, egendom och/eller yttre miljö.

Olycksrisk kan ofta leda till andra typer av risker, en olycka kan påverka försäkrings- och affärsrisk.

Ordet risk kan användas i så många olika sammanhang att det är en god idé att använda olycksrisk om missförstånd kan befaras.

> I denna handbok avses med begreppet säkerhet just frånvaro av olycksrisk vilken kan leda till oavsiktlig skada. På engelska används ordet safety.

Säkerheten har med tiden blivit allt viktigare eftersom katastrofer anses möjliga att undvika och numer inte längre ses som slumpartade händelser. Samhällets ovilja att acceptera olyckor tillsammans med insikten om alla människors lika värde har bland annat lett till införande av Arbetsmiljölagen (AML). Dess syfte är att främja en god arbetsmiljö för alla arbetstagare.

Kunskapen om vad som orsakar skada växer fortlöpande. Flera ämnen och arbetssätt som tidigare ansågs säkra anses nu skadliga. Exempel på detta är asbest, bullrig miljö och freoner. Där ett ämne eller arbetssätt ger en vinst/förmån samtidigt som det orsakar skada, är det nödvändigt att ha vissa objektiva sätt att balansera de två. Ett exempel på en sådan avvägning är användningen av ett visst läkemedel mot en mycket allvarlig sjukdom, men där läkemedlet samtidigt som det botar sjukdomen kan ge upphov till mer eller mindre allvarliga biverkningar.

Säkerhet är ett känslobetonat och personligt färgat område. Många människor vill att alla risker som kan påverka dem personligen ska elimineras. Men alla risker kan inte tas bort eftersom detta dels i vissa fall samtidigt tar bort den nyttiga effekten, dels kan vara kostsamt. Tillgängliga resurser måste då prioriteras till de områden där insatsen gör störst nytta.

En balanserad syn måste tillämpas, där säkerheten varken negligeras eller tillåts dominera, så att genomförande av effektiv verksamhet möjliggörs på ett tillräckligt säkert sätt.

2.2 Därför behövs ständigt pågående säkerhetsverksamhet

Moderna system är komplexa och innehåller ofta många faror varför olyckor kan vara svåra att förutse. Vissa olyckor kan ha katastrofala konsekvenser. Teknisk utveckling leder till behov av att ersätta beprövad teknik med ny teknik, vilket leder till att konstruktioner och metoder som förr har haft en hög säkerhet, inte självklart har det längre.

Många olycksutredningar visar att det ofta är samma generella brister som återkommer. Exempel sådana är:

- Kända problem som tidigare har lett till smärre tillbud, men som aldrig till fullo har utretts och därmed inte heller åtgärdats. (Jämför stävportar som gått upp på flera av svenska försvarets stridsbåtar innan Stridsbåt 848 sjönk 2006.)
- Bedömd sannolikhet för viss olycka har underskattats, då ingen kunde föreställa sig att de omständigheter som ledde till olyckan verkligen skulle kunna inträffa. (Jämför färjan Estonia 1994.)
- Folk tror att någon annan ansvarar för och tar hand om säkerheten.
- Befintliga säkerhetsrutiner urvattnas eller slutar att tillämpas och förenklade rutiner införs mer och mer under tiden (om inga olyckor sker) eftersom de underlättar eller förbilligar verksamheten. (Jämför tillbudet i kärnkraftverket i Forsmark 2006, som till och med föranledde en inspektion av IAEA respektive katastrofen 1967 på hangarfartyget Forrestal där cirka 140 personer omkom som en direkt följd av förenklade rutiner.)
- Utrustning förändras eller används på sätt som den inte är konstruerad för. (Jämför brandkatastrofen i Kaprun 2000 där ett modifierat bergbanetåg började brinna inne i en tunnel och kostade 170 människor livet. Modifieringen bestod i att en elektrisk kupévärmare monterades under en likaledes nyinstallerad hydraulledning som senare började läcka.)

- Rapportering av tillbud sker inte alltid. Orsaken kan till exempel vara att personen som drabbats av tillbudet är rädd för att rapportera, eftersom han/hon själv har gjort ett misstag och inte vill bli straffad för detta eller att rapporteringssystemet är för krångligt att använda.

Om hanteringen av avvikelser ska fungera väl, krävs att ansvarig befattningshavare har en proaktiv *(förutseende och förekommande)* attityd. Ambitionen bör vara att förebygga olyckor istället för att reagera först när olycka eller tillbud har inträffat eller, ännu värre, att söka efter syndabockar.

Olyckor är ofta indikationer på misslyckanden från ledningens sida. Ett tydligt exempel på ett sådant misslyckande påvisas i den officiella utredningsrapporten om det kapsejsade fartyget Herald of Free Enterprise, där 188 människor dog. Rapporten innehöll bland annat följande synpunkter:

- Rederiet ansågs inte ha tagit sitt ansvar för säkerheten på sitt fartyg. Detta ansågs vara det grundläggande och huvudsakliga felet.
- Samtliga berörda i ledningen, från styrelsen ner till ledande personal ombord var medskyldiga till olyckan genom att de inte hade tagit sitt fulla ansvar inom ramen för tilldelad uppgift.

Tills alldeles nyligen lades vanligen skulden för en olycka enbart på de personer som var direkt berörda. Numera är det uttalat att säkerheten berör alla. Självklart är enskilda medarbetare ansvariga för sina handlingar, men främst chefer har behörighet och resurser att, förutom hos materiel, också rätta till attityder och organisatoriska brister, faktorer som ofta orsakar olyckor.

Säkerhetsledning är en tillämpad form av kvalitetsstyrning och definieras som alla åtgärder som syftar till att påverka säkerheten på ett verksamhetsställe och omfattar bland annat följande:

- säkerhetspolicy (att ange mål för säkerheten, till exempel att ange vad som ska skyddas respektive vad som inte får inträffa)
- säkerhetskrav
- säkerhetsorganisation, befogenheter, uppgifter

- teknisk konstruktion
- konfigurationsledning och dokumenthantering
- riskhantering (inkluderar identifiering och bedömning av risker samt riskreducering)
- erforderliga åtgärder för att styra upp utbildning
- erforderliga åtgärder för att styra upp säkerheten under användning (operatörer)
- erforderliga åtgärder för att styra upp säkerheten i anslutning till vidmakthållande (teknisk personal)
- erforderliga åtgärder för att styra upp säkerheten i anslutning till praktiska åtgärder för genomförande av avveckling (teknisk och förrådspersonal).

Försvarsmaktens säkerhetsledningssystem avser verksamhetssäkerhet och redovisas i *avsnitt 2.6*.

2.3 Hur säker är säkert?

Är detta tekniska system säkert? Det är en lätt fråga att ställa, men svår att besvara enkelt och förståeligt. Ett sätt att börja är att studera statistik från ett antal vardagsaktiviteter. I *tabell 2:1* nedan ges exempel på sannolikheten för att avlida till följd av olika aktiviteter som vi betraktar som rimliga och normala.

Tabell 2:1 Genomsnittlig sannolikhet för dödsfall vid ett antal olika aktiviteter

Sannolikhet för dödsfall per exponerad person och år (ungefärlig)	Aktivitet
1 av 100	Fem timmars ensam bergsklättring varje veckoslut
1 av 200	Rökning av 20 cigaretter per dag
1 av 5 000	Arbete i riskintensiv industri
1 av 50 000	Användning av p-piller
1 av 100 000	Arbete i den säkraste delen av industrin
1 av 500 000	Vara passagerare i ett reguljärt flygplan
1 av 1 miljon	Normal vistelse i bostad, dödad av elchock
1 av 10 miljoner	Vistelse utomhus, dödad av blixtnedslag

Dessa siffror är hämtade från ”The Tolerability of Risk from Nuclear Power Stations”, HMSO 1992 *[47]*, respektive Reliability, Maintainability and Risk, David J Smith and Butterworth Heinemann, paperback 2005 *[37]*, och kan användas för jämförelse vid bedömning av olycksrisker i den egna verksamheten.

Numeriska värden framräknade i säkerhetsanalyser bör användas med försiktighet, eftersom de flesta data enbart grundas på modeller. Även en olycksutredning är ju ett försök att bedöma hur olyckan har gått till. Fakta vid en olycka begränsas till att den har inträffat och förorsakat ett visst skadeutfall.

Alla olyckor är oönskade och kostsamma. Militära olyckor är speciella såtillvida att olyckor förorsakade av materielfel kan ha demoraliserande inverkan på militär trupp, särskilt i strid. Systemsäkerhet skapar förtroende för materielen, vilket är en av förutsättningarna för god stridsvilja.

Det är därför nödvändigt att satsa aktivt för att förhindra att olyckor kan inträffa eller att de får allvarliga konsekvenser. Tillgängliga resurser för detta inom varje enskilt projekt är dock begränsade. Därför är det viktigt att vi har bra verktyg för att identifiera VAR insatserna ska göras och HUR långt man behöver driva det riskreducerande arbetet!

2.4 Lagar

Lagar och förordningar ställer krav på de egenskaper som system ska ha för att inte skada person, egendom eller yttre miljö. I det följande redovisas några av de viktigaste lagarna. Här ges också vissa anvisningar för hur systemsäkerhetsmetodiken ska tillämpas då samtidigt särskilt lagrum (lag, föreskrift, med mera) gäller. Ett tekniskt system kan bestå av flera delsystem. Det gäller att identifiera vilka regler som är tillämpliga för respektive teknikområde. Här måste säkerställas att integrationen mellan de olika delsystemen riskanalyseras fullt ut. Exempel på överväganden och regeltillämpning lämnas sist i *avsnitt 2.5*.

I handboken redovisade referenser, dokumentbeteckningar är de som var aktuella vid handbokens färdigställande. I det fall att viss referens behöver tillämpas rekommenderas att förekomsten av senare utgåva kontrolleras.

2.4.1 Arbetsmiljölagen

Arbetsmiljölagens (AML) *[5]* ändamål är att förebygga ohälsa och olycksfall i arbetet samt att även i övrigt uppnå en god arbetsmiljö. AML reglerar såväl arbetsgivarens som arbetstagarens skyldigheter. Med arbetstagare i Försvarsmakten avses all personal, det vill säga anställd personal i Försvarsmakten samt Hemvärnets personal och personal ur de frivilliga försvarsorganisationerna då personalen deltar i verksamhet inom Försvarsmakten.

Arbetsmiljölagen är en ramlag som kompletteras med föreskrifter vilka meddelas med stöd av lagen. AML utgår från att arbetsgivaren ansvarar för att personalens säkerhet är tillfredsställande. Tillsynsmyndighet avseende AML är Arbetsmiljöverket (AV) med undantag för arbetsmiljön ombord på örlogsfartyg där Transportstyrelsen är tillsynsmyndighet.

Enligt AML ska arbetsmiljön vara tillfredsställande med hänsyn till arbetets natur och den sociala och tekniska utvecklingen i samhället. Arbetsförhållandena ska anpassas till människans olika förutsättningar i fysiskt och psykiskt avseende.

I situationer då höjd beredskap är påkallad kan regeringen meddela särskilda föreskrifter.

Arbetsgivarens ansvar anges bland annat i AML 3 kap, §§ 2 och 2a:

> ”Arbetsgivaren skall vidta alla åtgärder som behövs för att förebygga att arbetstagaren utsätts för ohälsa eller olycksfall. ...
>
> Arbetsgivaren skall systematiskt planera, leda och kontrollera verksamheten på ett sätt som leder till att arbetsmiljön uppfyller föreskrivna krav på en god arbetsmiljö. Han skall utreda arbetsskador, fortlöpande undersöka riskerna i verksamheten och vidta de åtgärder som föranleds av detta.
>
> ...”

Arbetsgivarens ansvar framgår även av 8 § Arbetsmiljöverkets föreskrifter om systematiskt arbetsmiljöarbete *[2]*:

> ”...
>
> När ändringar i verksamheten planeras, skall arbetsgivaren bedöma om ändringarna medför risker för ohälsa eller olycksfall som kan behöva åtgärdas.”

Det är viktigt att hitta riskerna innan de ”byggs in i systemet”.

Generella krav på arbetsmiljöns beskaffenhet framgår bland annat av AML 2 kap 1 §

> ”...
>
> Teknik, arbetsorganisation och arbetsinnehåll skall utformas så att arbetstagaren inte utsätts för fysiska eller psykiska belastningar som kan medföra ohälsa eller olycksfall. Därvid skall även löneformer och förläggning av arbetstid beaktas. Starkt styrt eller bundet arbete skall undvikas eller begränsas.
>
> ...”

AML 2 kap 5 §

> ”Maskiner, redskap och andra tekniska anordningar skall vara så beskaffade och placerade och brukas på sådant sätt, att betryggande säkerhet ges mot ohälsa och olycksfall.”

DesignA och leverantörs ansvar framgår av AML 3 kap, §§ 1, 8–10

1 §

> ”Bestämmelserna i detta kapitel skall tillämpas med beaktande av kraven på arbetsmiljöns beskaffenhet enligt 2 kap. Lag (1994:579).”

8 §

”Den som tillverkar, importerar, överlåter eller upplåter en maskin, ett redskap, skyddsutrustning eller annan teknisk anordning ska se till att anordningen erbjuder betryggande säkerhet mot ohälsa och olycksfall, när den släpps ut på marknaden, avlämnas för att tas i bruk eller ställs ut till försäljning.

...

Anvisningar för anordningens montering, installation, användning och skötsel samt övriga uppgifter om anordningen som är av betydelse för att förebygga ohälsa och olycksfall (produktinformation) ska medfölja vid avlämnandet genom tydlig märkning, i form av handlingar eller på annat sätt. Information av särskild betydelse för arbetsmiljön ska lämnas vid marknadsföring av anordningen. Lag (2008:295).”

9 §

”Den som tillverkar, importerar eller överlåter ett ämne, som kan föranleda ohälsa eller olycksfall, skall vidta de åtgärder som behövs för att hindra eller motverka att ämnet vid avsedd användning innebär risk från skyddssynpunkt.

Vad som sägs i 8 § tredje stycket om produktinformation och information vid marknadsföring skall gälla även i fråga om ämnen som kan föranleda ohälsa eller olycksfall. Lag (2002:585).”

10 §

”Den som överlåter eller upplåter en förpackad produkt skall se till att förpackningen inte innebär risk för ohälsa eller olycksfall. Lag (1991:677).”

Föreskrifter under AML

Arbetsmiljölagen är en ramlag som ger regeringen rätt att uppdra åt viss myndighet, i detta fall Arbetsmiljöverket (AV), att vid behov utge kompletterande föreskrifter till lagen vilket görs fortlöpande.

Föreskrifter om maskiner

AV:s föreskrift om maskiner (AFS 2008:3, vilken grundar sig på EU:s direktiv 2006/42 om maskiner) **undantar** ”maskiner som är särskilt konstruerade och tillverkade för *militära* eller *polisiära* ändamål”.

Maskin för militärt ändamål definieras här som tekniskt system avsett för att genomföra organiserad, väpnad strid.

AV:s särskilda föreskrift om maskiner (AFS 2008:3) specificerar en lång rad säkerhetskrav som ska användas för olika tillämpningar. Principen är att för en viss omnämnd tillämpning med generellt kända risker motverkas dessa risker genom föreskrivna säkerhetskrav.

Bakgrunden till detta undantag för militär materiel är att militär verksamhet ställer krav på avancerad materiel, ofta grundad på ny teknologi respektive särskilda applikationer vilka om möjligt inte ska delges potentiell motståndare. Att teknologi och applikation är sekretesskyddade omöjliggör därvid framtagande av harmoniserade säkerhetsstandarder som utgör krav vid framtagning av ”civil” materiel.

AV:s särskilda föreskrift för maskiner gäller därmed **inte** för militär materiel.

Behov av särskilt regelverk för militär materiel

För att säkerställa tillgång till en arbetsmetodik för hantering av risker vid framtagning och användning av militär materiel låter ÖB fastställa systemsäkerhetsmetodiken, vilken i detalj är reglerad i denna Försvarsmaktens handbok Systemsäkerhet 2011.

> Systemsäkerhetsmetodiken syftar till att identifiera och hantera risker.

AV föreskrifter med gränsvärden med mera

AV har utfärdat ett antal föreskrifter med detaljerade krav och regler. Majoriteten av dessa är generella och gäller alltid (med vissa undantag enligt nedan). Föreskrifterna ska vara väl kända av och noggrant tillämpas hos den som mottar uppdrag avseende framtagning av materiel till Försvarsmakten. I vissa av AV utfärdade AFS finns specificerade gränsvärden, för till exempel luftföroreningar (hygieniska gränsvärden), buller och vibrationer. Dessa gränsvärden ska speciellt beaktas.

Detta innebär att, utöver tillämpning av systemsäkerhetsmetodiken för angivet militärt tekniskt system, kan det samtidigt finnas krav som ska tillämpas enligt särskilda föreskrifter från AV för aktuellt tekniskt system, eller i detta ingående teknisk applikation, att särskilda certifikat eller motsvarande ska tas fram som intygar att dessa krav är uppfyllda.

Militärt undantag från gränsvärden med mera i AV föreskrifter

Vissa av AV:s föreskrifter innehåller särskilt uttryckta undantag för militär användning. Exempel på sådana föreskrifter är AFS om arbetsplatsens utformning, EU:s direktiv 1999/5 (radioutrustning och teleterminalutrustning) respektive AFS om maskiner. Genom undantaget för militär användning avser lagstiftaren att ge Försvarsmakten erforderlig handlingsfrihet att utforma tekniskt system enligt ”krigets krav”, men med fortsatt innehållande av grundkravet som ställs på arbetsgivaren i AML, se ovan. För att kunna använda den avsedda handlingsfriheten på ett ansvars-

fullt sätt behövs att Försvarsmakten tar fram egna tillämpningsanvisningar med riktlinjer, gränsvärden med mera som Försvarsmakten definierar som tolerabel för svensk militär personal.

Viss civil lagstiftning inom arbetsmiljöområdet anger uttryckligen undantag för militär materiel respektive militär användning (jämför *1.2*). Om sådan lag anger krav på gränsvärden behöver Försvarsmakten särskilt ange de krav som ska tillämpas i motsvarande syfte inom Försvarsmakten för att tillgodose skydd för den militära personal som ska bemanna/vistas i det tekniska systemet (avser till exempel AFS om arbetsplatsens utformning).

Eftersom lagstiftning fortlöpande förändras är det ett mycket omfattande arbete att fortlöpande identifiera lagar med militära undantag. Lämpligen hanteras identifiering av lagar med militärt undantag genom att ge leverantör ansvar för sådan identifiering. Uppgiften utformas som ett krav i anbudsinfordran så att leverantören redan under anbudstiden ska anmäla sådan lag till DesignA och begära anvisning om vilka krav som ska tillämpas för Försvarsmaktens tekniska system i aktuellt avseende. DesignA återkommer därvid till Försvarsmakten med begäran om kompletterande krav i aktuellt avseende.

2.4.2 Produktansvarslagen och systemsäkerhet

Produktansvarslagen (PAL) reglerar förutsättningar för skadestånd för skada som en produkt har orsakat på enskild person eller enskild egendom och är därmed en lag för konsumentskydd. Av 1 § framgår:

> ”Skadestånd enligt denna lag betalas för personskada som en produkt har orsakat på grund av en säkerhetsbrist.
>
> Skadestånd enligt denna lag betalas också för sakskada som en produkt på grund av en säkerhetsbrist har orsakat på egendom som till sin typ vanligen är avsedd för enskilt ändamål, om den skadelidande vid tiden för skadan använde egendomen huvudsakligen för sådant ändamål. Skador på själva produkten ersätts dock inte.”

Vidare ges en juridisk definition för begreppet säkerhetsbrist i 3 §:

> ”En produkt har en säkerhetsbrist om produkten inte är så säker som skäligen kan förväntas. Säkerheten skall bedömas med hänsyn till hur produkten kunnat förutses bli använd och hur den har marknadsförts samt med hänsyn till bruksanvisningar, tidpunkt då produkten satts i omlopp och övriga omständigheter.”

Denna beskrivning av Produktansvarslagen görs dels för att utgöra allmän information, dels för att visa att det inte finns några kopplingar till H SystSäk.

En produkt som används av en person i dennes anställning omfattas i första hand av AML 3 kap, 2 § med flera paragrafer samt av arbetsgivarens ansvar för en god och säker arbetsmiljö.

2.4.3 Miljöbalken och systemsäkerhet

Miljöbalken syftar till att främja en hållbar utveckling som innebär att nuvarande och kommande generationer tillförsäkras en hälsosam och god miljö. Balken gäller för all verksamhet som har, eller kan ha, miljöpåverkan. Den som bedriver en verksamhet är skyldig att ha kunskap om den miljöpåverkan som verksamheten medför. Verksamhetsutövare är skyldig att utföra de skyddsåtgärder, iaktta de begränsningar och vidta de försiktighetsmått som behövs för att förebygga, hindra eller motverka att verksamheten medför skada eller olägenhet för människors hälsa eller miljön. Bästa möjliga teknik ska användas och produkter ska väljas som har minst miljöpåverkan. Verksamhetsutövare ska hushålla med råvaror och energi samt använda möjligheterna till återanvändning och återvinning. Detaljerat regelverk finns i följdlagstiftningen till miljöbalken.

Dessa skyddsåtgärder, försiktighetsmått med mera ska vidtas så snart det finns skäl att anta att en verksamhet eller åtgärd kan medföra skada eller olägenhet.

Central tillsynsmyndighet för Miljöbalken är Naturvårdsverket (på det regionala planet har också länsstyrelserna ett delansvar). Inom försvarsdepartementets ansvarsområde utövar Generalläkaren tillsyn över Miljöbalken vid Försvarsmakten, Försvarets materielverk, Fortifikationsverket och Försvarets radioanstalt.

Utöver miljöbalken finns ett flertal andra lagar, förordningar och föreskrifter som ställer specificerade krav till skydd för yttre miljö.

Miljöbalken med flera lagar ska tillämpas för alla de tekniska system som tas fram till Försvarsmakten.

Tillämpning av H SystSäk syftar till att identifiera olycksrisker som ett tekniskt system kan vålla, och där konsekvenserna kan omfatta också skada på yttre miljö.

2.4.4 Ellagen och systemsäkerhet

Allmänt

God elsäkerhet är en förutsättning för Försvarsmaktens verksamhetssäkerhet.

Tekniska system och produkter ska vara konstruerade för avsett ändamål och kravställda klimat och miljöer.

För tekniskt system som innehåller el-spänning över 50 volt, ska god elsäkerhet säkerställas vid utveckling och anskaffning genom att krav på elsäkerhet och elektrisk konstruktion omhändertas.

Sveriges ellagstiftning har genom inträdet i EU förändrats väsentligt, från att tidigare ha haft en regelstyrande inriktning till målstyrning. Det övergripande målet är att system och produkter ska vara säkra. Detta ställer ökade krav på att det elektriska utförandet av system och materiel, vad gäller elsäkerhet, särskilt omhändertas i systemsäkerhetsarbetet.

DesignA ansvarar för att tekniska system och produkter är säkra och uppfyller tilllämplig lagstiftning och standarder, eller är utförda på annat, av DesignA, dokumenterat sätt.

Ellagen

Ellagen *[8]* behandlar bland annat elsäkerhet och anger i 9 kap 1 §:

> ”Elektriska anläggningar, elektriska anordningar avsedda att anslutas till sådana anläggningar, elektrisk materiel och elektriska installationer skall vara så beskaffade och placerade samt brukas på sådant sätt att betryggande säkerhet ges mot person- eller sakskada eller störning i driften vid den egna anläggningen eller vid andra elektriska anläggningar.”

Ellagens krav förtydligas i förordningar vilka också ger Elsäkerhetsverket möjlighet att ge ut föreskrifter inom elområdet. De förordningar som främst påverkar utformning av tekniskt system innehållande elektrisk materiel är:

Förordning om elektrisk materiel	SFS 1993:1068
Starkströmsförordning	SFS 2009:22
Elinstallatörsförordning	SFS 1990:806
Förordning om elektromagnetisk kompatibilitet	SFS 1993:1067

Lagar och förordningar inom elområdet har en övergripande utformning och lydelse med säkerhet som målsättning. Myndigheter och standardiseringsorganisationer tar fram föreskrifter och standarder för tillämpning inom elområdet, baserade på lagar och förordningar.

Föreskrifter

Elsäkerhetsverket är tillsynsmyndighet för elsäkerhet.

Ellagen anger att elanläggning, elanordning och motsvarande, ska vara säker. Vad som kan bedömas vara säkert vid olika situationer och utföranden redovisas i elsäkerhetsområdets föreskrifter och standarder, eller av DesignA speciellt dokumenterade och fastställda anvisningar utgivna som teknisk order (TO) eller annan form av teknisk publikation.

DesignA anger i anbudsinfordran till leverantör vilka särskilda krav som det tekniska systemet ska uppfylla avseende elsäkerhet, genom hänvisning till de standarder som är tillämpliga. Detta kan också ske genom hänvisning till DesignA speciellt fastställd anvisning eller en kombination av dessa.

Tekniska system och produkter för Försvarsmaktens ändamål kan i vissa fall kräva utföranden som inte finns beskrivna i standard, vilket då alltid kräver att DesignA beskriver och dokumenterar utförandet så att det kan uppfylla kravet på att vara säkert.

Handbok Elsäkerhet

Elsäkerhet ingår som en naturlig del i verksamhetssäkerheten inom Försvarsmakten. Handbok Elsäkerhet i Försvarsmakten *[30]*, H Elsäk, har som syfte att stödja förband, skolor och centra i deras arbete med att implementera och bedriva systematiskt elsäkerhetsarbete, förebygga olyckor och skapa ett samordnat synsätt för området elsäkerhet inom hela Försvarsmakten.

Systemsäkerhet

Utöver ovanstående utformningskrav, ska systemsäkerhetsverksamhet genomföras enligt H SystSäk metodik för hela det tekniska systemet, varvid bland annat riskanalys genomförs för systemet, dess gränsytor och dess användning för avsett ändamål.

Detta innebär att det för tekniskt system för vilket Ellagen är tillämplig, ska vidtas såväl riskreducerande åtgärder enligt H SystSäk som säkerhetsåtgärder enligt angivna utformningskrav.

2.4.5 Fartygssäkerhetslagen, RMS och systemsäkerhet

Förordningen om säkerhet på örlogsfartyg anger vilka delar av Fartygssäkerhetslagen som ska gälla för örlogsfartyg. Transportstyrelsen meddelar föreskrifter för örlogsfartygs sjövärdighet och har med föreskrift gett Försvarsmakten i uppgift att i samråd med Transportstyrelsen utarbeta regler för kontroll av fartygs sjövärdighet samt att kontrollera fartygs sjövärdighet. Inom Försvarsmakten har ÖB gett C SÄKINSP bemyndigande att fastställa sådana regler samt att utöva tillsyn över örlogsfartyg. Regelverket heter RMS, Regler för militär sjöfart.

RMS tillämpas på Militär sjöfart, örlogsfartyg och dykerisystem.

Alla fartyg och båtar som tillhör Försvarsmakten eller står under militärt befäl är örlogsfartyg.

För varje örlogsfartyg som ska utvecklas, inköpas, inhyras, byggas om, tilldelas nytt fartområde eller nya uppgifter, ska ett uppstartningsmöte med Militära sjösäkerhetsinspektionen genomföras. Vid detta uppstartningsmöte beslutas tillämpliga krav som ska uppfyllas (jämför bland annat RMS-F *[36]*).

Örlogsfartyg ska för att få användas i fredstid, vara sjövärdigt och försett med sjövärdighetsbevis och motsvarande gäller för dykerimateriel. Ett sjövärdighetsbevis eller motsvarande styrker alltså att gällande regelverk är uppfyllda.

Sjövärdighetsbevis omfattar normalt inte de ledningssystem, vapensystem och gränsytor till andra system som kan innebära andra risker för systemet.

Utöver sjövärdighetsbevis eller motsvarande, ska systemsäkerhetsverksamhet genomföras enligt H SystSäk metodik för hela systemet, varvid bland annat riskanalys genomförs för systemet, dess gränsytor och dess användning som sjöstridssystem.

Detta innebär att det ska vidtas såväl riskreducerande åtgärder enligt H SystSäk som säkerhetsåtgärder enligt RMS, för örlogsfartyg och dykerisystem.

Militär sjösäkerhet syftar till att inom den militära sjöfarten förebygga olycksrisker som kan orsaka död, olycksfall eller ohälsa, skada på eller förlust av utrustning, materiel och egendom eller skada på yttre miljö. Sjövärdighet är liksom arbetsmiljö, bemanning, last/ballast och yttre miljö delar av fartygssäkerheten. Ett fartyg sägs vara sjövärdigt när det, med hänsyn till sitt ändamål och fartområde, är så konstruerat, byggt, utrustat och underhållet att det ger betryggande säkerhet mot sjöolyckor.

Sjövärdighet utgörs, utöver arbetsmiljö till stora delar av tekniska krav på utförande och funktion rörande fartygskonstruktion och utrustning, till exempel skrov, flytbarhet, stabilitet, styranordningar, maskineri, rör och pumpar, läns- och läcktätningsanordningar, tryckkärl, lyftredskap, elektriska anläggningar, brandskydd, livräddning, förtöjning, navigations- och kommunikationsutrustning och sjösurrningar. Ett fartyg eller en båt sägs vara sjövärdig(t) om ställda krav är uppfyllda.

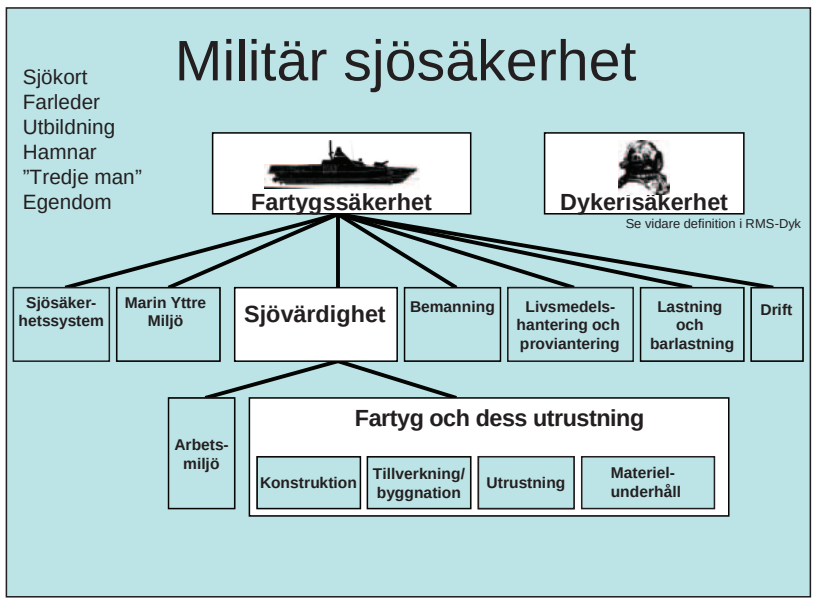


Bild 2:1 Militär sjösäkerhet

Avseende sjövärdigheten på Försvarsmaktens fartyg och båtar föreligger en förordning om säkerheten på örlogsfartyg, SFS 2003:440, vilken säger att vissa delar av fartygssäkerhetslagen, SFS 2003:364, ska tillämpas även på örlogsfartyg.

På grund av örlogsfartygs speciella karaktär och användning går det inte att inom alla områden direkt tillämpa Transportstyrelsens författningshandbok varför örlogsmarina tillämpningsbestämmelser har utarbetats och sammanställts i Regler för militär sjöfart, (RMS).

2.4.6 RMM och systemsäkerhet

Regler för militär markverksamhet, RMM *[35]*, är Försvarsmaktens styrdokument för genomförande av ett systematiskt marksäkerhetsarbete. Det systematiska marksäkerhetsarbetet omfattar utformning och granskning av Försvarsmaktens verksamhetsledningssystem samt utformning och granskning av specifika kravformuleringar på förband och materielsystem.

RMM är också styrdokumentet för utformning av Försvarsmaktens marksäkerhetsmanual, förbandsmanualer och kontingentsmanualer.

RMM ska tillämpas av alla som bedriver verksamhet inom Försvarsmakten eller i Försvarsmaktens regi, nationellt och internationellt, då verksamheten inte är hänförbar till militär sjöfart eller militär luftfart.

Verksamhetssäkerheten för de system på marken eller som hanteras från marken och som är direkt sjösäkerhets- respektive flygsäkerhetspåverkande hänförs till sjö- respektive flygsäkerhet och regleras i Regler för militär sjöfart (RMS) respektive Regler för militär luftfart (RML) och återfinns således inte i RMM.

RMM består av två delar, RMM-Grunder (G) och RMM-Marksäkerhetssystem (M). Avsikten är att komplettera med ytterligare delar efterhand, bland annat RMM-T som kommer att innehålla regler och krav på teknisk systemsäkerhet.

2.4.7 Luftfartslagen, RML och systemsäkerhet

Luftfartslagen

All verksamhet som anses som luftfartsverksamhet är tillståndspliktig enligt luftfartslagen. Regeringen eller den myndighet regeringen bestämmer anger de villkor och bestämmelser som gäller för att utöva luftfartsverksamhet i Sverige samt för svenskt registrerat luftfartyg som används utomlands.

För den civila luftfarten samt för flygtrafiktjänst för både civil och militär luftfart, har regeringen bemyndigat Transportstyrelsen att besluta om föreskrifter samt att vara tillsynsmyndighet. EU har genom EASA (European Aviation Safety Agency) stort inflytande över den civila luftfarten inom unionens område. Detta inflytande utövas bland annat genom EU-förordningar och EU-direktiv som direkt eller indirekt gäller för den civila luftfarten.

För det militära luftfartssystemet är Försvarsmakten den myndighet som utfärdar föreskrifter och utövar tillsyn. Detta förhållande gäller även för flygtrafiktjänst för militär luftfart om detta ska utövas av en auktoriserad verksamhetsutövare inom det militära luftfartsystemet utanför Sverige.

Det militära luftfartssystemet

Överbefälhavaren ansvarar för militär flygsäkerhet inom det militära luftfartsystemet.

Bestämmelser för den militära luftfarten framgår av Regler för militär luftfart (RML) *[34]*. Chefen för Säkerhetsinspektion inom Försvarsmakten är bemyndigad att fastställa RML. Försvarsmaktens Flygsäkerhetsinspektör, FSI, ansvarar för myndighetsutövning och tillsyn med stöd av RML och leder den militära flyginspektionen (FLYGI) vid Högkvarteret.

Definition av militär luftfart utgår från Försvarsmaktens definition av begreppet i RML. Genom definitionen anges att militär luftfart är all luftfart inom det militära luftfartssystemet. Det omfattar också all utveckling, anskaffning, nyttjande, vidmakthållande och avveckling av förband och materielsystem. Det är också fråga om mark, anläggningar, lokaler och förnödenheter i det militära luftfartssystemet.

I begreppet militär luftfart ingår därmed all flygning med mera som utförs för ett militärt ändamål och även den verksamhet som betecknas som luftfartsrelaterade tjänster. Till detta hänförs förutom Försvarsmaktens egen verksamhet, verksamhet inom Försvarets materielverk och hos viss försvarsindustri som till exempel Saab AB samt hos vissa civila underhållsverkstäder och leverantörer av luftfartsprodukter både inom och utom Sverige. Militär luftfart kan således bedrivas även av ett företag.

Auktoriserad designorganisation

När Försvarsmakten anskaffar nya luftfartsprodukter eller delar och anordningar till dessa eller beställer ändringar till luftfartsprodukter, krävs av aktuell leverantör (designorganisation) att denne är, av FSI, auktoriserad medlem av det militära luftfartssystemet. Auktorisation för viss designorganisation utfärdad av annan behörig myndighet (till exempel Transportstyrelsen, FAA, CAA, DGA) kan godtas av FSI.

Förenklat kan systemet beskrivas genom att det ska finnas:

- en enligt RML-V-5J auktoriserad designorganisation som har ansvaret på materielsystemnivå, (nivå 2 enligt RML), vilket normalt är Försvarets materielverk
- en enligt RML-V-5JA auktoriserad designorganisation som har ansvaret på produktnivå (nivå 3 enligt RML), vilket normalt är industrin, men också kan, för så kallade ”legacy aircraft”, vara Försvarets materielverk.

  Notera att RML-V-5N reglerar importförfarande.

På systemnivå 2 har designorganisationen ansvar för att det kompletta flygmaterielsystemet, luftfartyg, räddningssystem, vapensystem, personlig utrustning med mera, är säkert för tänkt användning.

Godkännande av produkt och materielsystem

Generellt sett ska ett beslut om användning (BOA) utfärdas innan materiel kan tas i bruk inom Försvarsmakten. Detta BOA avser tillse att materielen är säker ur främst arbetsmiljöperspektiv och att övriga förutsättningar finns.

För luftfartsprodukter tillkommer Regler för militär luftfart (RML), vilka ställer krav på materiel och organisation inom det svenska militära luftfartssystemet. Allmänt krävs att luftfartyg innan de tas i bruk i det svenska militära luftfartssystemet är certifierade av FSI, det vill säga att ett Militärt Typcertifikat (MTC) har utfärdats. Det flygmaterielsystem, vari luftfartyget ingår, ska även det vara godkänt av FSI, vilket sker via utfärdande av Materielsystemintyg (MSI). MTC och MSI är exempel på luftfartsdokument. Innehavaren (designorganisationen) åtar sig ansvar enligt RML (bland annat att följa luftfartsprodukten under drift och att vid behov införa nödvändiga förbättringar) för hela produktens respektive materielsystemets livslängd.

När FSI har utfärdat ett MSI och/eller MTC krävs inget ytterligare samråd från säkerhetsinspektionen inför CSSB eller BOA.

De av FSI godkända designorganisationerna ansöker om MTC eller MSI, varefter en kravsamling överenskoms och formaliseras, en så kallad certifieringsbas. Efter verifiering med mera utfärdar designorganisationerna en typ- eller materielsystemdeklaration, som bland annat anger att kraven är uppfyllda (eller, om så inte är fallet, hur kompensation skett så att likvärdig säkerhetsnivå uppnåtts) och att typen eller materielsystemet är säkert för tänkt användning. För att kunna konstatera detta krävs att systemsäkerhetsarbete genomförts. När FSI, efter FLYGI granskning, sedermera utfärdar ett MTC eller ett MSI kan dessa ses som FSI ”kvittens” på deklarationen.

Vilka krav som gäller för ansökan om och utfärdande av MTC och MSI framgår i RML-V-5B.

Vid större ändring av typ- eller flygmaterielsystemdeklaration används motsvarande process. I ändring av mindre omfattning se RML-V-5D.

Den standard som ska tillämpas för systemsäkerhetsarbetet föreslås av aktuell designorganisation och accepteras av granskande myndighet (FLYGI). Ett exempel på standard är MIL-STD-882C, men det finns flera standarder som tillämpas av flygindustrin. När det gäller programvarusystem ingående i luftfartyg är ofta den tillämpade processtandarden RTCA/DO-178B *[38]*.

Andra standarder och metoder vid redovisning än de som är angivna i H SystSäk får, efter FSI acceptans, användas vid systemsäkerhetsarbete avseende luftfartsprodukter.

Ovanstående beskrivning är generell och gäller som princip för samtliga materielsystem som är flygsäkerhetspåverkande. Dock kan det förekomma undantag som antingen är föranledda av att äldre materielsystem är konstruerade och tagna i bruk när andra regler gällde eller att materielsystem anses ha en lägre grad av flygsäkerhetspåverkan och därför inte bedöms behöva MSI och/eller MTC. Designkraven i RML V-5 ska dock alltid tillämpas vid nyanskaffning och större ändringar av flygmaterielsystem inklusive UAV-system.

Godkännande av enkel produkt eller enkelt materielsystem

Om produkt eller materielsystem inom det militära luftfartsystemet ska tas i bruk och det beslutats att det inte krävs MSI och/eller MTC ska systemsäkerhetsarbete normalt utföras enligt H SystSäk och samråd inhämtas hos säkerhetsinspektionen inför CSSB och BOA. FSI kan efter förslag från designorganisationen acceptera andra etablerade standarder och rapporteringsförfaranden även i dessa fall.

2.4.8 Fordons säkerhet, utrustning och systemsäkerhet

Fordonslagen

Fordonslagen *[13]* innehåller bestämmelser om

- kontroll av fordon samt därtill hörande system, komponenter och separata tekniska enheter
- kontroll av fordons last
- kontroll av färdskrivare och taxameter och kontroll av användningen av dessa
- den verksamhet som bedrivs av besiktningsorgan på fordonsområdet.

Fordonslagen gäller inte

- fordon som tillhör staten och är tillverkade för särskilda militära ändamål
- motordrivna fordon som är avsedda att föras av gående eller släpfordon som har kopplats till något sådant fordon
- fordon som används uteslutande inom inhägnade järnvägs- eller industriområden eller inom inhägnade tävlingsområden eller andra liknande inhägnade områden
- lekfordon.

Fordonsförordningen *[12]* innehåller bestämmelser om

- fordons beskaffenhet och utrustning
- kontroll av fordon samt därtill hörande system, komponenter och separata tekniska enheter
- den verksamhet som bedrivs av besiktningsorgan på fordonsområdet.

Fordonsförordningen gäller inte

- fordon som tillhör staten och är tillverkade för särskilda militära ändamål
- motordrivna fordon som är avsedda att föras av gående, eller släpfordon som har kopplats till något sådant fordon
- fordon som används uteslutande inom inhägnade järnvägs- eller industriområden eller inom inhägnade tävlingsområden eller andra liknande inhägnade områden
- lekfordon
- trafik på väg och i terräng vid militär operation och militär övning med mera.

Militärtrafikförordningen *[31]* innehåller särskilda bestämmelser om

- beskaffenhet och utrustning för fordon som brukas av Försvarsmakten, Försvarets materielverk och Försvarets radioanstalt
- besiktning av fordon för registrering i det militära fordonsregistret
- registrering av fordon i det militära fordonsregistret
- behörighet att föra fordon som brukas av Försvarsmakten, Försvarets materielverk och Försvarets radioanstalt
- utbildning av fordonsförare inom Försvarsmakten
- förordnande av personal att utföra vissa uppgifter inom trafikområdet.

Militärtrafikförordningen 3 kap innehåller bestämmelser om fordons beskaffenhet och utrustning.

Försvarsmakten får meddela föreskrifter om fordon som tillhör staten och är tillverkade för särskilda militära ändamål. Ett sådant fordon får brukas i trafik endast om det är tillförlitligt från trafiksäkerhetssynpunkt och i övrigt lämpligt för trafik.

För fordon som tillverkats för särskilda militära ändamål får Försvarsmakten själva meddela föreskrifter om registreringsbesiktning av fordon. Registreringsbesiktning och provning inför ett enskilt godkännande får utföras av ett ackrediterat besiktningsorgan eller av en militär besiktningsman.

Godkänns ett fordon vid en registreringsbesiktning eller genom enskilt godkännande ska de uppgifter som ska föras in i det militära fordonsregistret lämnas till Försvarsmakten.

I Vägverkets författningssamling (VVFS 2003:22) ges fordon som är registrerade i militära fordonsregistret och som brukas av Försvarsmakten, Försvarets materielverk och Försvarets radioanstalt undantag avseende viss utrustning för fordon.

På uppdrag från Försvarsmakten utarbetar Försvarets materielverk underlag för föreskrifter, allmänna råd och riktlinjer avseende trafikvärdighet hos fordon som är registrerade i militära fordonsregistret (MIFOR) eller som tillhör eller brukas av Försvarsmakten, Försvarets materielverk och Försvarets radioanstalt.

Dessa underlag kan gälla följande:

- fordons beskaffenhet och utrustning
- registrering av fordon
- löpande kontroll av fordon.

Ett fordon är trafikvärdigt om det är konstruerat, byggt, verifierat, utrustat och underhållet på ett sådant sätt, samt har sådana egenskaper, att säkerhets- och miljökrav är uppfyllda.

Militärtrafikförordningen 2 kap ger Försvarsmakten möjlighet till vissa undantag från civil trafiklagstiftning.

Systemsäkerhet för fordonsmateriel

Trafikvärdighet omfattar ett fordons egenskaper i trafik. Fordonssystem kan vara komplext och förutom fordon omfatta till exempel ledningssystem, vapensystem samt eventuella gränsytor till andra system. Det komplexa tekniska systemets olycksrisker kan därmed ha varierande ursprung.

Utöver åtgärder för att uppfylla krav på trafikvärdighet, ska systemsäkerhetsverksamhet genomföras enligt H SystSäk metodik för det totala tekniska systemet, inklusive gränsytor, för dess användning som markstridssystem.

FMV har sammanställt en designregelsamling (FMV Handbok Fordonssäkerhet, H FordonSäk) *[10]*.

H FordonSäk syftar till att hantera risker i fordonssystem innehållande känd teknik. För att hantera risker i nyare teknik samt risker till följd av integration tillämpas H SystSäk parallellt med H FordonSäk.

2.4.9 Förbindelsemateriel och systemsäkerhet

Allmänt

Det tekniska systemet förbindelsemateriel syftar till att skapa förbindelse över vattendrag och andra terränghinder. Systemet måste grupperas innan avsedd förmåga kan levereras. För förbindelsemateriel är kraven på grupperingsplats mycket höga vad avser markens förmåga att ge tillräcklig bärighet för att förhindra att det tekniska systemet sjunker ner i marken, varvid tippning eller vältning kan inträffa. Markens bärighet måste fortlöpande kontrolleras då förbindelse är upprättad.

Förbindelsemateriel delas in i fast och flytande bromateriel. Med materielen kan både broar och färjor byggas.

Krav för förbindelsesystem delas in i två delar, utformnings- respektive driftsäkerhetskrav, de senare kraven beskrivs inte i H SystSäk.

Utformningskrav

Lagkrav för dimensionering och användning av förbindelsemateriel är definierade i Plan- och bygglagen *[33]* samt Sjölagen *[41]*.

För utformning av och verifiering av militära förbindelsesystem tillämpas regelverket, Trilateral Design and Test Code for military bridging and gap-crossing equipment från 2005.

Systemsäkerhet

Utöver ovanstående utformningskrav ska systemsäkerhetsverksamhet genomföras enligt H SystSäk metodik för hela systemet, varvid bland annat riskanalys genomförs för systemet, dess gränsytor och dess användning som förbindelseskapande tekniskt system.

Detta innebär att det för förbindelseskapande tekniskt system ska vidtas såväl riskreducerande åtgärder enligt H SystSäk som säkerhetsåtgärder enligt angivna utformningskrav.

2.4.10 Medicinteknisk utrustning och systemsäkerhet

Allmänt

Medicinteknisk utrustning avser tekniskt system med förmåga att ge medicinsk vård respektive medicinsk transport. På grund av de särskilda krav som finns om patientsäkerhet är medicintekniska system till sin karaktär specifika.

Läkemedel omfattas inte av detta avsnitt då detta ansvarsområde omhändertas av Försvarsmedicinskt Centrum.

Utformningskrav

Lag om medicintekniska produkter *[29]* samt förordning om medicintekniska produkter *[15]* innehåller bestämmelser om medicintekniska produkter. För vissa sådana produkter finns härutöver bestämmelser i annan lagstiftning.

Med en medicinteknisk produkt avses i lagen en produkt som enligt tillverkarens uppgift ska användas, separat eller i kombination med annat, för att hos människor:

- påvisa, förebygga, övervaka, behandla eller lindra en sjukdom
- påvisa, övervaka, behandla, lindra eller kompensera skada eller funktionsnedsättning
- undersöka, ändra eller ersätta anatomin eller en fysiologisk process
- kontrollera befruktning.

Läkemedelsverket får föreskriva att lagen om medicintekniska produkter ska gälla även för andra produkter som nyttjas i ett medicintekniskt system eller som på annat sätt i fråga om användningen står nära medicintekniska produkter. Läkemedelsverket får också föreskriva att lagen om medicintekniska produkter helt eller delvis inte ska gälla i fråga om vissa medicintekniska produkter.

Systemsäkerhet

Utöver ovanstående utformningskrav ska systemsäkerhetsverksamhet genomföras enligt H SystSäk metodik för aktuellt medicintekniskt system för att identifiera olycksrisker som kan vålla skada på person (också som patient), egendom och yttre miljö. Vid eventuellt motstridiga krav går patientsäkerhet före systemsäkerhet.

2.4.11 Ammunition och systemsäkerhet

Allmänt

Lagen om Brandfarliga och explosiva varor (LBE) *[28]* gäller hantering och import av brandfarliga och explosiva varor. Lagens syfte är att hindra att sådana varor orsakar brand eller explosion som inte är avsedd samt att förebygga och begränsa skador på liv, hälsa, yttre miljö eller egendom genom brand eller explosion vid hantering av sådana varor.

Lagen om brandfarliga och explosiva varor (LBE) *[28]* anger i 12 §:

> ”För att en explosiv vara ska få släppas ut på marknaden ska den ha bedömts överensstämma med vad som ska godtas enligt bestämmelser som gäller inom Europeiska ekonomiska samarbetsområdet eller, om det inte finns sådana bestämmelser, ha godkänts av den myndighet som regeringen bestämmer.”
>
> *Avviker från den tryckta boken H SystSäk 2011; ovanstående text är hämtad från Lag (2010:1011) om brandfarliga och explosiva varor.*

Sprängämnesinspektionens[1] föreskrifter om import och om överföring av explosiva varor (SÄIFS 1997:5) *[42]* lyfter fram Europarådets direktiv 93/15/EEG om harmonisering av bestämmelserna om utsläppande på marknaden och övervakning av explosiva varor för civilt bruk (explosivvarudirektivet). Föreskriften säger i avsnitt 1.2 att:

- ”Vad avser godkännande av explosiv vara som importeras samt bedömning av överensstämmelse eller godkännande av explosiv vara som överförs gäller särskilda bestämmelser.
- Godkännande som avses i 10 § förordningen om brandfarliga och explosiva varor erfordras inte vid hantering, import eller överföring av ammunition som omfattas av vapenlagen (1996:67) om ammunitionen genomgått kontroll i enlighet med konventionen av den 1 juli 1969 om ömsesidigt erkännande av kontrollstämplar på handeldvapen (CIP-konventionen) och försetts med CIP-stämpel.”

Utformnings- och granskningskrav avseende ammunition för militärt ändamål (”militär ammunition”)

Förordningen om folkrättslig granskning av vapenprojekt *[16]* anger att granskning av projekt ur folkrättslig synvinkel ska ske av Delegationen för folkrättslig granskning av vapenprojekt. Förordningen ställer krav på att bland annat Försvarsmakten snarast möjligt ska anmäla till Delegationen varje projekt som avser studium, utveckling, nyanskaffning eller modifiering av vapen eller stridsmetoder.

Försvarets materielvek har under en lång följd av år, och på Försvarsmaktens uppdrag, sammanställt och vidareutvecklat en designregelsamling (FMV Handbok Vapen- och Ammunitionssäkerhet, H VAS) *[11]*. H VAS omfattar ammunition avsedd för militärt ändamål. H VAS redovisar krav på säkerhetsegenskaper hos de funktioner som förekommer i militär ammunition.

1. SÄI har upphört att vara egen myndighet. Funktionen återfinns numer i Myndigheten för samhällsskydd och beredskap, MSB.

H VAS syftar till att hantera risker i ammunition innehållande känd teknik. För att hantera risker i nyare teknik samt risker till följd av integration tilllämpas H SystSäk parallellt med H VAS. Vid anskaffning av ammunition behöver detta kravställas särskilt.

H VAS innehåller även specifika krav för militär ammunition som följer av folkrättskrav.

Vid Försvarets materielverk finns en särskild funktion för oberoende granskning av militär ammunition. Vidmakthållande av funktionen sker på uppdrag från Försvarsmakten. Denna funktion har kompetens att utföra granskning av militär ammunition, också på uppdrag direkt av Försvarsmakten samt av annan leverantör/DesignA som genomför uppdrag för Försvarsmakten.

Oberoende granskning tillämpas generellt då det tekniska systemets olycksrisker är att anse som stora/allvarliga. Se vidare *avsnitt 5.12*.

2.5 Handbok systemsäkerhet

2.5.1 H SystSäk

Syftet med H SystSäk har tidigare redovisats i *avsnitt 1.2*.
H SystSäk omfattar:

- **Beskrivning** av den systemsäkerhetsmetodik som ska användas för att säkerställa att olycksrisker i Försvarsmaktens tekniska system hålls så låga att de innehåller ställda krav under livslängden.
- **Redovisning av aktiviteter** inom systemsäkerhetsmetodiken (krav, beslut, verktyg, metoder och deras inbördes sammanhang) som underlag för organisationers utformning av ansvarsfördelning, organisation, arbetsformer, framtagning av egna stödprocesser och deras anpassning till egna skedesbegrepp – allt i syfte att underlätta framtagning av säkra militära tekniska system.

- **Metodanvisning** avseende Försvarsmaktens systemsäkerhetsmetodik till alla de som medverkar i Försvarsmaktens systemsäkerhetsverksamhet; Försvarsmakten som ägarföreträdare (ÄF), Försvarsmakten som beställare, Försvarsmakten som brukare, Designansvarig (DesignA; sammanfattande benämning på FMV, FORTV, FOI, FRA, FömedC respektive OPS-partner) samt leverantör.

2.5.2 Definitioner

För att definiera systemsäkerhetsmetodiken använder H SystSäk tre grundläggande definitioner:

- **Systemsäkerhet** definieras som egenskapen hos ett tekniskt system att inte oavsiktligt orsaka skada på person, egendom eller yttre miljö. (Person; död, fysisk skada eller ohälsa. 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.)
- **Tekniskt system** definieras i samordningsavtalet *[40]* 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. (Avses annan typ av system måste detta tydligt anges.)

  Ammunition är alltid ett fristående tekniskt system samtidigt som den ofta utgör integrationsprodukt i ett eller flera andra tekniskt system.
- **Systemsäkerhetsverksamhet** är 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 olycksrisker, eliminera dessa eller reducera dem enligt ställda krav.

2.5.3 Tillämpning

H SystSäk tillämpas vid all verksamhet som avser utveckling, produktion, vidmakthållande samt avveckling av tekniska system. Se Förord, Instruktion om Försvarsmaktens handbok systemsäkerhet.

> Att H SystSäk tillämpas innebär inget undantag från skyldigheten att efterleva tillämpliga lagar.

2.5.4 Jämförelse av metodinriktning

Lagar, Försvarsmaktens regelverk med RMM, RML och RMS samt övriga etablerade säkerhetsverksamheter beskrivna ovan i *avsnitt 2.4*, är alla av föreskrivande natur. Framtagna föreskrifter syftar till att undvika skador och kan utgå antingen från ett dimensionerande skadeutfall, eller värsta möjliga skadeutfall (konsekvensbaserad = *deterministisk*). Föreskrifterna kan till exempel ange regler för konstruktion, fördela ansvar samt ställa krav på dels verksamhet och dels systemegenskaper. Metoden syftar till att genom regelefterlevnad uppnå godtagbar säkerhet.

H SystSäk är å andra sidan främst *probabilistisk* (sannolikhetsbaserad) *[27]*. Detta innebär att H SystSäk metodik är inriktad mot att identifiera och åtgärda olycksrisker hos tekniska system.

Olycksrisker i tekniska system kan generellt uppkomma dels som ett resultat av att ny teknik tillämpas som det saknas tidigare erfarenhet av, respektive av att känd teknik används i nya tillämpningar som det saknas tidigare erfarenhet av. (Härutöver kan olycksrisker uppkomma genom brister vid konstruktion och tillverkning, se *H SystSäk del 2, kapitel 2*.)

En logisk följd härav är att det för tillämpad teknik fortlöpande hos DesignA uppstår nya kunskaper om olycksrisker, deras natur och vilka åtgärder som använts för att minska dessa i befintliga system.

DesignA bör säkerställa att sådana erfarenheter återanvänds. Se *avsnitt 3.8*.

2.5.5 Övervägande om regeltillämpning då tekniskt system innehåller flera delsystem

Nedan återges ett belysande exempel på överväganden.

Exempel: Drivmedelsfordon vid marint basförband.

Fråga: Genom vilken säkerhetstillämpning säkerställs tankningsfordonets egenskap att inte vålla oavsiktlig skada på människa, egendom eller yttre miljö under just tankningsförfarandet?

Alternativa svar: Regler för militär sjöfart (RMS) för fartyget, Trafikvärdighet för tankningsfordonet respektive Systemsäkerhetsmetodik.

Korrekt svar: Systemsäkerhetsmetodik.

Överväganden

Trafikvärdighet avser endast fordonets egenskap att kunna uppträda säkert i trafik.

RMS avser Militär sjöfart, örlogsfartyg och dykerisystem. Sjövärdighetsbevis utfärdas för tekniskt system som uppfyller gällande regelverk. Sjövärdighetsbevis omfattar normalt inte de ledningssystem, vapensystem och gränsytor till andra system som kan innebära andra olycksrisker för det tekniska systemet.

Ytterligare ett alternativ skulle kunna vara ADR-regelverket *[1]*. Detta syftar till att farligt gods som transporteras med drivmedelsfordonet inte ska vålla skada på människa, egendom eller yttre miljö på grund av brister i fordonet. Men det förhindrar inte operatörens fall från tanköverredet vid arbete på dess topp (vid till exempel inspektion genom manlucka alternativt för att utföra maskeringsarbete i fält). Sådan olycksrisk upptäcks enbart genom systemsäkerhetsmetodik.

2.6 Verksamhetssäkerhet respektive systemsäkerhet

2.6.1 Grunder

Personer som söker anställning vid Försvarsmakten inser dels att det finns allvarliga faror i arbetet, dels att god säkerhet är extra viktig för Försvarsmakten.

Överbefälhavaren har i sin egenskap av arbetsgivare moraliskt och juridiskt ansvar för sina anställda. Försvarsmakten har också ansvar för andra människor som utsätts för eventuella brister och fel i Försvarsmaktens verksamhet.

Försvarsmakten är kravställare och slutanvändare av alla tekniska system som används i svenska försvaret och påverkar därigenom konstruktion, utveckling, tillverkning och underhåll. Ju säkrare utrustning som Försvarsmakten anskaffar och använder, desto lättare kan Försvarsmakten uppfylla sitt juridiska och moraliska ansvar.

Utöver detta har Försvarsmakten också ett ansenligt ansvar för att fortlöpande säkerställa sin generella kompetens att hantera alla de risker som samhällets uppdrag att bedriva försvarsverksamhet medför.

I företagsvärlden anses ett företags goda namn och rykte vara en stor tillgång som kan skyddas med stöd av systemsäkerhetsverksamhet. Ett företag som förlorar detta konkurreras snabbt ut från marknaden. Försvarsmaktens goda namn och rykte bör kunna betraktas på motsvarande sätt. Försvarsmakten i sin nya roll förväntas på den internationella arenan bjudas in att delta i samfällda militära missioner. Ett fortsatt gott namn och rykte för god förmåga att föra väpnad strid krävs för framtida uppdrag. Jämför också *avsnitt 3.2* vad som skrivs om militär risk. Systemsäkerhetsverksamheten tillsammans med ett gott riskmedvetande kan bidra till detta.

Försvarsmaktens uppgift avseende väpnad strid måste lösas under iakttagande av tillämpliga lagar. Metodiken för detta har utformats till ett internt säkerhetsledningssystem som benämns Försvarsmaktens verksamhetssäkerhet och definieras enligt följande:

> 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, egendom och yttre miljö uppfylls.

Verksamhetssäkerhet inom Försvarsmakten indelas avseende verksamhetsområden i: militär marksäkerhet, militär sjösäkerhet och militär flygsäkerhet.

Försvarsmaktens yttersta uppgift att kunna bedriva effektiv väpnad strid ställer särskilda krav på gott riskmedvetande vid såväl utbildning och övning som vid insats.

Verksamheten inom Försvarsmakten blir alltmer tekniskt avancerad och komplex. Detta förhållande, i kombination med ett ökat internationellt engagemang och samhällets generellt ökade säkerhetskrav, innebär att säkerhetsfrågorna också har fått ändrade och vidgade dimensioner.

Den nivå av verksamhetssäkerhet som upprätthålls är en effekt av det verksamhetssäkerhetsarbete som bedrivs inom Försvarsmakten och andra berörda organisationer som verkar på uppdrag av Försvarsmakten.

Det svenska ordet ”säkerhet” används som översättning för både ”safety” och ”security”. Verksamhetssäkerhet omfattar i denna jämförelse framför allt begreppet ”safety” men det är också uppenbart att eventuella svagheter i den säkerhet som motsvarar begreppet ”security” i sin förlängning kan leda till en lägre verksamhetssäkerhet. Någon skarp gräns mellan ”safety” och ”security” är därför inte meningsfullt att dra inom ramen för verksamhetsäkerhet. En verksamhetsutövare (till exempel en insatschef) behöver fortlöpande förvissa sig om att säkerheten är tillräckligt bra i båda dessa avseenden.

Grunden för effektiv och säker verksamhet är brukarens kunskap om verksamhet och materiel, samt förmåga att tillämpa denna kunskap i praktiska situationer. Realistiska övningar ökar denna kunskap. En öppen attityd och en vilja hos ledningen att ständigt förbättra säkerheten genom att rapportering av avvikelser ses som en naturlig del i verksamheten är en hörnsten i allt verksamhetssäkerhetsarbete.

2.6.2 Omfattning

Verksamhetssäkerhetsarbetet omfattar regelgivning, genomförande av verksamheten enligt dessa regler samt uppföljning av att så sker.

Regelgivning innebär komplettering av lagar, förordningar och andra rättsregler med föreskrifter och interna bestämmelser där så krävs.

Lagar, förordningar och föreskrifter gäller för Försvarsmaktens verksamhet och personal på samma sätt som för samhället i övrigt. Dock finns föreskrifter som uppmärksammar Försvarsmaktens verksamhet och ger Försvarsmakten möjlighet att utforma regler för sådan verksamhet.

Genomförande av verksamhet enligt givna regler innebär att verksamhetssäkerhetsarbetet är en integrerad verksamhet vid genomförandet av uppdrag eller insats. Försvarsmakten kan tilldela chef uppgift att vara central verksamhetsutövare med åtföljande verksamhetssäkerhetsansvar. Detta innebär skyldighet att inom aktuellt ansvarsområde skapa verksamhetssäkerhetssystem som säkrar att givna regler följs och därmed möjliggör att målet, säker verksamhet, uppnås.

Uppföljning av att genomförd verksamhet bedrivs enligt givna regler sker dels genom att kontrollera att verksamhetsutövare uppfyller sin skyldighet att rapportera avvikelser dels genom inspektion, tillsyn och revision.

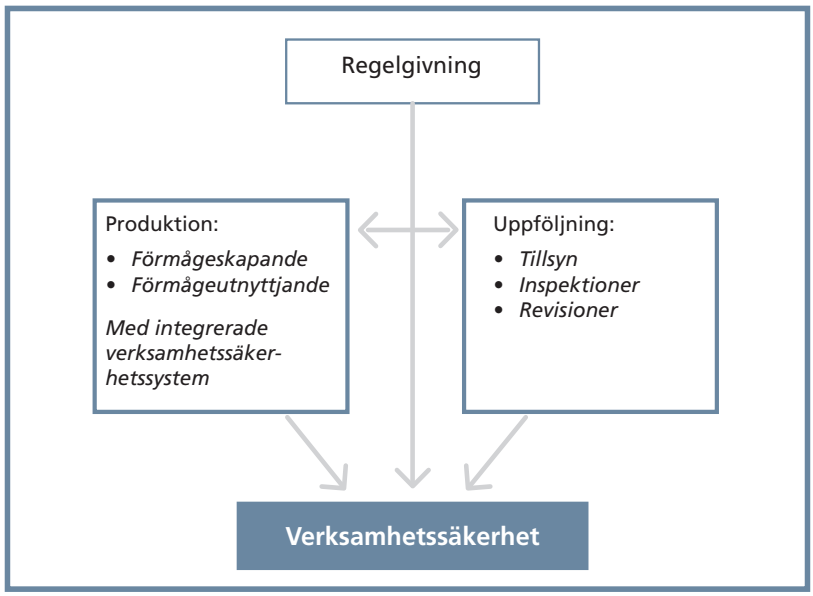


Bild 2:2 Verksamhetssäkerhet skapas genom produktion, regelgivning samt uppföljning

2.6.3 Regelgivning

Försvarsmakten beslutar föreskrifter i form av författningar som kungörs i Försvarets författningssamling (FFS) och i Försvarsmaktens interna bestämmelser (FIB). FFS och FIB beslutas av ÖB eller av honom bemyndigad. FFS används även av Fortifikationsverket, Totalförsvarets forskningsinstitut och Försvarets materielverk. I FIB kungörs enbart Försvarsmaktens interna bestämmelser.

Regelgivning är och kommer alltid att vara en kontinuerlig verksamhet. Ny materiel och nya typer av verksamheter ställer både nya krav och gör gamla krav inaktuella. Allt mer komplexa system ställer också allt högre krav på att person/förband/materiel/system i alla stycken fungerar tillsammans för att både uppnå effekt och ge godtagbar säkerhet.

Regelgivning inom verksamhetssäkerhetsområdet utformas som föreskrift och ges ut i form av instruktioner och regler som till exempel Försvarsmaktens säkerhetsinstruktion för vapen och ammunition med mera (SäkI), Regler för Militär Markverksamhet (RMM), Regler för Militär Sjöfart (RMS) och Regler för Militär Luftfart (RML).

Kunskap om gällande regler är en nödvändig förutsättning för att uppnå god verksamhetssäkerhet.

2.6.4 Uppföljning

I all verksamhet uppkommer oundvikligen avvikelser från planerad verksamhet, från givna regler och från förväntat beteende hos materielen. Sannolikheten för avvikelser ökar ju större påfrestningar som användningssituationen medför. Ju tidigare en avvikelse uppmärksammas och hanteras desto lättare är den att åtgärda och desto mindre blir risken för allvarliga konsekvenser.

Försvarsmakten ska ha ett fungerande verksamhetsledningssystem som innehåller system för att fånga upp, dokumentera och analysera avvikelser samt initiera förbättringsåtgärder. Detta system ska vara väl integrerat i all verksamhet inom Försvarsmakten och ligga till grund för en ständig förbättring av säkerheten.

Verksamhetsledningssystemet kompletteras med oberoende inspektioner, revisioner och tillsyn. Resultatet från denna granskningsverksamhet dokumenteras och integreras i Försvarsmaktens förbättringsverksamhet.

Iakttagelser från tillsyn, inspektioner och revisioner ska användas för framtagning av korrigerande åtgärder.

Uppföljning ska ske av att förbättringsverksamheten ger avsedd effekt.

Försvarsmaktens verksamhetsledningssystem bygger på egenkontroll vilket kan innebära risk för konflikt mellan säkerhets- och produktionskrav.

Den som observerar en avvikelse ska rapportera denna, även om individen själv gjort fel och förorsakat avvikelsen. Rapporten är bra underlag för förbättringsförslag.

En öppen och trygg attityd till alla rapporterade avvikelser är en nödvändig förutsättning för Försvarsmaktens verksamhetssäkerhet.

2.6.5 Verksamhetssäkerhet i ett livslängdsperspektiv

Verksamhetssäkerhetsarbetet börjar då mål formuleras för nytt förband eller nytt tekniskt system. Alternativt inleds det då nya uppgifter formuleras för befintligt förband eller befintligt tekniskt system. Redan i detta tidiga skede måste systemsäkerhetskrav identifieras och krav på risknivå anges. Kraven ställs för avsedd livslängd.

I den fortsatta verksamheten med att sätta upp ett nytt förband och anskaffa ny eller utveckla befintlig materiel måste säkerhetsaspekterna ingå som en integrerad del och fortlöpande bearbetas. Målet är att det nya förbandet med sin nya materiel ska vara säkert under utförande av alla krävda verksamheter, i alla krävda miljöer, och under alla krävda förhållanden. De krävda verksamheterna omfattar normalt alltid utbildning, övning och strid under insats.

2.6.6 Försvarsmaktens systemsäkerhetsverksamhet

I instruktion om Försvarsmaktens handbok systemsäkerhet 2011 *[26]* anges att systemsäkerhet utgör en del i Försvarsmaktens verksamhetssäkerhet.

Försvarsmakten har lång erfarenhet av att hantera olycksrisker i såväl tekniska system som i verksamheter. Historiska data om olyckshändelser visar att Försvarsmaktens åtgärder successivt har lett till lägre olyckstal. Systemsäkerhetsmetodiken möjliggör för Försvarsmakten att vid kravställning avseende nya system överföra dessa erfarenheter för att fortsatt uppnå allt lägre olycksrisker.

Försvarsmakten har infört systemsäkerhetsverksamhet som omfattar metodik för att uppnå och bibehålla god säkerhet hos de tekniska systemen. Systemsäkerhetsmetodiken omfattar verktyg för såväl styrning som genomförande och uppföljning av systemsäkerhetsverksamheten vid Försvarsmaktens produktion avseende tekniska system.

Systemsäkerhetsmetodiken är en generell tankemodell för hur risker identifieras (i ny teknik och i nya tillämpningar av känd teknik). Systemsäkerhetsverksamhet ska alltid vara en integrerad del i ett tekniskt systems utveckling, vidmakthållande och avveckling.

2.7 Försvarsmaktens gemensamma riskhanteringsmodell

Försvarsmaktens gemensamma riskhanteringsmodell *[19]* behandlar de risker som en förbandschef möter under bland annat insats. Dessa risker kommer från såväl antagonistiska som icke antagonistiska hot riktade mot ett förbands skyddsvärda tillgångar (till exempel personalens liv och hälsa, operationell förmåga). Det engelska ordet som används i detta sammanhang är security. Riskhanteringsmodellen syftar till att underlätta förbandschefs beslut i fält om medveten risktagning och insats av skyddsåtgärder i samband med att stridshandling planeras/kan förekomma.

Denna beskrivning av Försvarsmaktens gemensamma riskhanteringsmodell görs dels som allmän information, dels för att visa att det endast finns perifera kopplingar till H SystSäk som ju enbart hanterar olycksrisker (inte antagonistiska hot, security) kopplade till tekniskt systems egenskaper.

3 Risk

3.1 Grunder

Riskhantering är en generell teknik som används inom många olika områden (jämför *avsnitt 2.1*). Texten i detta avsnitt är till vissa delar hämtad från An Introduction to System Safety Management and Assurance *[3]*.

Under utveckling är strävan att identifiera systemets samtliga risker. I den internationella systemsäkerhetsvärlden råder idag stor enighet om att endast cirka 50% av alla risker hittas under utveckling och tillverkning. Det inses därmed att sannolikheten är stor för att resterande risker kommer att göra sig påminda under systemets användning. Systemsäkerhetsmetodiken behöver därför innehålla verktyg för riskhantering med såväl proaktiv som reaktiv inriktning. Med proaktiv riskhantering avses att identifiera och hantera risker i förväg. Reaktiv riskhantering genomförs (”på förekommen anledning”) när en olycka eller tillbud har inträffat. Syftet är i båda fallen att utreda och åtgärda orsaker, identifiera vad som utgör riskens grund och att genom lämpliga åtgärder försöka förhindra en olycka.

Risk och riskhantering beskrivs med hjälp av vissa termer, som även om de ingår i normalt språkbruk, ändå här används i specifik betydelse. Exempel på sådana termer är fara, riskkälla, farligt tillstånd, risk, tillbud och olycka. Syftet med kapitlet är att göra läsaren bekant med metodikens grundläggande språkbruk.

Den funktionella säkerheten hos systemet avser tillgång till den förmåga/funktion eller tillgång till tjänst som systemet ska tillhandahålla. Förmågan att så ofta som krävs, utföra avsedd funktion benämns **tillförlitlighet** och behandlas inte vidare här. Det är dock att märka att tillförlitlighet i vissa militära situationer kan utgöra en livsavgörande förutsättning. Till exempel så hävdar engelska förbandschefer med stridserfarenhet från de båda Gulfkrigen, att när förbandet har skjutit första skottet, så har förbandet röjt sin närvaro och sin position. Tillförlitligheten hos verkan i målet, presterad av vapen och ammunition, är därför av vital betydelse (det vill säga direkt säkerhetskritisk).

Olycksrisk avser risk för skada på människa, egendom och/eller yttre miljö.

Olycksrisk kan ofta leda till andra typer av risker, en olycka kan påverka försäkrings- och affärsrisk.

Ordet risk kan användas i så många olika sammanhang att det är en god idé att använda ordet ”olycksrisk” om missförstånd kan befaras.

Begreppet risk bygger på antagandet att fullständig säkerhet inte är uppnåelig. Riskhantering innebär bland annat att jämföra olika säkerhetsbrister, värderade efter hur allvarliga de är och prioritera vilka risker som bedöms nödvändiga att reducera. Riskhantering kan utföras för alla typer av risker.

Även om det inte gör någon skillnad för den enskilde förolyckade individen, om han förolyckats ensam eller tillsammans med 100 andra, så är det väsentligt att vid riskanalys identifiera hur många personer som utsätts för en viss olycksrisk.

Denna inriktning har lett till följande två begrepp:

- **Individuell risk** definieras som frekvensen som en individ kan förväntas att utsättas för av en given nivå av skada, orsakad av specificerade faror. Den är vanligtvis beräknad för en genomsnittsperson i gruppen.
- **Samhällsrisk** definieras som relationen mellan frekvens och antalet människor som drabbas av en specificerad nivå av skada i en given folkmängd som exponeras för specificerad risk. Den uttrycker därvid hur många människor som kan komma att omfattas av en olycka.

3.2 Militär olycksrisk

Militär olycksrisk *[3]* definieras här som risk för skada under militär verksamhet som förorsakas av brister i materielens utförande och funktion. Särskilt avgörande är den fördel fienden kan få i en stridssituation av sådan brist.

Bakgrunden till att denna specifika risk har identifierats är bland annat att det under Gulfkriget samt andra nyligen inträffade konflikter har orsakats fler skador av olyckor än av fientliga handlingar. Säkra tekniska system, bra anvisningar för hur dessa ska användas samt en säker verksamhetsmiljö, är viktiga bidragande faktorer för möjligheten att kunna upprätthålla militär förmåga.

Att soldaten har förtroende för sin materiel är av vital betydelse för ett förbands slagkraft. Det är därför minst lika viktigt med hög systemsäkerhet hos tekniska system som används i strid, som hos tekniska system som används i fredstida utbildning. Systemsäkerhetsverksamhet ska ge förbandschef tekniska system som är effektiva (och säkra) för avsedd militär användning och därigenom möjliggöra för förbandet att genomföra stridsinsatser utan (onödiga!) förluster förorsakade av brister i eget tekniskt system. Jämför också ovan *avsnitt 2.3* om militära olyckors demoraliserande effekt.

3.3 Vapeninsats mot eget system

Systemsäkerhetsverksamhet omfattar normalt inte risker för fientlig vapenverkan mot eget system, personal eller yttre miljö. Värdering av risker för fientlig upptäckt, vapeninsats, vapenverkan och följdskador ska beredas som en del av kravanalys och kravuppfyllnad med avseende på prestanda såsom systemeffekt, stridseffekt och skyddsförmåga. Målsättningar och krav framgår av TTEM och specifikationer, jämför *avsnitt 6.5*.

Vid tveksamheter ska DesignA tillsammans med HKV (ÄF) klarlägga vilka risker som ska analyseras. Tveksamma fall kan t ex vara ammunitionsröjning i fred (övningsröjning av utländsk skarp minammunition), bogsering av skjutmål (målgång) och deltagande i internationella insatser. Ska risker från vapenverkan analyseras krävs noggrann specificering av vilka vapensystem som avses och vilka prestanda hos dessa som ska antas/ansättas.

Olycksrisker förorsakade av egna vapen ska dock alltid analyseras som en del av systemsäkerhetsverksamheten. Vådaskjutning med egna vapen, behov av riktningsbegränsningar för att omöjliggöra beskjutning av egen plattform, flammor vid robotskjutning, bakblås hos rekylfria pansarvärnsvapen, ammunitionssäkerhet och så vidare ska alltid omfattas av den systemsäkerhetsverksamhet som genomförs för ett nytt eller modifierat tekniskt system.

3.4 Samband mellan säkerhet och risk

Försvarsmakten definierar säkerhet som frihet från oavsiktlig skada på person, egendom och/eller yttre miljö. En oavsiktlig skada kan vara såväl omedelbar (till exempel ett nedkört staket eller en bruten arm) som en skada som tar lång tid att utveckla (till exempel ohälsa/cellförändring orsakad av högfrekvent strålning, ohälsa/hörselnedsättning orsakad av buller, ohälsa/belastningsskada orsakad av felaktig arbetsställning eller utrotning av viss djurart orsakad av giftiga utsläpp).

3.5 Olycksrisk

Begreppet risk är centralt för systemsäkerhet. Risk uttrycker en kombination av allvarlighet hos skadan, ohälsan, belastingsskadan (konsekvensen det vill säga hur illa det kan gå) och sannolikheten för (hur ofta) en händelse/olycka med just denna konsekvens bedöms kunna inträffa.

Varje enskild risk utgår från en fara. Fara förorsakas endera av en riskkälla eller ett farligt tillstånd.

Riskkälla är en företeelse som för stunden inte skadar, men har potential att göra det, givet sådana förutsättningar att en vådahändelse kan utlösas (till exempel arsenik i en glasflaska som går sönder vid ett fall mot golvet).

Ett farligt tillstånd kännetecknas av att dess farlighet är direkt närvarande utan villkor (till exempel en oskyddad roterande kapklinga).

En skadehändelse eller olycka förorsakad av dessa faror kan dock inte uppstå om inte också någon eller något exponeras för farans effekter.

Även en långsamt verkande fara påverkar och skadar endast under den tid då till exempel en person är exponerad för faran. Tidpunkten för när skadeverkan faktiskt visar sig är beroende av koncentrationen av det farliga eller graden av dålig ergonomi samt personens motståndskraft mot det giftiga eller den dåliga ergonomin. Exempel på långsamt verkande förlopp kan till exempel vara ohälsa utvecklad på grund av tobaksrökning (jämför *tabell 2:1* som visar att sannolikheten att drabbas av lungcancer och dö för en person som röker 20 cigaretter per dag, är en per tvåhundra rökare och år). Ett annat exempel är belastningsskada som efter lång tid visar sig hos en soldat som kört stridsfordon med för låg takhöjd i förhållande till påtagen stridsutrustning.

Ibland används uttrycken olycksrisk eller risk för sjukdom/ohälsa för att öka tydligheten i aktuellt sammanhang.

Risk relaterar därför både till olycka (akut händelse där skada uppstår) och till ett mer långsamt verkande förlopp med skadekonsekvens, betingad ohälsa.

I H SystSäk kommer fortsättningsvis ordet risk att avse just olycksrisk. Oftast används också ordet olycksrisk. Detta för att tydligt markera vilken typ av risk som avses.

3.6 Riskmodell

En generell riskmodell har tagits fram för att underlätta förståelsen (hos exempelvis konstruktörer) för det tekniska systemets olika olycksrisker, deras ursprung, deras olika möjliga händelseförlopp samt exponeringens betydelse för om en olycka alls ska kunna uppstå.

Riskmodellen används lämpligen vid riskanalys för att möjliggöra identifiering av om olycksrisken förorsakas av en riskkälla (som kräver visst händelseförlopp för att utlösa en vådahändelse) eller om olycksrisken förorsakas av ett farligt tillstånd. I båda fallen krävs att förutsättningarna för eventuell exponering identifieras, för att olycksrisken helt ska kunna uppskattas.

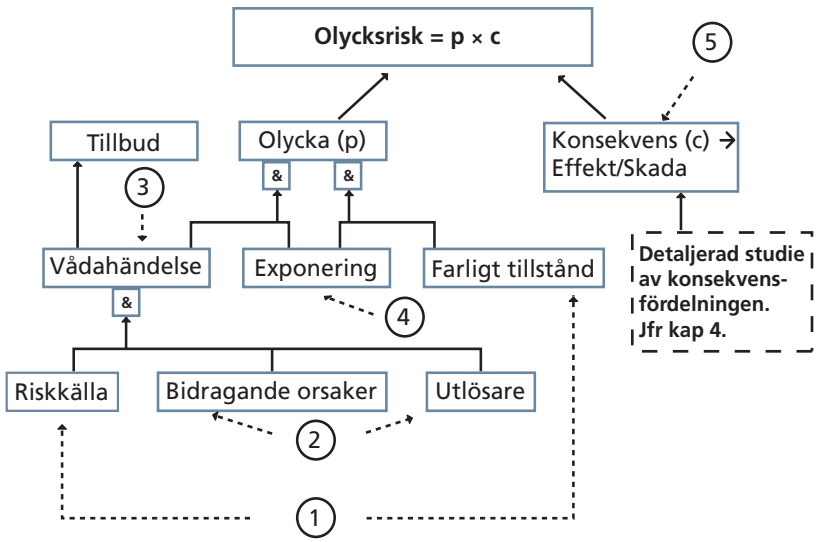


Bild 3:1 Riskmodell

Kommentarer till bild 3:1.

Modellens båda begrepp **riskkälla** och **farligt tillstånd** är något överlappande och inte alltid varandra helt uteslutande. Det finns inget behov av att skapa en entydig klassificering. Dock behövs båda begreppen för att underlätta för riskanalytiker att identifiera och beskriva faror i ett visst system. Modellen gör heller inte anspråk på att direkt täcka in varje möjlig risksituation.

Ibland kan således en riskkälla som kan utlösas ofta ses som ett farligt tillstånd.

Ett farligt tillstånd som försetts med en barriär kan å andra sidan uppfattas som en riskkälla där fel hos barriären får formen av utlösande faktor.

Riskmodellen i *bild 3:1* utgör stöd för tanken vid riskhantering. Under identifiering av olycksrisker ställs lämpligen nedanstående numrerade frågor. Frågornas nummer och sammanhang framgår också av bilden.

1. Centralt för att en olycksrisk ska kunna uppkomma, är att det finns antingen en riskkälla eller ett farligt tillstånd (=fara). Här ställs frågan ”Vari består faran?”
2. Riskkällan kan utlösas och orsaka en vådahändelse. Utlösningen av riskkällan kan ske genom någon företeelse i användningssätt eller användningsmiljö. Här ställs frågan ”Vilket är användningssättet och hur ser användningsmiljön ut? Finns något där som kan utlösa aktuell riskkälla?”
3. Vådahändelse kan identifieras genom att utgående från viss riskkälla ställa frågan: ”Vad får inte hända?” För att svara på frågan måste alla möjliga händelsevarianter identifieras.

   Notera att när en vådahändelse inträffar, så leder denna inte alltid till olycka. När en vådahändelse inträffar utan att någon/någonting exponeras, så uppstår ”enbart” ett tillbud.
4. En olycka inträffar om någon/någonting exponeras för vådahändelsen. För att hitta det exponerade så ställs frågan ”Vem/vad exponeras”. (Därmed inte sagt något om det faktiska utfallet av olyckan, det kan variera från mycket litet till katastrof.)

   Faran kan också utgöras av ett ”farligt tillstånd”. Ett farligt tillstånd kännetecknas av att det alltid existerar (förutsatt att det tekniska systemet är i drift respektive uppträder på aktuell plats) och därmed har sin farliga egenskap fullt utvecklad.

   En kraftledning behåller ständigt sin farlighet även om dess ledningstråd är nedfallen, och den är farlig ända till dess att strömmen aktivt stängts av. Stjärtrotorn på en helikopter är alltid farlig när helikoptern är i drift. Personer kan exponeras för dess farlighet när helikoptern ”uppträder” på marknivå.

   Om någon eller något exponeras för ett farligt tillstånd inträffar en olycka med viss konsekvens.
5. En olyckas konsekvens kan bedömas genom att följa metodiken i *bilaga 1, Riskuppskattning*, för respektive personrisk, ekonomisk risk och risk för skada på yttre miljö.

En **olycka** definieras som en händelse där någon person, någon materiel eller någon del av den yttre miljön exponeras för vådahändelsen eller farligt tillstånd och det uppstår en skada. Skadans karaktär kan vara omedelbart verkande, till exempel benbrott, eller den kan verka långsiktigt och till exempel vålla ohälsa som tar decennier att utveckla. En olycka är alltid oplanerad och inte resultat av till exempel fientlig handling.

Ett **tillbud** definieras som en vådahändelse där ingen person, ingen materiel/egendom eller någon del av den yttre miljön exponeras för vådahändelsen. Det förekommer vanligtvis många fler tillbud än det inträffar olyckor. Från båda händelsetyperna kan värdefull information erhållas för att förbättra säkerheten genom att minska antalet möjliga vådahändelser eller begränsa/reglera riskfylld exponering.

> Den fulla innebörden av begreppet tillbud i handboken är mer specifikt än vad som normalt förekommer i allmänt språkbruk. Så till exempel står det engelska uttrycket **Near misses** för en typ av olyckor där det ofta bara beror på slumpen att det inte har uppstått allvarligare konsekvenser. Detta uttryck gör alltså ingen skillnad på olycka med nollkonsekvens och tillbud (vådahändelse utan exponering).

Skador av utsläpp av farliga ämnen, inom tillåtna gränsvärden, är inte att se som systemsäkerhetsproblem.

Sannolikhet för olycka förorsakad av en riskkälla, består av sannolikhet för vådahändelse kombinerad (multiplicerad) med sannolikhet för exponering. Detta faktum är ofta missförstått varför det ibland inträffar att det sannolikhetstal som anges för en viss olycksrisk egentligen endast avser vådahändelsen och inte olyckan. Detta sätt att hantera sannolikheter leder fram till ett för högt värde på bedömd olycksrisk.

Sammanhangen mellan de olika delar som kan leda till olycka är ganska komplexa. Därför behöver handbokens metodik för riskhantering användas. Den bygger på att först hitta systemets faror. Därnäst identifieras vad respektive fara inte får förorsaka (= vådahändelse). Därefter identifieras användningssätt och användningsmiljö och i dessa, farans alla förutsättningsskapande händelser och eventuell nödvändig utlösande faktor. För att identifiera möjliga olyckor ska också alla de skyddsföremål (människa, egendom och yttre miljö) identifieras, vilka kan komma att exponeras för effekten från möjliga vådahändelser.

3.7 Risktyper på olika systemnivåer

Faror (riskkällor och farliga tillstånd) är i jämförelse med varandra mycket olika. Olikheterna förekommer inom ett brett spektrum av fysikaliska områden. Ofta är systemnivå avgörande för vilka faror som alls kan förekomma och därmed utgöra hot. Begreppet systemnivå kan utgöra en lämplig grund, då ett tekniskt systems olycksrisker avses identifieras. *Bild 3:2* syftar till att visa kopplingen mellan systemnivå och typ, för flertalet olycksrisker som kan förekomma på angiven nivå av tekniskt system.

En närmare beskrivning av de olika risktyperna finns i *avsnitt 4.2.2*.

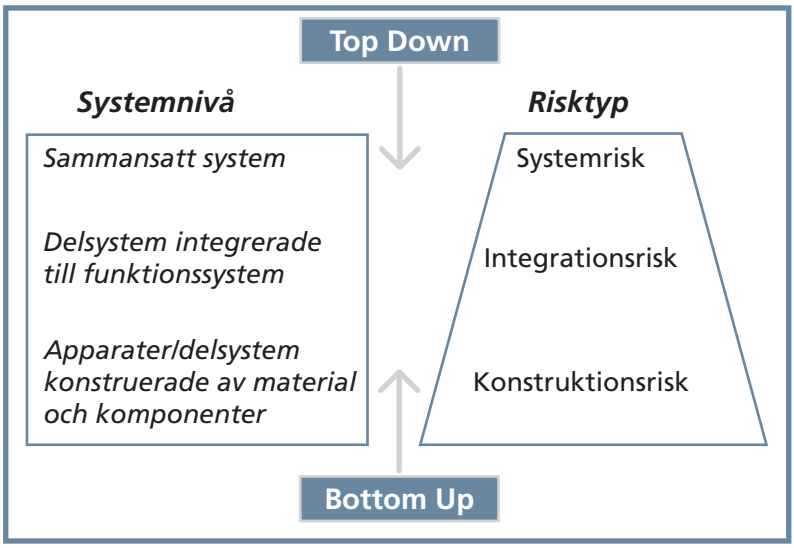


Bild 3:2 Risktyper på olika systemnivåer

3.7.1 Nivå – Apparater, delsystem

På lägsta systemnivå är farorna av mycket basal och grundläggande natur.

- Riskkällor kan utgöras av farligt ämne (exempelvis giftigt, explosivt, brännbart, oxiderande) eller farlig fysikalisk effekt (elektrisk spänning), mekanisk farlighet (vassa kanter, roterande delar) eller något annat på lägsta tekniska nivå.
- Farligt tillstånd kan bestå av en spänd fjäder, en laddad kondensator, att en person befinner sig på hög höjd eller något annat direkt hotande.

Också viss apparat/komponent kan avge fysikalisk farlighet såsom hög effekt av elektromagnetisk strålning (radar, laser) respektive akustisk energi (hörbart ljud) eller impulsljud (från skjutvapen), och kan därvid utgöra riskkälla.

3.7.2 Nivå – Delsystem integrerade till funktionssystem

På en något högre systemnivå där apparater/delsystem kopplas ihop kan farliga tillstånd uppstå som en följd av integrationen och medföra olycksrisker. Exempel på scenarier är vapen som laddas, radarstation som startar sändning, lasermätare som startar sändning, helikopter som startar sina rotorer, fartyg som startar sina propellrar. När sådana händelser startar oavsiktligt, eller vid fel tillfälle och med personal exponerad, så uppkommer oavsiktliga olycksrisker.

3.7.3 Nivå – Sammansatta system

På den högre systemnivån där sammansatta system har getts viss förmåga, till exempel verkan, finns oftast någon form av kontroll- eller ledningssystem som ska rikta verkan mot rätt mål. Sådant ledningssystem kan vara lokalt eller så kan ledning/styrning utföras från visst avstånd (fjärrstyrning). I båda fallen kan styrningen upphöra att fungera. Den lokala styrningen kan störas av till exempel kortslutning i styrkrets, roderlinor som går av, joystick som mekaniskt eller elektriskt havererar. Fjärrstyrning kan fallera på grund av kabel som går av, kortslutning i styrkretsar eller att radiokontroll störs ut eller på annat sätt sätts ur funktion. Därigenom kan ett fullt fungerande vapensystem komma att okontrollerat sätta in sin verkan mot ett oavsiktligt mål och därvid utsätta alla och envar inom verkansområdet för dödlig fara.

3.8 Designregler

3.8.1 DesignA:s designregler

Vid uppföljning av inträffade olyckor och avvikelser, uppstår normalt hos DesignA ny kunskap om tekniska systems riskinnehåll och riskegenskaper (jämför *avsnitt 3.9.4*). Det är angeläget att information om avvikelser, olycksrisker och vidtagna riskreducerande åtgärder kommer till DesignA:s kännedom.

Det är ett grundläggande ansvar för DesignA att fortlöpande sammanställa och dokumentera vunna kunskaper om olycksrisker i tekniska system. Också kunskap som framkommit genom omvärldsanalys, nya standarder med mera tas in i denna dokumentation.

Under bruk av tekniskt system tar DesignA fortlöpande fram konstruktionsändringar för att minska identifierade risker. Konstruktionsändring som skulle kunna tillämpas för att undvika den upptäckta olycksrisken vid en framtida tillämpning av motsvarande teknik omformas till ett generellt konstruktionskrav (designregel). Också dessa designregler läggs löpande till vunna erfarenheter.

Exempel på befintliga regelsamlingar är RMM (Regler för militär markverksamhet) *[35]*, RMS (Regler för militär sjöfart, framtagen av Försvarsmakten *[36]*), RML (Regler för militär luftfart, framtagen av Försvarsmakten *[34]*), H VAS (FMV Handbok Vapen- och Ammunitionssäkerhet *[11]*), H FordonSäk (FMV Handbok Fordonssäkerhet *[10]*), Försvarsmakten och FMV respektive handböcker om Elsäkerhet *[30]* och H Progsäk (Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar *[20]*).

Bakgrunden till att dessa har tagits fram är att aktuella tekniska system är särskilt farliga, och att sedan tidigare ett stort antal farliga tillstånd samt riskkällor och deras möjliga vådahändelser samt möjliga olyckshändelser är kända. I flera fall har faktiska olyckor inträffat.

Designregler anger hur kända olycksrisker kan neutraliseras/undvikas genom viss konstruktion eller krav på principer för sådan konstruktion. Syftet med ett designregelverk är att för beprövad teknik ange lämpligt sätt att genom konstruktion eller krav på konstruktionens egenskaper, förebygga/reducera effekten av kända olycksrisker.

Vid genomgång/uppföljning av konstruktionsarbete används designregelsamlingar som checklistor för att stödja arbetet med att identifiera förekommande olycksrisker.

3.8.2 Försvarsmaktens designregler

I *avsnitt 2.4.1* har under rubriken Militärt undantag från gränsvärden med mera i Arbetsmiljöverkets föreskrifter, konstaterats behov av att Försvarsmakten låter ta fram egna tillämpningsanvisningar med riktlinjer, gränsvärden med mera som Försvarsmakten definierar som tolerabel för svensk militär personal. För det fall att sådana gränsvärden inte har tagits fram, hanteras frågan istället som risk för viss skadeverkan och värderas med aktuellt tekniskt systems riskmatris.

Framtagna och accepterade gränsvärden för militära tekniska system avseende olika typer av belastningar från buller, vibration, impulsljud med mera medför ofta en effektivare materielframtagning än att via riskhantering under konstruktion påvisa behov av riskreducerande åtgärd.

3.9 Riskmedvetande

3.9.1 Definition

Försvarsmakten är beroende av tekniska system som har avsedd effekt i strid. Med nödvändighet måste Försvarsmakten acceptera en viss risktagning för att få tillgång till denna stridseffekt. Medveten risktagning är därför en del av Försvarsmaktens normala verksamhet, inte minst under strid. Dock avses inte en generell vårdslöshet med risker, utan istället en av chef beslutad risktagning efter noggrant övervägande. Förfarandet kräver att varje risk ska vara känd och hanterad, och att risker i verksamheten fortlöpande ska beaktas.

Organisationen med sina medarbetare ska hela tiden sträva efter så bra säkerhet som möjligt genom att bearbeta riskerna. En parallell dras med fördel till det civila samhällets begrepp ”Säkerhetskultur” som definieras som ”den samling av egenskaper och attityder i organisationer och hos individer som säkerställer att säkerhetsfrågor får den uppmärksamhet som behövs” (IAEA, International Atomic Energy Agency).

Systemsäkerhetsverksamhet är en angelägenhet också för Försvarsmaktens organisation och personal, och behöver fungera kontinuerligt vid ordinarie verksamhet. Strävan måste vara att fortlöpande hitta de tekniska systemens och verksamhetens olycksrisker.

Ett gott riskmedvetande med nödvändig stimulans från revisioner, avvikelserapporter, förbättringsförslag och positiv uppmärksamhet av de individer som engagerar sig i verksamheten, är en förutsättning för att verkligen hitta alla olycksrisker.

Ett gott riskmedvetande existerar när alla inser och accepterar sitt ansvar för riskhantering och organisationens hantering av systemsäkerhetsrisker är en självklar del av ordinarie verksamhet.

Ett gott riskmedvetande utmärks av berörd personals positiva engagemang och delaktighet. Endast genom ett gott riskmedvetande finns förutsättningar att få reda på och effektivt kunna ta hand om de olycksrisker som ännu inte är upptäckta respektive de olycksrisker som uppstår under materielens livslängd.

3.9.2 Fördelning av ansvar mellan organisation och individ

För att gott riskmedvetande ska utvecklas krävs en atmosfär i vilken individer inte straffas eller anklagas för sina oavsiktliga misstag. System ska vara robusta och klara felhantering. Om ett systemfel identifieras, så bör detta ses som en fördel, för då går det att rätta till felet innan en olycka inträffar (i en stridssituation skulle felet dessutom kunna försvaga vår styrka och kanske leda till förluster).

Detta är det ideala tillståndet som kan vara svårt att uppnå i praktiken. När någon person förorsakat en avvikelse så är det nämligen en vanlig mänsklig reaktion att skylla ifrån sig eller att försöka skylla på andra, istället för att bara på enklaste sätt uppriktigt och ärligt redovisa vad som inträffat. Särskilt en organisation som verkar med komplex materiel med stora risker, måste ta hänsyn till denna kunskap om den mänskliga naturen och förbereda sig på att praktiskt hantera denna typ av (systemmässiga) avvikelser. En sådan pragmatisk anpassning är nödvändig eftersom tillbudsinformation är livsviktig för att förhindra framtida fel.

Försvarsmakten styrs av regler och föreskrifter. En individ som är skyldig till allvarlig och medveten försummelse bör naturligtvis inte gå fri från sitt ansvar. Försvarsmakten strävar att uppnå en rättvis kultur där ärlighet och uppriktighet premieras. Detta innebär att omedvetna misstag och felgrepp ska kunna rapporteras som avvikelser utan risk för bestraffning. En sådan attityd finns idag inom Försvarsmaktens flygtjänst, där en positiv avvikelsehantering har bidragit till att riskreducerande åtgärder har kunnat genomföras. Fel och misstag är oundvikliga och säkerhet kan endast förbättras om organisationen kan lära sig av sina misstag, vilket kräver tillgång till denna typ av information om brister i säkerheten.

Materielfel eller felaktiga instruktioner kan medföra olycksrisk. Rapportering av alla typer av avvikelser är av vital betydelse för att uppnå och kunna vidmakthålla en god säkerhet och måste därför uppmuntras. Disciplinära åtgärder eller hot om sådana, äventyrar allvarligt viljan att rapportera.

Människans roll i ett tekniskt system är inte okomplicerad och måste därför ständigt beaktas under ett systems livslängd.
Se *H SystSäk del 2, avsnitt 5.17, Operating and Support Hazard Analysis (O&SHA) – Task 206*.

3.9.3 Rapportering av avvikelser

Ett grundelement för att skapa och vidmakthålla ett gott riskmedvetande är att studera hur säker materielen och verksamheten faktiskt är. Detta kan göras genom att följa upp drifttidsuttag, underhållsrapporter, avvikelserapporter avseende iakttagelser, tillbud och olyckor samt dra slutsatser från den totala informationen. Härigenom kan risker och faror identifieras samt kan erforderliga riskreducerande åtgärder tas fram, verifieras, valideras och införas. Detta är i korthet en beskrivning av systemsäkerhetsverksamheten under vidmakthållandefasen. Endast genom dessa aktiva systemsäkerhetsåtgärder kan ställda krav på risknivå fortlöpande innehållas.

Studier av verksamheten vid en rad företag har visat att de flesta vådahändelser inte resulterar i olyckor utan endast i tillbud. Men ofta var det endast slumpen som gjorde att det inte blev en olycka eftersom ingen person eller annat skyddsvärt exponerades för vådahändelsen. Jämför grundprincipen för en olyckas uppkomst enligt riskmodellen i *bild 3:1*.

Flertalet vådahändelser är till sin natur högst triviala; till exempel en brusten skruv, en trasig rem, ett punkterat däck, vilka inte i något fall upplevs som särskilt allvarligt.

Det hela upplevs i stället som bristande kvalitet, låg tillförlitlighet och inte egentligen som en säkerhetsbrist. Trots det har merparten av vådahändelserna potential att leda till allvarlig skada = olycka. Flertalet olycksrisker förblir dock oupptäckta. Trots att många av dem har visat sig som någon form av kvalitetsbrist som varit så liten att ingen kommit sig för att rapportera. Bara en försvinnande liten del förorsakar avvikelser som uppfattas som säkerhetskritiska.

Av detta inses att den största kunskapsbanken till stöd för att förhindra nya olyckor består i de närvarande personernas kunskap om inträffade avvikelser.

Endast ett fåtal risker leder till allvarliga olyckor. Därför skulle endast en försvinnande liten del av nödvändig kunskap om systembrister kunna hittas genom att enbart utreda redan inträffade olyckor.

Alla tillbud och olyckor innehåller viktig information om det tekniska systemets kvarvarande olycksrisker. Alla olycksrisker har potentialen att vara säkerhetskritiska och ska därför rapporteras som avvikelser, oavsett om olycka har inträffat eller inte.

Tillgången till *information om viss olycksrisk, där olycka inte har inträffat*, bör ses som ”*kostnadsfri information*”, det vill säga aktuell kunskap har erhållits utan kostnaden av en olycka.

Informationen har dessutom egenskapen att utgöra ”färskvara” med ”bäst-före-datum”. Detta innebär att informationen endast kan användas för avsett ändamål om den rapporteras och hinner användas för riskhantering, innan en olycka/ny olycka inträffar.

Förmåga att effektivt omhänderta information om avvikelser kräver tillgång till ett rapporterings- och utsökningssystem som underlättar hantering av dessa och möjliggör framtagning av konstruktiva, riskreducerande åtgärder.

Ett sådant system syftande till riskreducering kräver minst följande:

- Avvikelser (iakttagelser, tillbud, olyckor samt övriga kunskaper om existerande felaktigheter i materiel/system, med mera) rapporteras.
- Det är lätt för alla att rapportera och registrera den nödvändiga informationen (vad, var, när, vem).
- Erfaren personal utreder avvikelsen (hur och varför det hände).
- Orsaker, både direkta och indirekta identifieras effektivt.

- Där det är möjligt tas förslag fram om korrigerande åtgärder, för att minska risken för en upprepning av avvikelsen (till exempel ändrad konstruktion, ytterligare eller ändrad instruktion, utbildning, skyddsåtgärder).
- Det finns uppföljning för att kontrollera att förbättringarna har fungerat eller om liknande avvikelser har inträffat igen.
- Återmatning till den som lämnat rapporten och till övriga användare av materielen sker snarast.

3.9.4 Avvikelseundersökning

För att undersökning av avvikelser ska kunna fungera på ett effektivt sätt ska ständigt finnas någon funktion med ansvar för att omhänderta avvikelserapporter från användning med mera av tekniska system. Inkommen och hopsamlad information analyseras i syfte att identifiera bakomliggande orsaker. Huvudsyftet är alltid att ta fram korrigerande åtgärder så att risker elimineras och olyckor förhindras.

Orsakssamband är ofta komplexa och omfattar såväl materielens konstruktion, hur materielen har använts, personalens utbildning, vilket riskmedvetande som råder vid aktuell enhet samt organisationens förmåga att skapa och vidmakthålla en till organisationens verksamhet anpassat riskmedvetande.

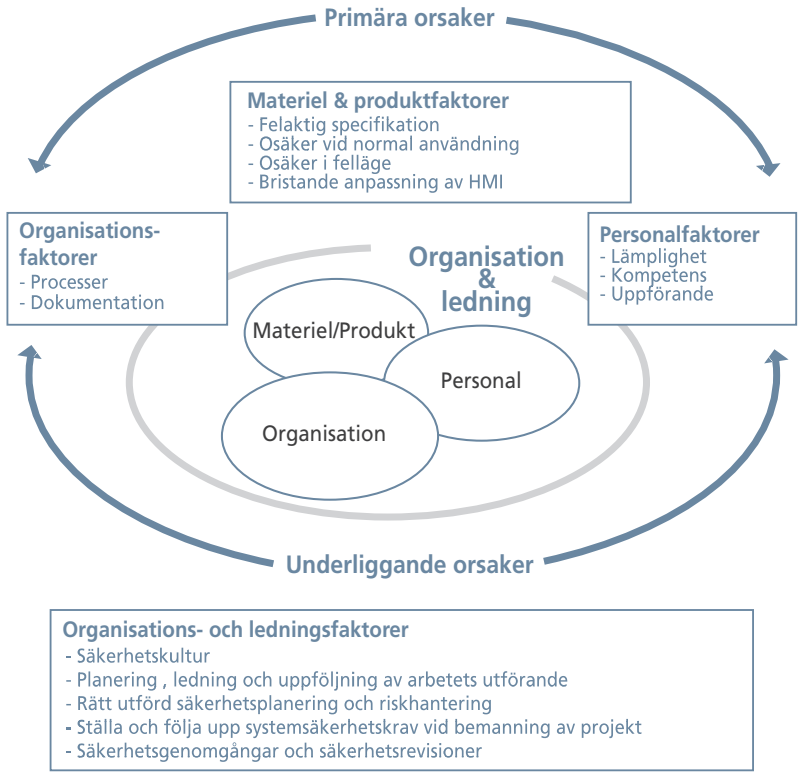


Bild 3:3 Direkta och indirekta orsaker till avvikelser

Sammanhangen mellan direkta och indirekta orsaker visas översiktligt i *bild 3:3* ovan. Bilden visar bland annat att alla funktioner som omnämns i bilden kan ha en påverkan på uppkomsten av rapporterad avvikelse. Därför är det väsentligt att den utredning som ska föreslå korrigerande åtgärder också är öppen för att föreslå åtgärder inom alla de områden som kan ha del i orsaken till inträffad avvikelse (samverkande primärorsaker respektive samverkande underliggande faktorer).

Målsättning med undersökning av en avvikelse; iakttagelse, tillbud eller olycka, är att klarlägga fakta om avvikelsen, inte att fastställa skuld eller ansvarsfrågor. Fakta ska efter analys med slutsatser ge underlag till rekommendationer i avsikt att genomföra korrigerande åtgärder och därmed förebygga olyckor.

Vid Försvarsmaktens HKV bör finnas utpekat kompetenta resurser med uppgift att organisera, leda och följa upp avvikelsehanteringen. HKV bör ge ut regler och rutiner för avvikelserapportering och uppföljning.

Vid avvikelser genomförs en avvikelseundersökning av antingen externa aktörer eller Försvarsmakten. Externa aktörer som kan genomföra en undersökning vid avvikelser inom Försvarsmakten är (tillsynsmyndighet/tillsynsområde): Arbetsmiljöverket/arbetsmiljölagen, Elsäkerhetsverket/ellagen, Polismyndigheten/lag om transport farligt gods, Myndigheten för samhällsskydd och beredskap/lag om brandfarliga och explosiva varor, Strålsäkerhetsmyndigheten/strålskyddslagen och Statens Haverikommission, SHK/lag om undersökning av olyckor.

Försvarsmaktens undersökning genomförs i tre olika nivåer: förbandet/kontingenten, central verksamhetsutövare respektive FMUK (Försvarsmaktens undersökningskommission).

Förbandsnivå – En undersökning efter inträffad avvikelse ska normalt genomföras av förbandet där avvikelsen inträffat.

Central verksamhetsutövare *[18]* – En undersökning av avvikelse som inneburit eller bedöms kunna leda till allvarlig skada eller haveri ska normalt hänskjutas till central verksamhetsutövare. C PROD kan i samverkan med berörd central verksamhetsutövare vid särskilda tillfällen delta i eller själv leda undersökningar som normalt genomförs av ett förband.

FMUK – FMUK är en självständig undersökningsgrupp som har uppgift att undersöka en olycka eller ett tillbud som SHK undersöker. C SÄKINSP beslutar i varje enskilt fall om tillsättande av FMUK. Central verksamhetsutövare och Personaldirektören kan till C SÄKINSP begära att en undersökning genomförs av FMUK.

3.9.5 Ständiga förbättringar

En naturlig del i ett gott riskmedvetande är att aktivt arbeta med ständiga förbättringar. Mängden risk i ett tekniskt system är inte statisk utan ökar ofta med tiden, dels på grund av att materielen slits, underhålls felaktigt eller bristfälligt med mera och att därigenom nya risker kan uppstå, dels på grund av att såväl människor som organisationer blir mindre vaksamma och kanske självbelåtna eller hemmablinda, särskilt om det inte har varit några olyckor under en längre tidsperiod. Vaksamhet, uppföljning och återkoppling krävs därför kontinuerligt för att fortlöpande innehålla ställda krav på risknivå.

Det finns flera metoder för att minska systemets risker. Nedanstående kan ses som proaktiva metoder (förutseende och förekommande):

- avvikelserapportering, utredning och återkoppling
- säkerhetsgranskning och revision
- systemsäkerhetsverksamhet under såväl anskaffning (SSWG-1) som bruk av system (SSWG-2)
- förslagsverksamhet som inkluderar identifiering av potentiella risker.

När en olycka har inträffat utreds denna genom avvikelseundersökning. Detta är dock en reaktiv metod (att i efterhand förhindra upprepning), vilket innebär att skadan redan har inträffat.

4 RISKHANTERING

4.1 GRUNDER

Riskhantering är en generell teknik som används inom många olika områden (jämför *avsnitt 2.1*). Några av de generella begreppen framgår av *bild 4:1* nedan.

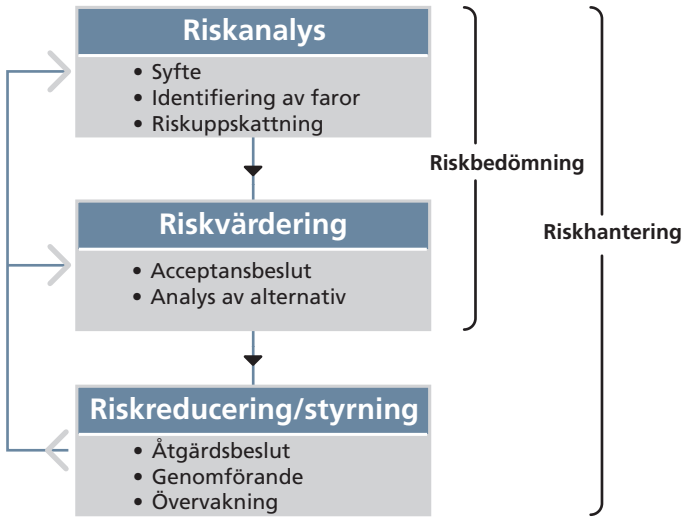


Bild 4:1 Generella riskhanteringsaktiviteter (IEC 60300-3-9) [7]

Riskhantering genomförs i princip under två skeden av tekniskt systems livslängd, utveckling och brukande. (Tillämpade metoder för riskhantering framgår av del 2 Metoder.)

4.2 Riskanalys

4.2.1 Syfte

Riskanalys under utvecklingsfasen syftar till att, innan någon olycka har inträffat, identifiera och uppskatta det tekniska systemets olycksrisker. Detta förutsätter tillgång till vederhäftiga data om systemets uppträdande/reaktion under framtida användning, såväl dess goda egenskaper som dess dåliga. Goda egenskaper är till exempel driftsdata som tillförlitlighet och tillgänglighet. Med dåliga egenskaper avses till exempel systemets benägenhet att ”gå sönder”, ge upphov till olika typer av vådahändelser och olyckor. Det är naturligtvis mycket svårt att identifiera data som beskriver dessa systemegenskaper, eftersom de avser systemets funktion i framtiden. Av samma skäl är det svårt att när dessa värden väl är framtagna, verifiera att de är tillräckligt sanna. I brist på en korrekt databank som beskriver systemets uppträdande i framtiden, gäller det att hitta verktyg som har förmåga att ge en godtagbar bild av det tekniska systemets framtida funktions- och riskegenskaper.

Riskanalys under brukandefasen syftar till att identifiera risker föranledda av ändringar och modifieringar. Det omfattar också att utgående från sammanställda data om rapporterade avvikelser, analysera dessa för att identifiera möjliga orsaker till inträffade händelser och på så sätt förhindra upprepning.

> Proaktiv (förutseende och förebyggande) riskhantering sker på vaga underlag och med ofullständiga verktyg, vilket kräver personal med erfarenhet och ödmjukhet som utför bedömningar med stor dynamik.

4.2.2 Identifiering av olycksrisk

Systemrisk

Beställaren/användaren har alltid ett uttalat syfte med varje beställt tekniskt system; det ska kunna leverera en viss förmåga till Försvarsmakten i vissa specifika operationsmiljöer.

Samtidigt som denna förmåga definieras, finns anledning att tidigt försöka identifiera vilka faror denna förmåga kan generera, direkt eller indirekt och vilka olyckshändelser som därvid skulle kunna inträffa. Detta utgör olycksrisker på systemnivå, ”Systemrisk”.

Riskanalys avseende systemrisker kan enklast utföras genom att specificera det tekniska systemets förmåga och sedan flera gånger ställa frågan: ”Vad får absolut inte lov att inträffa på grund av denna förmåga?” (Antingen som direkt effekt av ”felriktad” förmåga eller sekundär effekt av förmågan.)

På så sätt kan bland annat följande systemrisker identifieras:

- fartygsbesättning riskerar att drunkna om fartyget behöver överges till sjöss
- stridsfordonsbesättning riskerar livet om fordonet välter ner i vatten och landar på enda utgången
- ubåtsbesättning riskerar livet om ubåt inte kan inta ytläge
- flygplansbesättning riskerar livet om flygplan störtar
- egenbekämpning (någon typ av vapenverkan/störning som förutom att träffa motståndaren också riskerar att skada egna förband).

Krav på specifika **systemsäkerhetsegenskaper** som kan skydda mot identifierade systemrisker identifieras med fördel mycket tidigt, helst redan under studiefasen. Jämför *avsnitt 6.4 Studier* och *avsnitt 6.5.3 Krav avseende systemrisk*.

Notera att MIL-STD-882C innehåller System Hazard Analysis, Task 205, som handlar om att identifiera risker som är föranledda av den totala systemkonstruktionen. Dock anges inte i standarden hur detta ska utföras.

System av system

En ny förmåga kan skapas genom att använda befintliga tekniska system och produkter på nytt sätt, eventuellt tillsammans med nytillförd materiel. Det specifika är att den avsedda förmågan tidigare inte har systemsäkerhetsanalyserats och därför saknar systemsäkerhetsbeslut.

Vid integration av system/delsystem/produkt kan ofta nya olycksrisker uppstå genom att det tillförs nya sätt på vilka befintliga riskkällor kan utlösas (nya vådahändelser, nya former av exponering för vådahändelser) och nya farliga tillstånd tillförs.

Att övergå till ”högre systemnivåer” innebär ofta att:

- olycksrisker på ”lägre systemnivåer” finns kvar
- olycksrisker på ”högre systemnivåer” tillkommer.

Vid framtagning av nya system/funktioner behöver identifiering ske av nya olycksrisker som uppkommer genom nya förutsättningar, nya utlösande faktorer, nya farliga tillstånd, nya objekt som tillkommit och som kan exponeras.

Även vid riskanalys för system av system är alltså syftet att identifiera olycksrisker.

Konstruktionsrisk

Att identifiera primära olycksrisker (det vill säga olycksrisker på lägsta tekniska nivå) redan tidigt, är en viktig del av konstruktionsarbetet och ingår alltid i leverantörs åtaganden (och utförs med hjälp av handbokens metoder). Skälet till att leverantör åläggs detta ansvar är att kostnaden för en tidigt vidtagen riskreducerande åtgärd är förhållandevis låg. Betydligt mer resurskrävande är att åtgärda olycksrisk som upptäcks först när produktionen har påbörjats eller är avslutad.

Olycksrisk som upptäcks ännu senare under tekniskt systems livslängd visar sig ofta som tillbud eller olycka. Den kan då ha förorsakat förlust av människoliv plus att det som regel är mycket kostsamt att vidta riskreducerande åtgärder på tekniska system i bruk.

Vid konstruktion identifieras fortlöpande olycksrisker förorsakade av enskilda komponenter/apparater/tekniska delsystem. Konstruktör utför fortlöpande riskanalys i samband med materialval, val av komponenter och apparater och vidtar fortlöpande effektiva riskreducerande åtgärder som en naturlig del av konstruktionsarbetet.

Riskmodellen enligt *bild 3:1* ovan avser att utgöra ett stöd när riskkällor och farliga tillstånd ska identifieras. Bilden underlättar också att identifiera flera olika alternativ för att eliminera/reducera en viss identifierad olycksrisk. Alternativ kan bygga på att:

- reducera riskkällans/det farliga tillståndets fysiska egenskap genom att till exempel byta mot något mindre farligt
- motverka/avbryta den mekanism som möjliggör för riskkällan att ”bli farlig”
- bromsa/förhindra utlösning av riskkällans farliga egenskap
- för riskkälla som likväl utlöses, respektive för farligt tillstånd, kan olycka möjligen undvikas genom att förhindra exponering, till exempel genom att konstruera in fysiskt skydd för personal eller flytta personal utom räckhåll för faran.

Det är konstruktörens uppgift att dels säkerställa krävd funktion och prestanda, dels att uppfylla ställda krav på systemsäkerhet. Konstruktören väljer riskreducerande åtgärder så att alla krav samtidigt uppfylls. Allt detta utförs på ett så ekonomiskt sätt som möjligt. Kunden anger genom krav på risknivå, hur långt konstruktören behöver gå i sin strävan att reducera de risker som uppkommer/identifieras under konstruktionsarbetet.

Integrationsrisk

Delsystem förutsätts tas fram enligt gällande systemsäkerhetsmetodik och ges egenskaper så att ställda krav på systemsäkerhet uppfylls (se ovan).

När två olika delsystem, framtagna enligt denna princip, integreras med varandra, finns ändå ingen garanti för att resultatet (integrationen) uppfyller ställda krav på risknivå. Det är istället så att nya olycksrisker uppstår ur förhållanden som att delsystemen inte automatiskt kommunicerar med varandra på ett säkert sätt inom alla de fysikaliska områden som system kan kommunicera. Till exempel kan radioförbindelser störa varandra, elektromagnetisk strålning från opererande maskiner kan störa ut funktioner, gemensam strömförsörjning kräver exakt kunskap om frekvenser, effektförbrukning, spänningar, hydraulsystem ska ha gemensamma oljor, tryck och kopplingsdon.

Det är naturligt att förvänta sig att tillverkare/konstruktör ska hitta dessa olycksrisker eftersom de är direkt förorsakade av konstruktionens fysiska egenskaper samt att de direkt kan avlägsnas om konstruktionen utförs på ett anpassat sätt. Det är därför systemintegratörs uppgift att ta hand om och utföra nödvändig riskreducering avseende integrationsrisk.

Om de delar som ska integreras inte samtliga är framtagna med krav på att integreras med varandra, de kan till exempel utgöras av COTS, så måste designansvar för delsystemen respektive för det sammansatta systemet hanteras. Om inte uppdragsgivaren lägger ut (köper) designansvaret för det integrerade systemet från en enda leverantör så kvarstår denna uppgift hos uppdragsgivaren.

Metoder

Det finns flera angreppssätt, med skilda syften, för att utföra riskidentifiering. De olika angreppssätten skiljer sig åt beroende av vilken teknisk systemnivå analysen avser. Jämför *tabell 4:1*.

Tabell 4:1 Angreppssätt för riskidentifiering

Syfte	Angreppssätt för riskidentifiering
Systemrisk, även system av system	Identifiering av sådana övergripande systemfunktioner som kan utlösas oavsiktligt eller på annat sätt hota (Svarar ofta på frågan: ”Vad får inte inträffa?”)
Konstruktionsrisk	Identifiering av riskkällor och farliga tillstånd samt riskidentifiering vid val av konstruktionselement och konstruktion
Konstruktionsrisk respektive integrationsrisk	Teoretisk genomgång av funktionskedjor såsom vapensystem, maskinsystem, avioniksystem, för att identifiera riskkällor och farliga tillstånd (Exempel på vapensystem: sensor-ledningssystem-eldledningssystem-vapenlavett)
Konstruktionsrisk respektive integrationsrisk	Fysisk rundvandring i utrymmen där det tekniska systemet är installerat, utrymme för utrymme, för att identifiera riskkällor och farliga tillstånd

Identifiering av säkerhetskritisk funktion

Det kan finnas säkerhetskritisk prestanda/funktion hos ett tekniskt system. Med detta avses prestanda/funktion som om den inte fungerar leder till en farlig situation som utsätter operatör/förband för förhöjd olycksrisk. Motorn i ett enmotorigt flygplan är ett exempel på detta. Ett annat exempel är nyckelförsedd strömbrytare som bryter ström till roterande radarantenn avsedd att användas av tekniker som försiktighetsåtgärd inför underhållsåtgärd.

Det kan finnas tillfällen när ett annat tekniskt system är beroende av ”stöd” (indata, kraft med mera) för sin funktion som är säkerhetskritisk i någon mening. Problemet kan till exempel lösas med redundanta stödfunktioner, det vill säga alternativa källor för leverans av stödet. Ansvaret för att kravställa en lösning ligger hos det tekniska system som efterfrågar stödet.

> Fientlig verkan är inte en olycksrisk utan en del av normal verksamhet och motverkas med militärt uppträdande, skyddsåtgärder, taktik och stridsteknik.

Resultat av riskidentifiering

Resultat från riskidentifiering sammanställs som en lista över identifierade olycksrisker, med ursprung i redovisat farligt tillstånd respektive vådahändelse, samt förekommande exponering. Denna sammanställning görs företrädesvis i Risklogg. En närmare redovisning för denna aktivitet samt riskloggen och dess tillämpning lämnas i *bilaga 2*. En kortare redovisning av riskloggen återfinns i *avsnitt 4.5*.

4.2.3 Riskuppskattning

Riskuppskattning består i att uppskatta möjliga konsekvenser av varje identifierad olycksrisk. Handboken redovisar i *bilaga 1 Riskuppskattning* en omfattande beskrivning av lämpligt tillvägagångssätt för detta. Resultat av aktiviteten riskuppskattning dokumenteras i Risklogg med angivande av uppskattade värden för sannolikhet och konsekvens.

Bedömd sannolikhet för viss olycksrisk avser användning enligt angiven driftprofil av ett exemplar under avsedd livslängd av det tekniska systemet.

Riskuppskattning av miljörisk

Olycksrisk för skada på yttre miljö kan resultera i konsekvenser som kan återställas/saneras, respektive skador som är bestående, till exempel helt utplånar en djurart eller varaktigt förstör ett visst fysiskt område.

- Olycksrisk med reparabla konsekvenser kan uppskattas i ekonomiska termer.
- Olycksrisk med bestående konsekvenser ska alltid betecknas som icke tolerabel (det vill säga som röd olycksrisk). Beslut om stängning av sådan olycksrisk kan endast tas av Försvarsmakten.

Riskuppskattning av ekonomisk risk

Risk för ekonomisk förlust anses i denna handbok utgöras av:

- direkt skada på eller förlust av materiel, delsystem, system
- skada på annans egendom
- kostnad för sanering av skada på yttre miljö som Försvarsmakten har orsakat genom sin verksamhet med aktuellt tekniskt system.

4.3 Riskvärdering

4.3.1 Kravställning avseende olycksrisk

Grunden för Försvarsmaktens riskhanteringsmetod är att kravställa högsta tillåtna värde för olycksrisk i tekniskt system. Detta görs med hjälp av riskmatriser, en för personskada och en för ekonomisk skada.

En riskmatris (avseende risk för personskada respektive risk för ekonomisk skada) anger **den högsta risknivå som godtas** (= tolerabel risknivå) för enskild olycksrisk.

Egenskaper hos riskmatris – aversionsfaktor

Samhället betraktar enstaka dödsfall som oönskade, ej tolerabla men egentligen oundvikliga. Olyckor med flera människooffer utlöser oftast stora reaktioner i samhället och krav på samhällsinsatser och lagändring. I konsekvens med detta ses smärre blessyrer, benbrott och viss grad av invaliditet som ganska lyckosamma utgångar av olyckor som ”kunde ha slutat värre”.

Sammantaget innebär detta att det i samhället råder olika acceptans för olyckor beroende på vilken skada som kan uppstå. Lindriga skador accepteras som oundvikliga, men det finns en aversion mot allvarligare olyckor.

Handbokens exempel på riskmatriser har därför en aversionsfaktor inlagd. Denna faktor beaktar just synsättet att allvarlig olycka tolereras i lägre utsträckning än motsvarande olycka som resulterar i lindrigare skador.

Värderingsmetoder

Värdering är enskild olycksrisk kan göras:

- kvalitativt (verbal beskrivning av sannolikhet och konsekvens)
- kvantitativt, där siffervärde används för att ange sannolikhet och konsekvens.

Riskmatris för personskada

Nedan redovisas exempel på riskmatris för personskada. Matrisen är hämtad ur MIL-STD-882C, samt förekommer i Handbok Materielförvaltning Sjö (HMS) *[24]*.

Till matrisen hör beskrivning av skadeklass respektive sannolikhet alternativt frekvens.

Matrisen är kvantitativ. Om kvalitativ riskvärdering ska utföras, så bortses från sifferkolumnen i *tabell 4:3* respektive *tabell 4:4*.

Notera att riskmatrisen avser användning av ett exemplar under det tekniska systemets livslängd.

Sannolikhet / Skadeklass	A	B	C	D	E
I	ET	ET	ET	ET	T
II	ET	ET	ET	BT	T
III	ET	BT	BT	T	T
IV	BT	T	T	T	T

Bild 4:2 Exempel på riskmatris för värdering av personskada

De begrepp för risknivåer som används i bilden ovan är:

- ET = Ej tolerabel
- BT = Begränsat tolerabel
- T = Tolerabel.

Kategorisering för skadeklass avseende person, sker enligt *tabell 4:2*.

Kategorisering av sannolikhet sker enligt *tabell 4:3* och för frekvens enligt *tabell 4:4*.

Tabell 4:3 och *4:4* kan användas alternativt. Notera dock att frekvensklassernas (A-E) faktiska värden inte överensstämmer mellan de två tabellerna.

Tabell 4:2 Kategorisering för personskada

Skadeklass	Beskrivning av skada på person
I	Dödsfall
II	Allvarlig skada
III	Mindre allvarig skada
IV	Försumbar skada

Tabell 4:3 Kategorisering för olyckssannolikhet

	Beskrivning av olyckssannolikhet, för ett exemplar av systemet	Sannolikhet under livslängden
A	Kommer troligen att inträffa frekvent	$>10^{-1}$
B	Kommer att inträffa flera gånger under livslängden	$10^{-2} – 10^{-1}$
C	Kan inträffa någon gång under livslängden	$10^{-3} – 10^{-2}$
D	Osannolikt men möjligt att olyckan inträffar någon gång under livslängden	$10^{-6} – 10^{-3}$
E	Så osannolikt att olyckan inte bedöms inträffa någon gång under livslängden	$<10^{-6}$

Tabell 4:4 Kategorisering av olycksfrekvens

	Beskrivning av olyckssannolikhet, för ett exemplar av systemet	Frekvens
A	Kommer troligen att inträffa frekvent	>1 gång/år
B	Kommer att inträffa flera gånger under livslängden	1 gång under 1 - 5 år
C	Kan inträffa någon gång under livslängden	1 gång under 5 - 75 år
D	Osannolikt men möjligt att olyckan inträffar någon gång under livslängden	1 gång under 75 - 1000 år
E	Så osannolikt att olyckan inte bedöms inträffa någon gång under livslängden	< 1 gång per 1000 år

Riskmatris för ekonomisk skada

Nedan redovisas exempel på riskmatris för ekonomisk skada.

Till matrisen hör beskrivning av skadeklass respektive sannolikhet alternativt frekvens.

Matrisen är kvantitativ. Om kvalitativ riskvärdering ska utföras, så bortses från sifferkolumnen i *tabell 4:3* respektive *4:4*.

Notera att riskmatrisen avser användning av ett exemplar under det tekniska systemets livslängd.

Sannolikhet / Skadeklass	A	B	C	D	E
I	ET	ET	ET	BT	T
II	ET	ET	BT	T	T
III	ET	BT	T	T	T
IV	BT	T	T	T	T

Bild 4:3 Exempel på riskmatris för värdering av ekonomisk skada

Kategorisering av sannolikhet för ekonomisk skada genomförs på samma sätt som för personskada, det vill säga med endera av *tabell 4:3* eller *4:4*.

Kategorisering för skadeklass av ekonomisk skada utförs enligt *tabell 4:5*.

Tabell 4:5 Kategorisering för ekonomisk skada

Skadeklass	Beskrivning av ekonomisk skada (egen och andras egendomsskada och saneringskostnad)	Skadan uttryckt i kronor
I	Ungefär samma kostnad som total systemförlust	> 10^9 SEK (> 1 miljard)
II	Betydande förlust	10^7 – 10^9 SEK (10 miljoner - 1 miljard)
III	Begränsad förlust	10^5 – 10^7 SEK (100 000 - 10 miljoner)
IV	Liten förlust	< 10^5 SEK (< 100 000)

Justering av skadeklass för ekonomisk risk

För att ha relevans för visst specifikt tekniskt system (billigare eller dyrare) kan riskmatrisen för ekonomisk skada behöva anpassas. Det är rimligt att de skador det tekniska systemet kan förorsaka sätts i relation till anskaffningskostnaden för ett exemplar av det tekniska systemet. (Skadeklass 1 = total kostnad för ett exemplar av aktuellt tekniskt system).

Detta innebär att i den anpassade riskmatrisen för ekonomisk skada för aktuellt tekniskt system, bör beloppen för respektive skadeklass ändras och grundas på total kostnad för ett exemplar.

Ett exempel på alternativ definition av skadeklasser, som uttrycker lägre värden/grundat på ett mindre kostsamt tekniskt system är följande:

I	> 10 miljoner
II	100 000 - 10 miljoner
III	1 000 - 100 000
IV	< 1 000

Anpassning utförs vid framtagning av TTEM.

Det finns också möjlighet att göra skillnad på typ av egendomsskada och tillämpa olika toleranskriterier för:

- skada på eget system
- skada på tredje parts egendom
- kostnader förknippade med att återställa skada på yttre miljö.

Se närmare i HMS *[24]*.

Användning av kvalitativ respektive kvantitativ riskmatris

Kvalitativ riskmatris används ofta vid den första inledande riskuppskattningen. När utvecklingen av tekniskt system fortsätter och uppfattningen om vald tekniks egenskaper klarnar, sker övergång till kvantitativ riskmatris.

Kvantitativ riskmatris möjliggör en mer precis värdering av exponeringens inflytande på olycksriskens storlek.

För riktigt enkelt tekniskt system och enskild produkt och då endast enstaka riskkällor förekommer, kan med fördel kvalitativ riskmatris vara enda tillämpad metod (det vill säga i *tabell 4:3* alternativt *4:4* stryks den tredje kolumnen; sifferkolumnen).

Befintlig äldre riskmatris eller riskmatris ur denna handbok

Om anskaffningen avser komplettering till ett redan befintligt tekniskt system är det rimligt och lämpligt att fortsatta att använda den riskmatris som använts för den ursprungliga anskaffningen.

Generellt om justering av riskmatris

Handbokens exempel på riskmatriser kan behöva ändras för viss anskaffning. Om det tekniska system som ska anskaffas kan anses skilja sig från ett tidigare anskaffat tekniskt system avseende krav på systemsäkerhet bör detta avspegla sig i de krav som riskmatrisen uttrycker. Sådant skiljande kriterium kan till exempel avse att:

- endast en lägre tolerabel risknivå kan godtas
- högre tolerabel risknivå kan godtas
- många personer kommer samtidigt att exponeras för det tekniska systemets risker.

Härvid kan Försvarsmakten i särskilda fall komplettera riskmatrisen med till exempel:

- ytterligare kolumn för sannolikhet, varvid samtliga sannolikhetsnivåer justeras
- ytterligare rad med skadeklassen ”flera dödsfall”.

Det bör observeras att antalet risker i ett system inte beaktas, vilket innebär att systemets storlek inte tillmäts betydelse. Det är endast risknivå för den enskilda olycksrisken, en i taget, som beaktas (identifieras, uppskattas respektive värderas).

DesignA kan justera i TTEM erhållen riskmatris i syfte att ålägga leverantör att redovisa grund för stängning av risk på ett mer kontrollerat sätt (= omvandla en eller flera gröna rutor till gula).

4.3.2 Stängning av risk – acceptansbeslut

För vardera av ett tekniskt systems olycksrisker, genomförs acceptansbeslut som bestämmer huruvida olycksrisken kan accepteras som den är eller kräver riskreducering. Vid acceptansbeslut jämförs olycksriskens värde, hämtat ur det tekniska systemets risklogg, med kravställt riskvärde. Jämförelsen görs med hjälp av riskmatris.

DesignA ska granska och godkänna leverantörs riskhanteringsarbete avseende samtliga risker, även sådana som leverantör har klassificerat som ”gröna”.

För olycksrisker inom gult område ska DesignA ta emot redovisning från leverantör om riskens egenskaper, vidtagna/föreslagna riskreducerande åtgärder, övervakning eller om ytterligare riskreducering ska genomföras, varefter DesignA beslutar om stängning av risken.

Röd olycksrisk, för vilken det inte har kunnat tas fram tillräckliga åtgärder för att komma ifrån rött område, anmäls skyndsamt av DesignA till Försvarsmakten. Försvarsmakten beslutar om vilka åtgärder som ska vidtas med anledning av röd olycksrisk.

Beslut med stöd av riskmatris

Öppna dokumentet Risklogg. För aktuell olycksrisk, läs av de fyra riskdelarnas sannolikhet. Avläs i riskmatrisen vardera riskdelens placering och färg. Färgen avgör om storleken av aktuell delolycksrisk kan tolereras eller inte. Om någon de fyra riskdelarna har hamnat inom rött (gult) område, betraktas hela olycksrisken som ej tolerabel (begränsat tolerabel), och riskreducering krävs.

Först när alla fyra markeringar ligger inom grönt område är olycksrisken tolerabel.

(Se *bilaga 1 Riskuppskattning*, för detaljer om enskild risk och dess riskdelar. Se *bilaga 2 Risklogg*, för detaljer om dess användning).

Beslutsfattare

Det är Försvarsmaktens ansvar att specificera vem som har rätt att fatta beslut om olika typer av risker. Vid anskaffning ska detta anges i TTEM som krav till DesignA. Normalt utformas kravet på följande sätt:

Leverantör stänger risken efter samråd med DesignA

Leverantör meddelar DesignA om risken och presenterar dokumentation. DesignA stänger risken

Leverantör meddelar DesignA om risken och presenterar dokumentation snarast när risken är upptäckt. DesignA meddelar Försvarsmakten om risken. Endast den som fastställt Försvarsmaktens krav, kan stänga risken.

4.3.3 Analys av alternativ

I fall att olycksrisk inte är tolerabel ska riskreducering ske. Varje riskreducerande åtgärd behöver beredas konstruktionsmässigt. Härvid är det effektivt att ställa flera ingenjörsmässiga lösningar mot varandra, för att hitta just den lösning som ger mest effekt för insatta resurser.

4.4 RISKREDUCERING/STYRNING

4.4.1 Åtgärdsbeslut

Riskreducering för ett tekniskt system under framtagning / utveckling ska bedrivas så länge som det behövs för att innehålla ställda krav; det vill säga säkerställa att risken flyttas till grönt område inom riskmatrisen.

Jämför texten om *ALARP-metodiken i H SystSäk del 2, avsnitt 5.4*. Observera skillnaden att den metodiken kräver att all möjlig/rimlig riskreducering ska genomföras för varje enskild olycksrisk, så länge insats av resurser står i rimlig relation till effekten.

4.4.2 Genomförande

Vid reducering av enskild olycksrisk kan följande faktorer påverkas för att uppnå riskreducering:

- förutsättningarna för att en olycka ska inträffa
- sannolikhet för respektive utfall.

Principen för riskreducering måste alltid vara att olycksrisker större än vad som kravställts i TTEM ska minskas till kravställd nivå. Riskhanteringsarbetet för ett tekniskt system måste därför alltid grundas på en riskuppskattning. Några lämpliga verktyg för detta redovisas i *bilaga 1 Riskuppskattning*.

Riskreducering av olycksrisker i ett tekniskt system kan generellt utföras på tre olika sätt:

- minskning av förekomst av farligt tillstånd och sannolikhet för vådahändelse
- minskning av sannolikhet för exponering
- minskning av olyckans konsekvens.

Olycksrisker för ett nytt tekniskt system bör ses som generellt hotande händelser, som vardera har ett brett möjligt scenario. Dessa scenarier påverkas i stor omfattning av yttre faktorer såsom tillämpning (hur tekniken används i det enskilda fallet) och den miljö i vilket det tekniska systemet ska verka/användas.

Att försöka identifiera framtida olycksrisker genom att titta i backspegeln och jämföra med erfarenheter från tidigare tekniska system är naturligtvis möjligt. Men sådana erfarenheter utgör en samling specialfall, nämligen inträffade olyckor. Var och en av dessa olyckor berodde mycket av de då rådande yttre förhållandena. Det inses att just dessa förhållanden torde vara helt unika och knappast gäller för en annan miljö och för en annan tillämpning.

Det finns därför behov av att hitta verktyg som möjliggör ett generellt betraktelsesätt som samtidigt ger möjlighet att variera ingående faktorer på ett spårbart och dokumenterbart sätt.

Av de verktyg som redovisas i *bilaga 1* är det bara Modellering/Simulering som har alla nödvändiga goda egenskaper som krävs för att ge ett kvalitetsmässigt bra och väl dokumenterat underlag. Med fördel kan underlag framtagna med hjälp av de andra redovisade verktygen användas som ingångsvärden vid tillämpning av metoden Modellering/Simulering.

4.4.3 Övervakning

En olycksrisk som har erhållit viss riskreducering har därigenom inte självklart minskats till avsedd risknivå. Resultatet av riskreducerande åtgärd måste verifieras. Metod för verifiering bör bestämmas vid samma tid som den riskreducerande åtgärden bereds och beslutas. Riskreducerande åtgärd där verifieringsmetod saknas bör inte väljas i första hand.

När önskad riskreduktion har genomförts och verifierats (jämför *bild 4:1*) görs förnyad riskanalys för att säkerställa att inte de riskreducerande åtgärderna samtidigt medfört riskhöjning eller introducerat nya olycksrisker.

Därefter genomförs ny riskvärdering.

4.5 Risklogg

Att ta fram och leverera fullständig riskdokumentation är ett obligatoriskt krav till leverantör. En del i riskdokumentationen utgörs av risklogg. Handboken redovisar den risklogg som uppfyller Försvarsmaktens minimikrav på redovisning av olycksrisk och dess delkomponenter.

Vid till exempel internationellt samarbete kan annan dokumentation användas varvid handbokens risklogg ska utgöra specifikation på innehåll men inte utförande.

Vid förande av risklogg inleds arbetet med att justera riskloggen efter det tekniska systemets krav och behov. Därefter identifieras riskkällor och farliga tillstånd, som allt efterhand förs in i riskloggen. Riskloggen kompletteras fortlöpande under riskhanteringens samtliga aktiviteter. Också åtgärder för att erhålla och verifiera riskreducering samt acceptansbeslut förs in i riskloggen.

Riskloggen följer det tekniska systemet under hela dess livslängd. Under vidmakthållandefasen kan till exempel SSWG-2 ges uppdrag att föra riskloggen.

Under vidmakthållandefasen redovisas i riskloggen varje enskild olycksrisk med beräkning av riskvärde före och efter eventuell riskreducerande åtgärd. (Detaljerad handledning i förande av risklogg framgår av *bilaga 2*.)

På engelska förkommer uttrycket ”initial risk” för att beteckna först uppskattad storlek av en viss olycksrisk. Med begreppet ”residual risk” (kvarstående risk) avses riskens storlek efter viss vidtagen riskreducerande åtgärd.

5 Beskrivning av systemsäkerhetsverksamhet

5.1 Försvarsmaktens ansvar för tekniskt systems säkerhet

Inför varje beslut om uppdrag avseende tekniskt system bör Försvarsmakten identifiera hur ansvaret för det aktuella tekniska systemets säkerhet fördelas på lämpligaste sätt. Nedanstående avser ge viss vägledning.

a. Försvarsmakten har generellt allt ansvar för de tekniska systemens säkerhet. Ordinarie verksamhet för framtagning av tekniskt system ska också omfatta genomförande av erforderlig systemsäkerhetsverksamhet. Ett antal aktörer är engagerade i denna verksamhet. Dessa har en etablerad ansvars- och rollfördelning.

b. Försvarsmakten kan genom uppdrag om designansvar anlita annan organisation för stöd avseende tekniskt systems säkerhet.

c. Det står Försvarsmakten fritt att anlita och utse valfri organisation att ta ansvar inför Försvarsmakten som DesignA. För mer komplext tekniskt system anlitas företrädesvis särskilt kompetent teknisk organisation. Designansvar behålls lämpligen under ett tekniskt systems hela livlängd.

d. Försvarsmakten ägnar särskild uppmärksamhet åt att säkerställa ansvaret för integration då krav avses ställas att tekniska system med olika DesignA ska kunna samverka

e. Om Försvarsmakten inte anlitar någon annan att ta ansvar för tekniskt systems säkerhet, kvarligger ansvaret hos Försvarsmakten.

f. Om Försvarsmakten utför ändring i tekniskt system som omfattas av anlitad DesignA ansvar, återgår ansvaret för det tekniska systemets säkerhet omgående till Försvarsmakten.

g. Vid anskaffning av ren COTS-produkt som används fristående (det vill säga inte tillsammans med tekniskt system) i enlighet med tillverkarens bruksanvisning, erfordras inget särskilt designansvar. Istället har Försvarsmakten som arbetsgivare ansvar att ställa krav på CE-märke och försäkran om överensstämmelse, att bruksanvisningar och underhållsinstruktioner medföljer, samt skyldighet att se till att nyanskaffad utrustning uppfyller gällande regler innan den ställs till arbetstagares förfogande *[6]*.

   För civil ammunition är CE-märkning ersatt med CIP-märkning.

5.2 Tekniskt designansvar

Tekniskt designansvar innebär att för tekniskt system fastställa teknisk struktur och konstruktion, samt att fastställa vilken integration av tekniska system, 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 hela livslängden.

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. Se vidare *avsnitt 7.7 DesignA:s mandat och ansvar för ändring*.

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 inför Försvarsmakten. Designansvaret för Militära luftfartsprodukter regleras i Regler för Militär Luftfart (RML) *[34]*.

5.3 Krav och beslut inom systemsäkerhetsverksamheten

Detta avsnitt redovisar de särskilda krav och beslut som erfordras för att styra systemsäkerhetsverksamheten för tekniskt system

Förkommande systemsäkerhetsaktiviteter under ett tekniskt systems hela livslängd framgår av *bild 5:1* nedan.

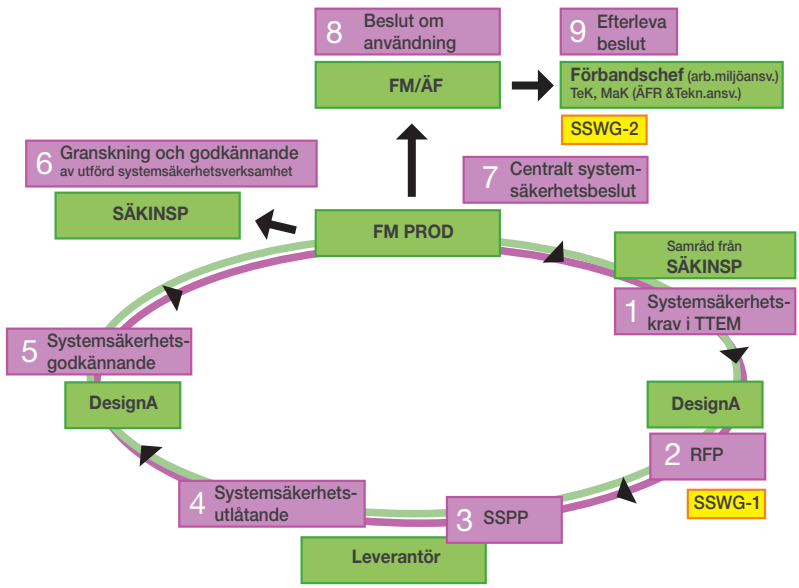


Bild 5:1 Förekommande systemsäkerhetsaktiviteter under livslängden

Aktiviteter redovisade i *bild 5:1* (numrering av nedanstående punkter överensstämmer med bildens numrering)

1. ÄF ställer systemsäkerhetskrav i kundbeställning (KB) och TTEM för visst tekniskt system. SÄKINSP tecknar samråd
2. DesignA ställer systemsäkerhetskrav i RFP (anbudsinfordran)
3. Leverantör redovisar avsedd systemsäkerhetsverksamhet i anbudet till DesignA genom preliminär SSPP
4. Leverantör beslutar om systemsäkerhetsutlåtande och överlämnar detta till DesignA
5. För alla tekniska system som överlämnas till Försvarsmakten samt för alla integrationsprodukter beslutar DesignA genomföra systemsäkerhetsverksamhet samt utfärda systemsäkerhetsgodkännande och överlämna detta till Försvarsmakten.

6. ÄF tar fram ett utkast till centralt systemsäkerhetsbeslut (CSSB) och överlämnar detta till Försvarsmaktens Säkerhetsinspektion som granskar genomförd systemsäkerhetsverksamhet och, förutsatt att genomförd systemsäkerhetsverksamhet bedöms vara av tillräckligt god kvalitet, lämnar samråd på CSSB.
7. ÄF fastställer CSSB och överlämnar detta till Försvarsmakten/ÄF. ÄFR och SSWG 2 är huvudintressenter av den riskdokumentation för tekniskt system som överlämnas av DesignA till Försvarsmakten vid nedanstående överlämningstillfällen:
   - överlämning av nytt tekniskt system
   - överlämning efter modifiering
   - överlämning efter underhållsåtgärd (vid underhållsåtgärd uppdateras riskdokumentationen endast då åtgärden medfört förändrad värdering av det tekniska systemets risker (riskkällor respektive farliga tillstånd).

   Se även Försvarsmaktens rutin avseende leveranser av produkter från FMV till Försvarsmakten *[9]*
8. ÄF fattar beslut om användning (BOA) och överlämnar detta bland annat till aktuella förbandschefer
9. Förbandschef tillser att förekommande krav i BOA innehålls vid brukandet av det tekniska systemet och att dess konfiguration överensstämmer med vad som anges i BOA.

   Förbandschef är huvudintressent till Försvarsmaktens beslut om användning. Förbandschef har ansvaret för att verksamheten genomförs med rätt materiel, rätt utbildad personal, med rätt föreskrifter, i rätt miljö och på rätt sätt. För att möjliggöra detta ansvarstagande behöver förbandschef information om vilka föreskrifter som gäller för visst tekniskt system, samt hur detta får och ska användas. Denna samlade information kan endast erhållas från systemsäkerhetsbeslut för visst tekniskt system.

5.4 Kravställning

Principer och detaljer vid kravställning är redovisade tillsammans med beskrivning av Försvarsmaktens systemsäkerhetsverksamhet. Se främst *avsnitt 6.5 Anskaffning*.

5.5 Systemsäkerhetsbeslut

Genomförd systemsäkerhetsverksamhet dokumenteras i de tre definierade systemsäkerhetsbesluten (som bland annat framgår av *bild 5:1* ovan):

- systemsäkerhetsutlåtande (leverantör)
- systemsäkerhetsgodkännande (DesignA)
- centralt systemsäkerhetsbeslut (ÄF).

Dessa beslut ska vara väl underbyggda. Inför varje sådant beslut erfordras alltid någon form av riskanalys och/eller framtagning av slutsats av eventuellt föregående beslut. Analyser, slutsatser och övriga överväganden ska dokumenteras i beslutet. Om dessa är mer omfattande sammanfattas de i beslutet och bifogas som bilaga.

> Det bör observeras att ett visst systemsäkerhetsbeslut godkänner i beslutet redovisad konfiguration för användning vid i beslutet redovisad verksamhet. Beslutet ”låser” därmed konfiguration och verksamhet. Märk även att systemsäkerhetsbeslutet sällan eller aldrig behöver vara tidsbegränsat. Behov att upphäva ett systemsäkerhetsbeslut uppkommer endast när det påvisats att aktuell konfiguration/användning/verksamhet ger upphov till risker större än vad som är tolerabelt.

För det speciella fall att DesignA har uppdragits att för visst tekniskt system utfärda ett systemsäkerhetsgodkännande, men där det tekniska systemet i fråga konstateras inte ha acceptabel säkerhetsnivå, lämnas istället rapport i form av ett **säkerhetsmeddelande**. (Se vidare i *H SystSäk del 2 under systemsäkerhetsgodkännande*.)

Provturskommando (PTK, se vidare i *H SystSäk del 2*) innehåller en särskild form av systemsäkerhetsgodkännande som av hävd benämns **säkerhetsintyg**. Detta 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.

5.6 Besluts- och produktdokument för tekniskt system

5.6.1 Generellt

Besluts- och produktdokument för tekniskt system ska alltid omfatta

- systemsäkerhetsbeslut
- riskdokumentation
- konfigurationsbeslut.

Sekretess

Besluts- och produktdokument för tekniskt system ska generellt alltid vara öppna. Om enskild uppgift är belagd med sekretess dokumenteras denna uppgift i särskild bilaga till ordinarie besluts- respektive produktdokument för tekniskt system. Bilagan hanteras på det sätt som åsatt sekretessgrad kräver.

Nedan redovisas detaljerat hur besluts- och produktdokument kan utformas för nytt tekniskt system, ändrat tekniskt system, respektive för justerat tekniskt system.

5.6.2 Nytt tekniskt system

Systemsäkerhetsverksamhet ska genomföras av DesignA för *alla nya tekniska system* som avses överlämnas till Försvarsmakten. Genomförd systemsäkerhetsverksamhet ska bland annat dokumenteras i riskdokumentation och systemsäkerhetsbeslut. Fastställande av det nya tekniska systemets omfattning och konfiguration dokumenteras med konfigurationsbeslut.

Med nytt tekniskt system enligt ovan förstås även sådant tekniskt system som skapas av befintlig materiel genom att sätta samman delsystem från flera olika tekniska system. Syftet kan till exempel vara att skapa ny förmåga (system av system).

Riskdokumentation för nytt tekniskt system beskriver genomfört riskarbete, samtliga identifierade olycksrisker, erforderligt underlag för instruktioner, anvisningar, handböcker med mera för att till operatör förmedla kunskap om det tekniska systemets olycksrisker och hur operatören ska undvika dessa. Det samlade underlaget omfattar:

- systemsäkerhetsrapport (SAR) med analysresultat (från utförda analysaktiviteter såsom PHL, PHA, SHA med flera)
- riskbeslut (för varje enskild risk)
- risklogg
- information om det tekniska systemets risker samt underlag för instruktioner, anvisningar, handböcker med mera för hur dessa ska undvikas
- eventuell restriktion (avser inskränkning i det tekniska systemets brukande för att temporärt hantera viss risk).

Systemsäkerhetsbeslut för nytt tekniskt system omfattar:

- systemsäkerhetsutlåtande
- systemsäkerhetsgodkännande
- centralt systemsäkerhetsbeslut (som utgör del av grunden för Försvarsmaktens beslut om användning).

DesignA:s konfigurationsbeslut för nytt tekniskt system omfattar bland annat följande:

- referens till gällande systemsäkerhetsgodkännande
- produktdokumentation som fastställer det nya tekniska systemets omfattning och konfiguration. Här ingår också underhållsplaner (TO UF) som erfordras för vidmakthållande av det tekniska systemet.

5.6.3 Ändrat tekniskt system

Ändring av tekniskt system definieras av att dess konfiguration har förändrats. Detta uppstår vid tillägg av nytt delsystem, ny komponent, utbyte av fastställd komponent mot en med utökad/ändrad funktion eller annan ändring av det tekniska systemet. (Se även *avsnitt 5.7 Beslutstillfällen*.)

Utförd systemsäkerhetsverksamhet för ändrat tekniskt system, dokumenteras med riskdokumentation och systemsäkerhetsbeslut. Fastställande av det ändrade tekniska systemets omfattning, konfiguration och åtgärder för införande, dokumenteras med konfigurationsbeslut.

Riskdokumentation för ändrat tekniskt system beskriver genomfört riskarbete och samtliga identifierade förändringar avseende olycksrisker (tillkomna, borttagna, ökade, minskade och oförändrade) och omfattar:

- systemsäkerhetsrapport (SAR) avseende förändrade systemdelar, med analysresultat (från utförda analysaktiviteter såsom PHL, PHA, SHA med flera, se *H SystSäk del 2, avsnitt 5.12*, *5.13* och *5.16*)
- riskbeslut för varje enskild berörd olycksrisk
- risklogg för varje enskild berörd olycksrisk.

Systemsäkerhetsbeslut för ändrat tekniskt system:

- systemsäkerhetsutlåtande (förekommer när leverantör medverkat)
- systemsäkerhetsgodkännande
- centralt systemsäkerhetsbeslut.

Centralt systemsäkerhetsbeslut anger om ändring av tekniskt system föranlett ny olycksrisk eller ökad risknivå. I dessa fall ska beslut om användning uppdateras.

Konfigurationsbeslut för ändrat tekniskt system omfattar bland annat följande:

- referens till gällande systemsäkerhetsgodkännande
- produktdokumentation som fastställer det ändrade tekniska systemets omfattning och konfiguration
- Teknisk Order (TO) som erfordras för att teknisk organisation vid mottagande förvaltning/förband ska införa aktuell ändring i det tekniska systemet.

Tillämpningsbestämmelser för hantering, beredning och ansvarsförhållanden med mera vid genomförande av ändring av tekniskt system regleras genom Försvarsmaktens och FMV gemensamma Ändringsstyrningsprocess *[17]*.

5.6.4 Justerat tekniskt system

Justering (smärre ändring) av tekniskt system definieras av att systemets konfiguration endast i mindre grad har förändrats, att riskanalys har utförts och att denna visat att ingen ny olycksrisk har tillförts, att inte heller befintliga olycksrisker berörts av justeringen samt att risknivån inte har ökats för någon enskild olycksrisk. Exempel på detta kan vara utbyte av fastställd komponent mot en med motsvarande funktion men annan specifikation, eller annan smärre förändring av någon del av det tekniska systemet.

Utförd riskanalys för justerat tekniskt system dokumenteras och bifogas TO.

För ett justerat tekniskt system erfordras även **Konfigurationsbeslut**.

Tillämpningsbestämmelser för hantering, beredning och ansvarsförhållanden med mera vid genomförande av justering av tekniskt system regleras genom Försvarsmaktens och FMV gemensamma Ändringsstyrningsprocess *[17]*.

5.7 Beslutstillfällen

Behov av systemsäkerhetsbeslut eller uppdatering av befintligt systemsäkerhetsbeslut för tekniskt system enligt ovan analyseras då någon av nedanstående omständigheter har uppstått. Vägledning för analysens genomförande och hantering av olika resultat, erhålls ur *bild 5:2*. Om analysen påvisar att nytt/uppdaterat beslut krävs, så tas beslut fram enligt normal rutin.

Analys genomförs då:

- avvikelserapport har tillställts DesignA och genomförd utredning visar på stora, tidigare okända olycksrisker. DesignA lämnar förslag till åtgärd med det tekniska systemet, och/eller förslag till tillfällig inskränkning i användningen (restriktion)
- SSWG-2 har identifierat ny olycksrisk/omvärderat risknivån på befintlig olycksrisk, vilket har dokumenterats i risklogg (eller risklista)
- nytt tekniskt system har skapats (till exempel genom att använda befintliga produkter ur andra tekniska system och eventuellt tillsammans med nyanskaffad produkt)
- nytt tekniskt system har anskaffats (ett antal produkter har anskaffats som sammanförts till ett tekniskt system)
- befintligt tekniskt system har getts ny konfiguration (en eller flera produkter har lagts till/förändrats/dragits ifrån, det befintliga tekniska systemet)
- befintligt tekniskt system i befintlig konfiguration avses användas på nytt sätt (till exempel köra fortare, lasta mer, skjuta med viss annan ammunition)
- befintligt tekniskt system i befintlig konfiguration avses användas på avsett sätt, men i ny miljö
- införande eller användning av konfiguration som inte har godkänts av DesignA, har skett
- förändring av reglerat underhåll har skett/avses ske
- förändring av reglerad utbildning har skett/avses ske.

En översikt över överväganden vid tillämpning av systemsäkerhetsmetodiken samt aktuella besluts- och produktdokument enligt *avsnitt 5.6* framgår av *bild 5:2* nedan.

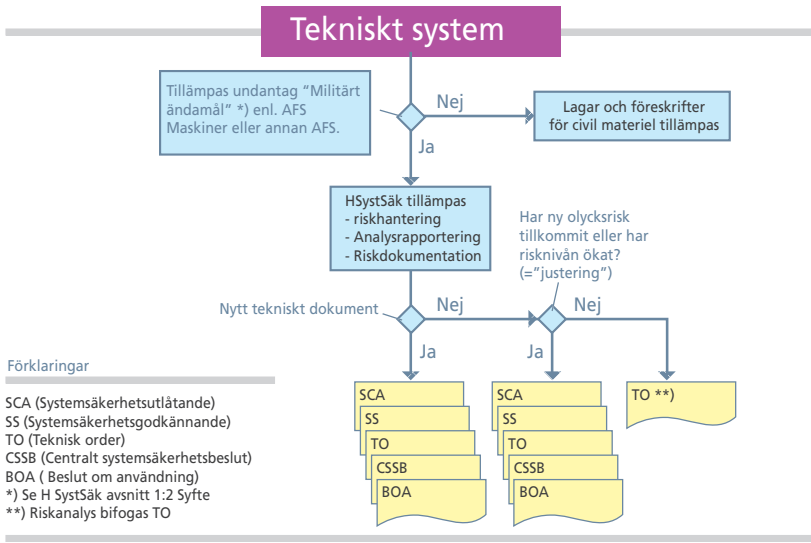


Bild 5:2 Överväganden, besluts- samt produktdokument för tekniskt system

5.8 Tekniskt system, struktur och gränsytor

Tekniskt system är den grundläggande materielenheten. Begreppet tekniskt system är generellt och används oavsett vilken systemnivå som avses. Ett visst tekniskt system kan av DesignA överlämnas till Försvarsmakten. Samma tekniska system kan också utgöra integrationsprodukt för att ingå i annat tekniskt system (ett eller flera).

Gränsytor finns runt alla tekniska system. De kan utgöras av andra tekniska system, strömförsörjning, vatten, avlopp, drivmedelsförsörjning, reparationsmöjligheter, flygtrafikledning och mycket annat. All systemsäkerhetsverksamhet måste utgå ifrån det tekniska systemet och alla dess gränsytor, såväl de som är kravställda av Försvarsmakten som de som är underförstådda med hänsyn till avsedd verksamhet med mera. Se *H SystSäk del 2, avsnitt 5.3 Systemsäkerhetskrav i TTEM (TTEM) – S11*

Som **produkt** benämns vanligen ett tekniskt system som levereras från viss leverantör. För produkt erfordras ett systemsäkerhetsutlåtande. Om ett tekniskt system utgörs av en civil produkt som köps ”över disk” (COTS, ofta CE-märkt produkt) så förutsätts

att riskreduceringsarbete har utförts enligt tillämpliga lagar och redovisas av tillverkaren i underlaget för CE-märket. För GFE (Government Furnished Equipment) ansvarar Försvarsmakten för motsvarande aktiviteter och underlag.

Integrationsprodukt är en produkt som avses integreras i flera olika tekniska system. Exempel på sådan produkt är radioapparat, laseravståndsmätare, ammunition, inbyggnadselverk och kryptoapparat. För integrationsprodukt ska systemsäkerhetsgodkännandet avse produktens kravställda egenskaper och dess faktiska konfiguration. Detta systemsäkerhetsgodkännande utgör senare en del av det underlag som erfordras för att ta fram systemsäkerhetsgodkännande för det tekniska system i vilket integrationsprodukten ingår.

Integration görs till tekniskt system som svarar mot kravställd förmåga. Härvid integreras erforderliga delar vilka kan utgöras av:

- kommersiell produkt
- GFE (Government Furnished Equipment)
- integrationsprodukt
- befintligt eller nyanskaffat tekniskt system.

Integrationen utförs av DesignA eller leverantör. Vid integrationen genomförs normal systemsäkerhetsverksamhet och DesignA utfärdar systemsäkerhetsgodkännande.

För kommersiell produkt enligt ovan som integreras in i ett tekniskt system, behöver en *särskild systemsäkerhetsanalys* genomföras. Analysens inriktning är att granska att den kommersiella produktens egenskaper i strid, med avseende på att egenskaperna då inte får bli särskilt farliga eller förstärka verkan av fiendens bekämpning av det tekniska systemet. Exempel på sådan egenskap kan vara att ett fordon har drivmedelstank nära passagerarutrymme, innehåller delsystem för säkerhet med explosiv vara (krockkudde/krockgardin).

Då integrationsprodukt utgörs av CE-märkt COTS-produkt analyserar DesignA denna utifrån ställda krav på geografisk miljö/användningsmiljö för det tekniska systemet i syfte att identifiera

om denna uppfyller systemsäkerhetskrav. Det bör vara en strävan att inte upprepa av leverantören redan utfört riskhanteringsarbete.

Om möjligt bör därför systemsäkerhetsanalysen av integrationen mellan tekniskt system och COTS-produkt grundas på genomfört riskanalysarbete för COTS-produkten som redovisats i dess i CE-märkningsunderlag.

5.9 Ammunition

5.9.1 Grunder

I de fall då explosiv vara eller pyroteknisk sats ingår i tekniskt system ska det i DesignA:s systemsäkerhetsgodkännande ingå ett beslut från MSB (Myndigheten för samhällsskydd och beredskap) avseende denna varas säkerhet vid transport och förvaring. Se *avsnitt 2.4.11*.

Ammunition för militärt ändamål är ett särskilt farligt tekniskt system som systemsäkerhetsmässigt alltid ska hanteras i två olika avseenden:

- I sin egenskap av *ammunitionsobjekt*, 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). Ammunitionen utgör här integrationsprodukt.

  Kraven på ammunitionen är att denna ska vara 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 mekaniska och andra påkänningar som följd av avsedd hantering i avsedd miljö.

5.9.2 Systemsäkerhetsgodkännande för ammunition för militärt ändamål

Båda ovanstående aspekter ska täckas in av det separata systemsäkerhetsgodkännande som DesignA alltid ska ta fram för varje enskilt militärt ammunitionsobjekt. Dessutom ska det ingå ett beslut från MSB (Myndigheten för samhällsskydd och beredskap) om godkännande av dessa varors säkerhet vid transport, förvaring och övrig hantering. Se *avsnitt 2.4.11*.

DesignA ska lämna detta systemsäkerhetsgodkännande till Försvarsmakten som tar fram centralt systemsäkerhetsbeslut och beslut om användning för aktuell ammunition i sitt transport- och förvaringsemballage.

5.9.3 Integration av ammunition med tekniskt system

För tekniskt system, vapen och motsvarande, i vilket aktuell militär ammunition ska kunna användas, ska systemsäkerhetsdokumentationen för detta tekniska system uppdateras enligt handbokens princip för integration. Härefter kan förekommande ammunitionsförteckningar uppdateras om att detta vapen respektive motsvarande, är godkänt för skjutning/användning av viss ammunition/ respektive att viss ammunition är kvalificerad att skjutas i visst vapen (och motsvarande för andra typer av tekniska system där ammunition brukas; jämför utläggningsutrustning för stridsvagnsminor).

5.9.4 Militär ammunition med IM-egenskaper

Det tekniska systemet ammunition utsätts för så allvarlig påfrestning vid hög temperatur att explosion kan inträffa. Hög temperatur kan till exempel uppstå vid oavsiktlig brand varvid skada på eget förband och skyddsvärda tillgångar kan uppstå. Eftersom det är egen ammunitions egenskaper som förorsakar/förstärker verkan, så kan denna egenskap mycket väl ses som en systemsäkerhetsbrist.

Motståndskraft hos ammunition mot hög värme, samt mot flera andra typer av stimuli, benämns IM-egenskap (”Insensitive Munitions”).

I vilken omfattning militärt ammunition kan vålla oavsiktlig skada på eget förband eller något annat skyddsvärt, identifieras genom hotanalys. En hotanalys grundas på ammunitionens avsedda användningsmiljö under hela livslängden (transport, förvaring, användning, avveckling) och de stimuli (värme, fall, beskjutning, splitter med mera) som ammunitionen kan komma att utsättas för i denna miljö. Ur denna hotanalys identifieras vilka skador som skulle kunna uppkomma på eget förband och annat skyddsvärt. Om skadorna bedöms som icke tolerabla är det möjligt att ställa krav på att ammunitionen ska ha sådana IM-egenskaper att dessa skador förhindras/begränsas.

Vid konstruktion kan IM-egenskaper med relativt enkla medel konstrueras och byggas in i militär ammunition och dennas förpackning. Om viss ammunition ska ha IM-egenskaper behöver detta kravställas särskilt i TTEM. Se *[4]* och *[44]*.

5.10 Vissa tekniska system och aspekter

5.10.1 Utbildningsmateriel

Vissa tekniska system/produkter avses enbart användas för utbildning/övning, istället för motsvarande skarp förbandsmateriel. Här inräknas alla typer av utbildningsanordningar, från lösskjutningsanordning för handvapen till simulator för stridsflygplan. Särskild systemsäkerhetsanalys behöver genomföras för sådan materiel för att säkerställa att materielens egenskaper (hantering, gränsyta mot operatör samt sätt att svara på operatörsåtgärd) inte avviker från den skarpa förbandsmaterielens egenskaper i alla för kunskap och färdighet väsentliga avseenden. Genom korrekt respons från utbildningsmaterielen motverkas så kallad negativ utbildning.

5.10.2 Ergonomisk utformning

Tekniskt systems skadliga belastning av brukare, fysiskt och psykiskt, behöver alltid analyseras för att identifiera möjliga risker för belastningsskador under förutsägbara användningsförhållanden. Sådana risker för ohälsa motverkas genom en god ergonomisk utformning av tekniskt system.

5.10.3 System av system

System av system bör ses som den högsta nivån av tekniskt system. Det kan anses att system av system inte är något annat än ett stort och komplext tekniskt system. Vanligen specificeras endast enstaka krav avseende viss förmåga, trots att den totala mängden ingående tekniska system möjliggör en rad andra förmågor.

Det är dock väsentligt att säkerställa att denna förmåga kan utövas på ett säkert sätt. På denna systemnivå som på alla andra systemnivåer, säkerställs detta genom att tillämpa Försvarsmaktens systemsäkerhetsmetodik.

En sådan ny konfiguration omfattar ofta redan systemsäkerhetsgodkända tekniska system. Detta kan utgöra grund för fortsatt systemsäkerhetsverksamhet. Fokus för systemsäkerhetsverksamheten är här att granska integrationen mellan ingående tekniska system då dessa tillsammans levererar avsedd förmåga.

Ett motsvarande synsätt tillämpas vid internationell insats för att bereda samverkan med utländska förbands ingående tekniska system.

5.10.4 Språk

Instruktioner, manualer och varningstexter avsedda för operatör ska utformas på svenska, engelska eller enligt särskilda krav, från till exempel RMS eller RML.

Språket i beslutshandlingarna: systemsäkerhetsgodkännande, centralt systemsäkerhetsbeslut och beslut om användning ska alltid vara svenska.

Vid köp av färdig produkt utomlands är det inte självklart att få all dokumentation på svenska av leverantören. DesignA ansvarar för att specificera krav på dokumentation och säkerställer att erforderliga dokument översätts till svenska.

I de fall att instruktioner, manualer och varningstexter avsedda för operatör ska översättas till svenska är det alltid aktuell leverantör av det tekniska systemet som ska ansvara för denna översättning.

I den svenska versionen ska finnas angivet att den utgör en översättning och från vilket språk. Den utländska versionen ska ingå i den produktdokumentation som levereras till DesignA.

Språk för teknisk dokumentation specificeras i TTEM. Bedöms den tekniska personal som ska underhålla systemet ha erforderliga kunskaper i teknisk engelska kan engelska väljas som språk för teknisk dokumentation och risklogg. I annat fall ska svenska väljas som språk.

I de fall engelska väljs som språk för teknisk dokumentation ska kravställaren specificera lägstanivå för den tekniska personalen enligt i utbildningen vedertagen NATO-standard eller annan etablerad standard.

5.10.5 Ledningssystem och vapensystem

Grunder

Olika tekniska system innehåller varierande mängd av riskkällor/farliga tillstånd. Systemsäkerhetsverksamhet genomförs med syftet att identifiera och hantera förekommande olycksrisker.

Teoretiskt kan det inträffa att efter genomförd systemsäkerhetsverksamhet det konstateras att ett visst ledningssystem helt saknar riskkällor/farliga tillstånd. Är det då självklart ”riskfritt” att integrera detta ledningssystem med ett visst vapensystem? Svaret är nej.

Vägledande synsätt

Ledningssystems funktion är att ge ledningsinformation till ett applikationssystem. Detta utgörs vanligen av olika vapensystem.

Varje vapensystem innehåller risk för att vapnet utlöses oavsiktligt eller riktas/utlöses mot oavsiktligt mål. Systemsäkerhetsmässigt är detta risker som tillhör vapensystemet. Om felaktighet i ledningsdata (eldledning/stridsledning) kan utlösa en sådan risk ska detta ses och behandlas som en systemsäkerhetsrisk hos vapensystemet. För ledningssystemets vidkommande hanteras detta som ett prestandakrav med visst kvalitetsmått på tillförlitlighet och tillgänglighet hos ledningsdata.

> Ovanstående synsätt innebär att ledningssystem och vapensystem endast redovisar sina egna olycksrisker. Följden är att systemsäkerhetsgodkännandet inte kräver specificering av vilka skjutande enheter ledningssystemet kan lämna ledningsdata till, respektive att vapensystemet inte begränsas av från vilka olika ledningssystem det kan ta emot ledningsdata.

För tekniskt system respektive teknisk produkt inom ledningssystemområdet som inte är avsett att integreras i vapensystem eller att användas för fältbruk, tillämpas *avsnitt 5.10.8 Fristående användning av civil materiel*.

5.10.6 Fordonssystem

Inom ramen för fordonssystem förekommer flera former för systembyggande. Detta är föranlett av att fordon är dyra, tillverkarna har ett marknadsintresse av att erbjuda ny och anpassad teknik förpackad i ändamålsenliga fordonsformer samtidigt som Försvarsmaktens behov snabbt förändras över tiden. En anpassad tillämpning av gällande regelverk underlättar Försvarsmaktens verksamhet, samtidigt som krav på säkerhet inte åsidosätts. *Tabell 5:1* nedan avser ge en sammanfattning över förekommande systembyggnadsformer och anpassad regeltillämpning.

Tabell 5:1 Regeltillämpning vid olika alternativ för fordonsanskaffning

Fordonstyp	Godkännande
Specialfordon (även MOTS)	Systemsäkerhetsgodkännande + registreringsbesiktning + CSSB → BOA
Standardfordon (COTS)	Tillverkarintyg/enskilt godkännande → BOA (ej CSSB)
Standardfordon (COTS) + civilt tillägg (COTS)	Befintligt typgodkännande för fordonet + typgodkännande för tillägget → BOA (ej CSSB)
Standardfordon (COTS) + mil tilllägg	Befintligt typgodkännande för fordonet + befintligt BOA + Systemsäkerhetsgodkännande av tillägget + Systemsäkerhetsgodkännande av integrationen
	CSSB → BOA (för tillägget och integrationen, det vill säga inget nytt systemsäkerhetsarbete på själva fordonet mer än som erfordras för att systemsäkerhetsanalysera integrationen)

5.10.7 Expertsystem

Bakgrund

Försvarsmaktens verksamhet kännetecknas av ett internationellt engagemang med krav på att med kort förvarning kunna verka på vitt skilda arenor. Detta ställer bland annat krav på tillgång till betydligt större kunskaper än tidigare. Kunskaperna måste vara uppdaterade och avse olika aspekter, såsom motståndarens taktik, organisation, materiel och stridsmiljö. Kunskaper krävs för att kunna fatta snabba taktiska beslut. Men också beslut på lägsta tekniska systemnivå förutsätter tillgång till kvalificerad information. Exempel härpå är röjning av minor och IED (Improvised Explosive Device).

En lösning på behovet av snabb tillgång till kvalificerad detaljinformation är expertsystem, ibland kallat beslutsstödsystem. Detta är ett datorprogram som besvarar frågor från användaren genom att dra slutsatser baserade på en samling regler och i förväg lagrade fakta. Expertsystem brukar räknas till kategorin program med artificiell intelligens. Syftet med expertsystem är att efterlikna rådgivning från en människa med mycket erfarenhet på området. Exempel på expertsystem är program för sjukdomsdiagnos som utifrån patientens symptom och bakgrund (ålder, kön, yrke, sjukdomar i släkten med mera) hjälper läkaren genom att ge förslag på möjliga sjukdomar med gradering efter sannolikhet och/eller farlighet.

En framtida teknik för att skapa expertsystem kallas neurala nätverk. Detta är ett samlingsnamn på sådana algoritmer för informationsbehandling som försöker efterlikna funktionen i nervceller och hjärnor.

Algoritmer som bygger på neurala nätverk kan ofta lösa problem som är svåra att hantera med konventionella datalogiska metoder. Exempel på tillämpningar är: mönsterigenkänning, signalbearbetning, reglerteknik, prognoser, självorganisering, problem med många bivillkor, schemaläggning.

Expertsystem och systemsäkerhet

De normala riskkällor som finns i expertsystemet och som kan förorsaka personrisker, ska vara omhändertagna av tillverkaren av den kommersiella datorutrustning som expertsystemet är ”förpackat” i. Några andra olycksrisker kan inte finnas så länge som expertsystemet inte är fysiskt förbundet med tekniskt materielsystem.

Expertsystemets felaktigheter begränsar sig till informationsbrister, korrupt information, rent felaktig information samt hemlig information som kommer på avvägar. Dessa brister kan ge upphov till ”security”-förluster men också missleda operatören så att olyckshändelse kan uppstå vid hantering av det objekt som expertsystemet beskriver.

Operatören kan själv förorsaka en olycka i sin kontakt med det objekt som expertsystemet beskriver, genom att operatören:

- missförstår informationen
- inte tillämpar informationen på avsett sätt
- är klumpig vid utförandet av korrekta handgrepp
- använder felaktigt verktyg
- på annat sätt avviker från rätt åtgärd och därmed inte uppnår avsett resultat på ett säkert sätt.

Om av olika skäl (till exempel extremt höga krav på tid) en konstruktion väljs, där expertsystemet integreras med eget tekniskt system tillkommer ett antal aspekter att hantera systemsäkerhetsmässigt, bland annat:

- Hur valideras inlärningsrelaterade system (neurala nätverk)?
- När kan full autonom funktion tillämpas?
- Vari består olycksriskerna?
- Vilka restriktioner och säkerhetsregler erfordras för att hantera identifierade olycksrisker?

5.10.8 Fristående användning av civil materiel

Generellt

H SystSäk är inte tillämplig för anskaffning och fristående användning av civil materiel utanför tekniskt system.

Civil standardmateriel

Civil materiel kan utgöras av utrustning till kontorsmiljö i fredsorganisationen, skolsalar, matsalar med mera. Om denna materiel inte omfattas av lag eller författning med militärt undantag (jämför *avsnitt 1.2*) erfordras inte heller någon systemsäkerhetsverksamhet. Inte heller ska något systemsäkerhetsbeslut tas fram.

Beslut om att systemsäkerhetsverksamhet enligt H SystSäk inte ska genomföras och att inget systemsäkerhetsbeslut ska tas fram, fattas av ÄF vid initiering av anskaffning. Detta dokumenteras i anskaffningsbeslutet. Beslutet ska också klargöra att materielen inte får användas integrerat med militärt tekniskt system.

I det särskilda fall att Försvarsmakten behöver fatta beslut om användning (BOA) för sådan civil standardmateriel/produkt, kan BOA, vad avser krav på CSSB, utfärdas på det underlag som möjliggjorde marknadsföring av den civila standardmaterielen/produkten.

Om civil standardmateriel/produkt avses integreras i tekniskt system gäller bland annat *avsnitt 5.6–5.8* ovan.

5.10.9 Fristående anskaffning av civila handvapen (COTS) respektive civil ammunition (COTS)

Generellt

Civil materiel kan utgöras av civila handvapen (COTS) samt civil ammunition (COTS) som avses användas i enlighet med tillverkarens bruksanvisning. Beslut om att systemsäkerhetsverksamhet enligt H SystSäk inte erfordras för sådan materiel, fattas av ÄF vid initiering av anskaffning. Beslutet dokumenteras i anskaffningsbeslutet. Beslutet ska också klargöra att materielen inte får användas integrerad med militärt tekniskt system eller för militärt ändamål (bekämpning av humanmål).

Om civila handvapen och civil ammunition avses integreras i tekniskt system gäller bland annat *avsnitt 5.6–5.8* ovan.

Handvapen av civil standardkaraktär (COTS)

Civilt handvapen som förekommer i handeln (COTS) och är försett med CIP-stämpel är godkänt att användas i enlighet med tillverkarens bruksanvisning. Sådant handvapen erfordrar inte särskild systemsäkerhetsverksamhet. Eventuellt beslut om användning kan, vad avser krav på systemsäkerhet, utfärdas på det underlag som möjliggjorde marknadsföring av produkten.

I det fall att TTEM fastställs för anskaffning av COTS-vapen anges i detta, dels att anskaffningen ska avse civilt vapen (CIP-märkt) för civilt bruk vid Försvarsmakten och att ingen särskild systemsäkerhetsverksamhet ska genomföras, dels att vapnet inte ska klassas som krigsmateriel.

Det är dock viktigt att den avsedda användningen av vapnet verkligen är att anse som civil. Om vapnet avses användas för militärt ändamål (bekämpning av humanmål) ställer förordningen om folkrättslig granskning av vapenprojekt *[16]* krav på att vapnet ska anmälas till och godkännas av Delegationen för folkrättslig granskning av vapenprojekt.

Handvapenammunition av civil standardkaraktär (COTS)

Civil handvapenammunition som förekommer i handeln (COTS) och är försedd med CIP-stämpel, är därigenom godkänd för hantering i Sverige vad avser lagen om brandfarliga och explosiva varor *[28]*. Sådan ammunition erfordrar ingen särskild systemsäkerhetsverksamhet. Eventuellt beslut om användning kan, vad avser krav på systemsäkerhet, utfärdas på det underlag som möjliggjorde marknadsföring av produkten.

I anskaffningsbeslut/TTEM för anskaffning av COTS-ammunition fastställs dels att anskaffningen ska avse civil ammunition (CIP-märkt) för civilt bruk i Försvarsmakten, dels att ingen särskild systemsäkerhetsverksamhet ska genomföras, samt att ammunitionen inte ska klassas som krigsmateriel.

Det är dock viktigt att den avsedda användningen av ammunitionen är att anse som civil. Om ammunitionen avses användas för militärt ändamål (bekämpning av humanmål) ställer förordningen om folkrättslig granskning av vapenprojekt *[16]* krav på att ammunitionen ska anmälas till och godkännas av Delegationen för folkrättslig granskning av vapenprojekt.

COTS-ammunition (CIP-märkt) som avses förvaras i Försvarsmaktens ammunitionsförråd tillsammans med militär ammunition, erfordrar dock alltid enligt IFTEX *[21]* en särskild militär förvaringskod (F-kod) som reglerar hur militär förvaring får lov att ske. F-kod erhålls genom hänvändelse till FMV.

5.11 Besluts- och produktdokument under insats

5.11.1 Grunder

Detta avsnitt är tillämpbart på alla typer av förband och tekniska system, oavsett om systemet är mark-, sjö- eller luftburet.

Avsnittet avser enbart att ge stöd för systemsäkerhetsöverväganden i samband med att tillämpningsbestämmelser för förband tas fram som reglerar rätt att genomföra teknisk anpassning, tillfällig reparation, krigsskadereparation respektive annan åtgärd under insats.

5.11.2 Teknisk anpassning

Teknisk anpassning av tekniskt system utförs i syfte att öka möjligheterna till framgång i strid. Verksamma medel utgörs dels av att öka verkan av eget tekniskt system, dels av att reducera verkan av motståndarens åtgärder. Härigenom förbättras möjligheten till överlevnad för egna styrkor och egen personal.

Kraven på ledtid från identifierat behov av anpassning till effektuering är oftast kort vilket innebär att ordinarie rutin för ändring av konfiguration, inte kan tillämpas.

Systemsäkerhetsbedömning ingår i beslutsunderlaget för teknisk anpassning.

Tillämpningsbestämmelser för teknisk anpassning bör ur systemsäkerhetssynvinkel omfatta följande:

- beslutsrätt
- minimikrav på riskanalys, inklusive bedömningsmall (exempel, se *bild 6:1*, dock att en ruta ska vara röd och övriga gröna)
- krav på beslutsunderlag (inträffad händelse/ skada/trend, alternativa möjliga åtgärder, för- och nackdelar med respektive alternativ)
- minimikrav på dokumentation av genomförd åtgärd
- minimikrav på dokumentation till brukare

- till vem rapport över genomförd åtgärd för tekniskt system (viss systemindivid) ska ställas
- när och hur beslut tas om återställande av tekniskt system
- till vem rapport ska ställas om att tekniskt system (viss systemindivid) återställts efter teknisk anpassning.

5.11.3 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, ta sig ur en farlig situation/område eller ta sig till kvalificerad reparationsresurs. Tillfällig reparation/krigsskadereparation är alltid ett andrahandsval och ska endast användas i lägen då ordinarie rutiner/resurser för avhjälpande underhåll/omhändertagande inte kan användas, och utförd reparation ska så snart läget medger ersättas av en med verifierade metoder utförd reparation.

Tillfällig reparation/krigsskadereparation kan utföras av såväl besättning (brukare) som av teknisk personal. Komplexiteten i möjliga reparationer skiljer sig dock åt beroende av utrustning och kompetens. Endast personal med särskild utbildning, är behörig att utföra tillfällig reparation.

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. Reparationen är oftast improviserad, utförs med okonventionella reparationsmetoder, och omfattar normalt endast att det absolut nödvändigaste åtgärdas (möjliggöra verkan och skydd). Systemsäkerheten bör om möjligt **beaktas** vid utförande av krigsskadereparation.

Resultatet av krigsskadereparation är ofta att del av funktionen/skyddsförmågan har kunnat återtas.

Tillämpningsbestämmelser för tillfällig reparation respektive krigsskadereparation bör ur systemsäkerhetssynvinkel omfatta följande:

- beslutsrätt
- krav på beslutsunderlag (inträffad händelse/ skada/trend, alternativa möjliga åtgärder, för- och nackdelar med respektive alternativ)
- minimikrav på riskanalys, inklusive bedömningsmall (exempel, se *bild 6:1*, dock att vid krigsskadereparation en ruta ska vara röd och övriga gröna)
- minimikrav på dokumentation av genomförd åtgärd
- minimikrav på dokumentation till brukare
- till vem rapport över genomförd åtgärd för tekniskt system (viss systemindivid) ska ställas
- när och hur beslut tas om återställande av tekniskt system
- till vem rapport ska ställas om att tekniskt system (viss systemindivid) återställts efter tillfällig reparation/krigsskadereparation.

5.11.4 Annan åtgärd

Också annan åtgärd än teknisk anpassning, tillfällig reparation och krigsskadereparation avseende tekniskt system kan övervägas, i syfte att öka möjligheterna till framgång i strid. Exempel härpå skulle kunna vara lokalt snabbanskaffat kompletterande tekniskt system.

Kraven på ledtid från identifierat behov till effektuering är oftast kort vilket innebär att ordinarie rutin för avsedd åtgärd, inte kan tillämpas.

Systemsäkerhetsbedömning ingår i beslutsunderlaget för sådan annan åtgärd.

Tillämpningsbestämmelser för ”Annan åtgärd” bör ur systemsäkerhetssynvinkel omfatta följande:

- beslutsrätt
- krav på beslutsunderlag
- minimikrav på riskanalys, inklusive bedömningsmall (exempel, se *bild 6:1*), dock att vid annan åtgärd en ruta ska vara röd och övriga gröna)
- minimikrav på dokumentation av genomförd åtgärd
- minimikrav på dokumentation till brukare
- till vem rapport över genomförd åtgärd ska ställas
- när och hur beslut tas om återställande/avveckling/fortsatt användning av tekniskt system
- till vem rapport ska ställas om att tekniskt system (viss systemindivid) återställts/avvecklats, med mera efter Annan åtgärd.

5.12 Kvalitetskontroll/granskning

5.12.1 Granskning

Före leverans av tekniskt system genomförs normalt någon form av kvalitetskontroll. Skälet är att DesignA måste kontrollera att beställd produkt uppfyller ställda tekniska krav inklusive prestanda och att kravställda verksamhetsåtaganden är utförda på avsett sätt.

Det är minst lika viktigt att dokument som redovisar utförd systemsäkerhetsverksamhet och dess resultat, granskas på motsvarande sätt.

Granskning utförs vid ett antal olika tillfällen (jämför *avsnitt 7.3.4 Styrning av leverantör*). Aktiviteten avser att på ett systematiskt sätt granska framtagna dokument och ska alltid ha syftet att redovisa hur och i vilken omfattning ställda systemsäkerhetskrav har uppfyllts.

Granskning kan utföras av vem som helst inom ett visst projekt.

5.12.2 Oberoende granskning

Utöver Granskning finns även formen Oberoende granskning. Denna form förutsätter att granskaren inte tillhör projektet eller i övrigt är anlitad av projektet (”oberoende”).

Oberoende granskning tillämpas främst i följande fall:

- När teknikområdets risker generellt kan anses som stora/allvarliga (till exempel ammunition, flygsystem, starkt oxiderande ämnen, allvarligt miljöfarliga ämnen).
- När anskaffning sker av tekniskt system som bygger på ny teknologi och andelen okända olycksrisker befaras vara relativt hög. I detta fall torde även möjliga systemrisker vara mindre kända och svåra att identifiera.
- När anskaffning sker av tekniskt system som utgör ny tillämpning av befintlig teknik och andelen okända olycksrisker befaras vara relativt hög.

När däremot anskaffning avses ske av tekniskt system där erfarenheter finns från såväl tidigare upphandling, aktuell teknik samt från Försvarsmaktens brukande av liknande tekniskt system, kan andelen okända olycksrisker antas vara relativt låg. Även övergripande systemrisker kan här antas vara kända. Om flera av dessa förutsättningar gäller, kan behovet av oberoende granskning anses vara litet.

5.12.3 Granskningsrapport

Resultat av granskning (båda ovanstående typer) ska alltid redovisas i en rapport som förses med en särskild sammanfattning vilken entydigt redovisar om granskat dokument uppfyller, eller inte uppfyller, ställda krav på systemsäkerhet.

Rapporten ska också innehålla förslag om åtgärder som erfordras med anledning av granskningsresultatet. Granskningsrapport ska alltid biläggas DesignA:s systemsäkerhetsgodkännande.

6 FÖRSVARSMAKTENS SYSTEMSÄKERHETSVERKSAMHET

6.1 ÖVERGRIPANDE LEDNING

ÖB har ett övergripande ansvar för de tekniska system som används i Försvarsmakten. Dels ska systemen ha erforderliga egenskaper för genomförande av strid, dels ska systemens olycksrisker vara så låga att de inte förorsakar oavsiktlig skada på person, egendom eller yttre miljö.

Krav på de tekniska systemens säkerhetsegenskaper anges i svensk lag. Aktuella lagar och deras tillämplighet avseende militära tekniska system redovisas i *kapitel 2*.

Försvarsmaktens Handbok systemsäkerhet som redovisar Försvarsmaktens systemsäkerhetsmetodik, är framtagen för att säkerställa att dessa lagar efterlevs.

För att säkerställa att systemsäkerhetsmetodiken tillämpas på rätt sätt krävs kompetens hos envar som hanterar systemsäkerhetsfrågor. De åtgärder ÖB genomför för att uppnå detta anges nedan.

ÖB ledningsåtgärder:

- Vidmakthåller och utvecklar den specifika metodik som systemsäkerhetsverksamheten utgör.
- Utser central verksamhetsutövare i Försvarsmakten och delegerar till denne att ansvara för verksamhetssäkerhetsprocess och systemsäkerhetsprocess inom Försvarsmakten.
- Uppdrar åt C SÄKINSP att teckna samråd på genomförd systemsäkerhetsverksamhet och utöva tillsyn över tillhörande arbetssätt (processer) samt besluta föreskrifter, instruktioner och handböcker om systemsäkerhet inom Försvarsmakten.

- Överenskommer (vanligen genom samordningsavtal) med stödjande myndighet att denna åtar sig rollen som designansvarig (DesignA) för vissa teknikområden och efterlever Försvarsmaktens föreskrifter, instruktioner och handböcker för systemsäkerhet samt att härvid långsiktigt upprätta och vidmakthålla designregelsamling inom dessa teknikområden.
- Utser vid behov visst tekniskt centrum inom Försvarsmakten med särskilt hög kompetens att också ta rollen som designansvarig (DesignA) för visst teknikområde samt att härvid långsiktigt upprätta och vidmakthålla designregelsamling inom detta teknikområde.

6.2 Vision

Ingen person (soldat, sjöman, officer eller civil) ska skadas av Försvarsmaktens tekniska system.

Inte heller ska egendom eller yttre miljö skadas.

6.3 Ledning

6.3.1 Genomförande av systemsäkerhetsverksamhet

Instruktion om Försvarsmaktens handbok systemsäkerhet 2011 *[26]* anger att vid all anskaffning, modifiering, renovering och avveckling av materiel från 1 januari 2011, ska beslut tas om och i vilken omfattning systemsäkerhetsverksamhet ska genomföras i enlighet med H SystSäk.

Systemsäkerhetsverksamhet erfordras för varje tekniskt system särskilt konstruerat och framtaget för militär användning.

Med tekniskt system förstås även sådant tekniskt system som har skapats genom integration av tekniska system, delar ur sådana och/eller andra produkter (såväl MOTS som COTS).

Systemsäkerhetskrav ställs för ett tekniskt systems hela livslängd.

Systemsäkerhetsverksamhetens omfattning och detaljeringsgrad anpassas till det tekniska systemets komplexitet och dess bedömda olycksrisker vid hantering.

ÄF i HKV leder och genomför systemsäkerhetsverksamhet under tekniskt systems hela livslängd. Styrinstrument är bland annat krav avseende högsta tillåtna nivå på enskild risk (= tolerabel risknivå) i tekniskt system samt att fortlöpande säkerställa att denna nivå inte överskrids.

För tekniskt system som innehas av Försvarsmakten fördelar ÄF ansvar att följa upp risker och föreslå/vidta riskreducerande åtgärder. Ansvaret för respektive tekniskt system fördelas till lämplig organisation. Ansvaret omfattar också att vidmakthålla det tekniska systemets riskdokumentation.

ÄF låter också ta fram och vidmakthålla centralt systemsäkerhetsbeslut (som utgör underlag för beslut om användning, BOA).

Den systemsäkerhetsverksamhet som generellt erfordras vid HKV för materielsystem, bör lämpligen analyseras av ÄF i HKV. Vidare bör ÄF besluta innehåll, ansvarsförhållanden, delegeringar, kravnivåer med mera. Överväganden och beslut kan dokumenteras i en särskild plan SSMP, som delges berörda. (Se *H SystSäk del 2 avsnitt 5.1*, aktiviteten SSP som resulterar i SSMP.)

Den systemsäkerhetsverksamhet som planeras för ett eller flera materielsystem eller grupp av materielsystem, bör lämpligen analyseras och planeras av ÄF i HKV. Planen benämns SSMP (se ovan) och utgör grund för fortsatt styrning av systemsäkerhetsverksamheten för aktuella tekniska system. Planen kan innehålla underlag för såväl nyanskaffning som vidmakthållande.

ÄF inriktar systemsäkerhetsverksamheten hos DesignA bland annat genom att vid beställning ställa systemsäkerhetskrav.

I följande avsnitt av kapitel 6 redovisas krav som kan användas vid ÄF styrning av DesignA.

Kraven är numrerade enligt följande exempel:

2.641.01, där 2 = H SystSäk Del 1, 641 = avsnittsnummer och de två sista siffrorna är ett löpnummer inom avsnittet.

Kravnummer med fet stil = obligatoriskt krav, resterande krav är valbara. Försvarsmakten kan lägga beställningar där inte alla obligatoriska krav är tillämpbara.

Valbara krav kan väljas av Försvarsmakten då så bedöms lämpligt för aktuellt tekniskt system.

Kraven till DesignA ställs endera i Försvarsmaktens beställning till DesignA (kundbeställning, KB) eller i TTEM. För varje krav redovisas här anges om detta bör ingå i KB eller TTEM.

6.3.2 Basresurser för drift av tekniskt system

Tekniska basresurser som el, kraft, värme, kyla, ventilation, vatten och avlopp är ofta nödvändiga för att möjliggöra funktion och drift av tekniskt system.

För tekniskt system som används mobilt ingår dessa basresurser oftast i aktuell plattform; fartyg, helikopter eller fordon. Mobila basresurser kan även byggas in i container avsedd för fältmässigt bruk men med lägre krav på rörlighet.

I det fall att Försvarsmakten kräver att det tekniska systemet ska ges fast gruppering och mer kvalificerat skydd, tillgodoses detta ofta genom en anläggning. I anläggning är det ofta lämpligt att tillhandahålla anläggningstekniska basresurser som el, kraft, värme, kyla, ventilation, vatten och avlopp. Framtagning av denna typ av resurser hanteras genom beställning från Försvarsmakten till FORTV som har rollen som DesignA för anläggningar. Genom tidigt samråd med aktuell DesignA för det tekniska systemet säkerställs att i beställning till DesignA för anläggningen, krav ställs så att dessa basresurser dimensioneras och i övrigt ges rätt egenskaper och gränsytor för att korrekt kunna stödja aktuellt tekniskt system.

Exempel på ovanstående är det tekniska systemet kammaranläggning för dykeriverksamhet (anskaffas av FMV), som för rätt funktion behöver försörjning med olika gaser. Härvid framtas gassystem och kompressorer av FORTV.

För ubåtsverksamheten krävs vidare batteriladdningsstation (anskaffas av FMV). För att ladda och hantera batterier i anläggningen behövs lyftanordningar och elanslutning (traverser och elanslutningar produceras av FORTV).

Försvarsmakten förutsätts härvid från DesignA för aktuellt tekniskt system, inhämta tekniska specifikationer för att i beställning till FORTV kunna kravställa rätt egenskaper hos de anläggningstekniska basresurserna. DesignA bör också uppmanas att ange om någon basresurs är säkerhetskritisk och därför behöver säkras på särskilt sätt för att minska olycksrisk till tolerabel nivå.

Systemsäkehetskrav

2.632.01	Redovisa teknisk specifikation av basresurser, avseende aktuellt tekniskt system, så att Försvarsmakten i beställning till FORTV, kan beställa rätt egenskaper hos de anläggningstekniska basresurserna. (Anges i KB). Ange särskilt om någon basresurs är säkerhetskritisk och därför behöver säkras på särskilt sätt.

6.4 Studier

6.4.1 Generellt

Utgångskrav för studier utgörs vanligen av att Försvarsmakten ställt krav på viss förmåga. Ofta tas flera alternativa koncept fram för att möjliggöra modellering av vilket koncept som bäst kan anses uppfylla ställda krav. För dessa koncept ska övergripande systemsäkerhetsanalys genomföras. Syftet är att undvika alternativ vars olycksrisker inte kan hanteras säkert och kostnadseffektivt.

Försvarsmakten har under en lång följd av år upparbetat omfattande erfarenhet om olycksrisker i tekniska system, bland annat grundat på rapporter om inträffade tillbud och olyckor.

Systemsäkerhetsverksamhet under studiefasen styrs och kravställs så att erfarenheter från tidigare tekniska system tas till vara.

Vid Försvarsmaktens kravställning utgör systemsäkerhetsmetodiken ett kraftfullt verktyg för att överföra och tillämpa tidigare erfarenheter på nya tekniska system.

Verktyget hanteras genom att vid kravställning för nytt tekniskt system, ställa krav på att:

- tidigare tekniskt systems förteckning över olycksrisker införlivas med studiematerialet
- nya olycksrisker identifieras och analyseras
- systemrisker identifieras och förslag till motåtgärder tas fram.

Tidigt i studiefasen är det tillräckligt att identifiera riskkällor och farliga tillstånd och att analysera dessas natur. Att undvika en riskkälla respektive ett farligt tillstånd är av stor betydelse trots att tillgång till sannolikheter och exponeringsdata saknas i de tidiga faserna.

Riskhanteringsarbetet blir extra effektivt om det påbörjas redan tidigt under studiefasen. Målet är att redan på konceptstadiet skapa sådan kunskap om nya systemlösningar, att en systemsäkerhetsmässig bedömning kan göras och utmönstring kan ske av alternativ som bedöms som säkerhetsmässigt svårhanterliga eller undermåliga.

När Försvarsmakten överväger olika alternativ för hur viss förmåga kan materialiseras (systemutformning) ska fortlöpande studierapporter tas fram för aktuellt objekt (kan ingå i spelkort) och en noggrann systemsäkerhetsanalys göras där olika alternativa studierapporter (spelkort) jämförs. Konsekvent bedriven leder denna verksamhet till hög säkerhet och låg kostnad över avsedd livslängd.

6.4.2 Krav vid studieuppdrag

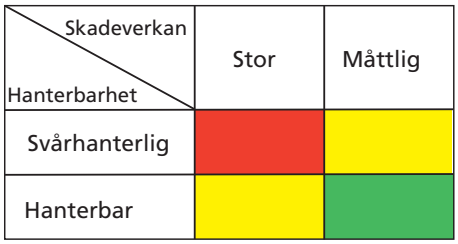
ÄF inriktar och målstyr systemsäkerhetsverksamheten vid genomförande av **studie** eller framtagning av **spelkort** för viss funktion, genom att dels specificera förutsättningar, dels ställa systemsäkerhetskrav.

Förutsättningar för studie/spelkort

- Det tekniska system där objektet avses ingå som tekniskt delsystem.
- Funktion som effektueras genom att samordnat meranvända tekniskt delsystem och produkter från redan befintliga tekniska system (enligt principen system av system).
- I vilket eller vilka tekniskt system som objektet i övrigt ska kunna ingå i, respektive samfungera med, (också vid internationell insats).
- Hur objektet ska kunna användas.
- I vilka fysiska miljöer objektet ska kunna användas.

Systemsäkerhetskrav

2.642.01	Identifiera det tekniska systemets systemrisker i enlighet med generell beskrivning i *avsnitt 4.2.2* (Anges i KB om studieuppdrag) Vid utformning av detta krav jämför *avsnitt 4.2*.
2.642.02	Identifiera och utforma principiellt specifika systemsäkerhetsegenskaper/systemsäkerhetsåtgärder som kan motverka identifierade systemrisker (Anges i KB om studieuppdrag). Vid utformning av detta krav jämför *avsnitt 6.5.3*.
2.642.03	Identifiera olycksrisker i det framstuderade tekniska systemet. (Anges i KB om studieuppdrag.)
2.642.04	Riskbedömning ska utföras med hjälp bifogad bedömningsmall. (Anges i KB om studieuppdrag.)



Stor/Måttlig avser den direkta skadeverkan hos viss riskkälla/ farligt tillstånd

Svårhanterlig/Hanterbar avser bedömd möjlighet att inom ramen för avsett tekniskt system "konstruera" in riskkällan i systemet på ett sådant sätt att den enskilda olycksrisken kan bli liten.

Bild 6:1 Bedömningsmall för studiefas

Vid en realiserbarhetsstudie läggs tyngdpunkten på att uppnå funktionsmålen och där det är relevant, att välja mellan konkurrerande alternativa konstruktioner.

Risklogg ska tas fram och omfatta känd information om tekniskt system och dess identifierade olycksrisker (jämför *bilaga 2*).

> Händelser eller fenomen som var förutsägbara redan vid konstruktionsskedet orsakar erfarenhetsmässigt huvuddelen av alla olyckor. Olycksrisker identifierade så här tidigt kan studeras och hanteras effektivare än de som framkommer senare under tekniskt systems livslängd.

Rangordning: Framtagna alternativ kan prioriteras och rangordnas ur ett systemsäkerhetsperspektiv med hjälp av aktivitet systemsäkerhetsvärdering (SSE)-S10, se *H SystSäk del 2 avsnitt 5.2*.

6.5 Anskaffning

6.5.1 Generellt

Försvarsmakten ställer krav på tekniskt system i TTEM. Grunder och struktur för kravställning framgår av H MÅL *[25]* som hänvisar till H SystSäk vad avser systemsäkerhetskrav.

De åtgärder som ska utföras av Försvarsmakten som en del av vidmakthållande och användning av ett visst tekniskt system för att vidmakthålla systemsäkerheten, samt för att undvika olyckor förorsakade av risker, regleras med instruktioner, handböcker, reglementen, materielbeskrivningar och tekniska order. Försvarsmakten reglerar framtagning av denna information i kundbeställning (KB) till DesignA.

6.5.2 Krav i KB på DesignA:s systemsäkerhetsverksamhet

Följande verksamhetskrav bör övervägas ingå då Försvarsmakten ställer krav på DesignA:s systemsäkerhetsverksamhet. Utvalda systemsäkerhetskrav tas in i Försvarsmaktens kundbeställning (KB) till DesignA.

Systemsäkerhetskrav

2.652.01	Säkerställ att leverantör genomför systemsäkerhetsverksamhet, så att det tekniska systemets olycksrisker hålls inom kravställd risknivå, samtidigt som det levererar krävd förmåga. (Anges i KB.)
2.652.02	**Militärt undantag** (Se *avsnitt 1.2* och *2.4.1*) Säkerställ att leverantör i anbud på visst tekniskt system, utförligt redovisar svensk lag/föreskrift med tillämpning på aktuellt tekniskt system, och som innehåller någon typ av undantag för militär materiel/militär användning/motsvarande. Om lagen/föreskriften meddelar gränsvärden för civil verksamhet (motsvarande) ska leverantören under anbudstiden begära komplettering avseende Försvarsmaktens krav på aktuella gränsvärden, så att anbudet kommer att grundas på rätt förutsättningar. (Anges i KB.)
2.652.03	Leverera systemsäkerhetsgodkännande med redovisning av det tekniska systemets omfattning och gränsytor. Systemsäkerhetsgodkännandet ska, utöver innehåll enligt exempel i *H SystSäk del 2, bilaga 1*, också innehålla följande särkilda avsnitt: xx, yy, zz. Leveransen ska ske xx veckor före leverans av det tekniska systemet. (Anges i KB.)
2.652.04	Leverera fullständig riskdokumentation enligt *avsnitt 5.6*. Leverans ska ske tillsammans med systemsäkerhetsgodkännandet. (Anges i KB.)

2.652.05	Leverera underlag för den utbildning som eventuellt krävs från systemsäkerhetssynpunkt. Leverans ska ske tillsammans med systemsäkerhetsgodkännandet. (Anges i KB.)
2.652.06	Leverera föreskrifter och anvisningar för användning och underhåll (inklusive underlag till SäkI). Leverans ska ske tillsammans med systemsäkerhetsgodkännandet. (Anges i KB.)
2.652.07	Vid utformning av för aktuellt tekniskt systems avvikelsehanteringsrutiner, ska Försvarsmaktens avvikelsehanteringssystem xx användas. (Anges i KB.)
2.652.08	Det tekniska systemets dokumentation får/ska avfattas på svenska/engelska. (Anges i KB.) Vid utformning av detta krav se också *avsnitt 5.10.4* och infoga tillämpligt alternativ för aktuella delar av dokumentationen.
2.652.09	Särskild granskning (kvalitetskontroll) ska genomföras av delsystem yy/produkt zz och ska redovisas med särskild granskningsrapport. (Anges i KB.) Vid utformning av detta krav se *avsnitt 5.12* och specificera aktuella systemdelar/produkter.

6.5.3 Krav avseende systemrisk

Olycksrisk på övergripande systemnivå (systemrisk) behöver identifieras och krav behöver ställas på lämplig skyddsåtgärd som motverkar identifierad systemrisk.

Systemrisk utgår från systemets krävda förmåga som oavsiktligt kan utlösas och därvid förorsaka skada. Systemrisk kan ofta identifieras som svar på frågan: Givet systemförmågan, vad får inte denna ställa till med/vad får inte hända?

Specificera systemsäkerhetskrav för aktuell systemrisk, så att systemet ges förmåga att motverka aktuell systemrisk. Sådan förmåga kan antingen utformas att förhindra utvecklingen av den händelsekedja systemrisken består av, alternativt kan krav ställas på att viss ”safety device” ska konstrueras in i systemets grund-

konfiguration. En sådan ”safety device” ska ge en viss säkerställd skyddsegenskap till systemet, jämför *avsnitt 4.2.2*, underavsnittet Systemrisk.

Exempel på sådant inbyggt säkerhetssystem är att ett stridsflygplan utrustas med katapultstol, transportflygplan utrustas med fallskärmar för besättningen, fartyg utrustas med livbåtar, stridsfordon förses med minst två av varandra oberoende utrymningsvägar för besättningen, automatiserat vapensystem med tidsstyrning, manuellt beslut/delbeslut eller fristående automatiserat kontrollsystem.

Systemsäkerhetskrav

2.653.01	Identifiera systemrisker (olycksrisk på systemnivå). (Anges i TTEM.)
2.653.02	Identifiera erforderliga systemsäkerhetsåtgärder för att motverka identifierade systemrisker. (Antingen genom att förhindra utvecklingen av den händelsekedja som utlöser systemrisken eller genom att viss ”safety device” konstrueras in i systemets grundkonfiguration. (Anges i TTEM.)

I det fall att identifiering av systemrisker och erforderliga motåtgärder har inletts redan under studiefasen, grundas här beskrivet arbete på detta resultat (jämför *avsnitt 6.4.2*).

6.5.4 Krav avseende ammunition

Militär ammunition

Här redovisade krav ställs alltid vid anskaffning av militär ammunition (jämför *avsnitt 5.9*).

Systemsäkerhetskrav

2.654.01	Systemsäkerhetsgodkännande för militär ammunition ska avse ammunitionen i dess två olika egenskaper, dels som ammunitionsobjekt, avsett för visst eller vissa vapen eller annan specificerad användning och dels som fristående transport- och förvaringsobjekt. (Anges i KB.)
2.654.02	H SystSäk och H VAS ska tillämpas (Anges i KB.) (H VAS är FMV designregler om ammunitionens säkerhetsegenskaper samt designregler för att innehålla folkrättsliga krav *[16]*. *Likvärdig designregelsamling eller standard kan godtas efter Försvarsmaktens prövning*
2.654.03	Systemsäkerhetsgodkännande för militär ammunition ska innehålla granskningsrapport från en oberoende granskningsfunktion. (Anges i KB.)

Den granskningsfunktion som finns idag vid FMV kan anlitas av Försvarsmakten. Jämför *avsnitt 2.4.11*.

Genom oberoende granskning av ammunitionens konstruktion med mera kontrolleras att ammunitionen uppfyller designregler enligt H VAS samt av Försvarsmaktens ställda krav på risknivå.

Godkännande av militär ammunition för transport och förvaring

Systemsäkerhetskrav

2.654.04	Inhämta godkännande av anskaffad militär ammunition avseende säkerhet vid transport och förvaring från MSB. (Anges i KB.)

Handvapenammunition av civil standardkaraktär (COTS)

Civil handvapenammunition som förekommer i handeln (COTS) och är försedd med CIP-stämpel, är därigenom godkänd att användas i enlighet med tillverkarens bruksanvisning. Sådan ammunition erfordrar inte särskild systemsäkerhetsverksamhet. Eventuellt beslut om användning kan, vad avser krav på systemsäkerhet, utfärdas på det underlag som möjliggjorde marknadsföring av produkten.

Här redovisade krav kan ställas vid uppdrag om anskaffning av civilt handvapenammunition som förekommer i handeln (COTS).

Systemsäkerhetskrav

2.654.05	Anskaffningen ska avse COTS-ammunition. Ammunitionen ska vara CIP-märkt varför ingen särskild systemsäkerhetsverksamhet ska utföras. Ammunitionen ska inte ska klassas som krigsmateriel. (Anges i anskaffningsbeslut.)
2.654.06	Särskild militär förvaringskod (F kod) enligt IFTEX *[21]* ska inhämtas genom hänvändelse till FMV. (Anges i anskaffningsbeslut.) F koden anger hur förvaring i Försvarsmaktens förråd ska ske.
2.654.07	Godkännande av ammunitionen ska inhämtas från Delegationen för folkrättslig granskning av vapenprojekt *[16]*. (Anges i anskaffningsbeslut.) Kravet ställs enbart i det fall att den civila ammunitionen av Försvarsmakten avses användas för militärt ändamål (bekämpning av humanmål).

6.5.5 Krav avseende strålningsemitterande utrustning

Operatör/passagerare kan eventuellt medföra strålningsemitterande utrustning, vilken kan komma att störa anskaffat tekniskt system. Sådan utrustning kan till exempel utgöras av:

- personlig/privat utrustning såsom mobiltelefon, GPS-navigator/mottagare
- förbandsutrustning med motsvarande egenskaper men med högre effekter.

Detta hanteras enklast och mest effektivt genom att i TTEM särskilt specificera viss utrustning och kräva att denna ska omfattas av förekommande systemsäkerhetsanalyser och upptas bland de förnödenheter som redovisas under systemsäkerhetsgodkännandets rubrik ”Det tekniska systemet avses användas tillsammans med”.

På samma sätt hanteras sådana tilläggsutrustningar av COTS-karaktär som ska/kan komma att användas inom ramen för det tekniska systemet (till exempel kaffebryggare, mikrovågsugn, persondator). Krav ställs lämpligen på att specificerade tilläggsutrustningar ska omfattas av förekommande systemsäkerhetsanalyser och upptas bland de produkter som redovisas under systemsäkerhetsgodkännandets rubrik ”Det tekniska systemet avses användas tillsammans med”.

Systemsäkerhetskrav

2.655.01	Följande utrustning ska kunna användas av aktuella operatörer: xx, yy, zz. Utrustningen ska omfattas av förekommande systemsäkerhetsanalyser och upptas bland de förnödenheter som redovisas under systemsäkerhetsgodkännandets rubrik ”Det tekniska systemet avses användas tillsammans med”. (Anges i TTEM.)
2.655.02	Följande förbandsutrustning ska kunna användas inom förbandet: mm, nn, pp. Utrustningen ska omfattas av förekommande systemsäkerhetsanalyser och upptas bland de förnödenheter som redovisas under systemsäkerhetsgodkännandets rubrik ”Det tekniska systemet avses användas tillsammans med”. (Anges i TTEM.)

6.5.6 Krav avseende nytt tekniskt system

Inför anskaffning av nytt tekniskt system behöver ett antal generella förutsättningar samt tekniska krav specificeras i TTEM/TEMU.

Generella förutsättningar:

- Avsedd användning
  - Krävd förmåga – hur och till vad det tekniska systemet ska kunna användas, respektive hur det inte avses kunna användas, till exempel köra max 60 km/tim och inte fortare, kunna lasta maximalt 20 ton, kunna transportera 12 soldater med stridsutrustning. Inte avsett för lastning av styckegods.
  - Krav på uthållighet samt driftsprofil (korrekt systemsäkerhetsverksamhet måste utgå från avsedd användning).
  - Vem som ska vara användare/operatör. Särskilda krav på användargränssnitt (HMI-krav) anges med hänsyn till avsedda lednings- och stridsförhållanden för operatörer, antal operatörer och deras avsedda kompetens.

  - Särskilda krav på ergonomisk utformning anges med hänsyn till avsedda användnings- och stridsförhållanden för operatörer, antal operatörer (till exempel att operatören ska framföra visst fordon med påtagen stridsutrustning och skyddsmask, att ett vapen ska hanteras med påtagna handskar, att operatören ska kunna fortsätta sitt arbete i minst 2 timmar utan uppehåll, utan att ergonomisk belastning uppstår)
  - Geografisk miljö/användningsmiljö.
- Konfiguration
  - Vilka produkter som ingår i det tekniska systemet samt vilka produkter som ska kunna ingå i det tekniska systemet.
  - Vilka andra tekniska system det ska kunna användas tillsammans med, ingå som tekniskt delsystem i, respektive samfungera med, vid till exempel internationell insats.
- Krav på viss säkerhetsegenskap som motverkar av Försvarsmakten identifierad systemrisk.
- Krav på IM-egenskaper hos ammunition.
- Risknivå – krav på den nivå som enskild olycksrisk i ett exemplar av systemet ej får överskrida under avsedd användning (anges i form av riskmatris).

Systemsäkerhetskrav

2.656.01	Ammunitionen ska ha följande IM-egenskaper xx, yy, zz. (Anges i TTEM.) Jämför Försvarsmaktens IM-Policy eller motsvarande styrdokument samt grunder i STANAG 4439 *[44]* och AOP-39 *[4]*).
2.656.02	Det tekniska systemets enskilda skade-/olycksrisker för person, ska inte överskrida tolerabel risknivå enligt bifogad riskmatris för personskada. (Anges i TTEM.)
2.656.03	Det tekniska systemets enskilda skade-/olycksrisker för ekonomisk skada, ska inte överskrida tolerabel risknivå enligt bifogad riskmatris för ekonomisk skada. (Anges i TTEM.)

Särskilda aspekter/krav för vissa militära handvapen

För militärt bruk särskilt anskaffat handvapen som är av civilt ursprung är som regel CIP-stämplat. Detta innebär att CIP-stämplad ammunition automatiskt är certifierad att kunna användas i detta vapen, dock inte för militärt bruk; bekämpning av humanmål. För att möjliggöra detta krävs att Försvarsmakten låter inhämta godkännande av varje enskild ammunitionstyp som avses användas mot humanmål från Delegationen för folkrättslig granskning av vapenprojekt *[16]*.

Vid anskaffning av för militärt bruk särskilt konstruerat och tillverkat handvapen som är av militärt ursprung och inte är CIP-stämplat, kan Försvarsmakten ändå kravställa att DesignA ska certifiera handvapnet för på marknaden förekommande CIP-stämplad ammunition (av angivna typer och passande kaliber). Denna ammunition kommer därmed att ingå i DesignA:s systemsäkerhetsgodkännande. Krav bör härvid också ställas på DesignA att framta F-kod för aktuella ammunitionstyper (se *avsnitt 5.10.9* sista stycket) samt att DesignA inhämtar godkännande av varje enskild ammunitionstyp från Delegationen för folkrättslig granskning av vapenprojekt *[16]* (se *avsnitt 5.10.9* näst sista stycket).

6.5.7 Krav avseende ny konfiguration för att skapa viss förmåga

I det fall att förmåga avses skapas genom att i huvudsak *meranvända* eller *återanvända* tekniska delsystem och produkter som redan ingår i/eller har ingått i annat tekniska system (enligt principen system av system), ska följande specificeras i TTEM/TEMU.

Generella krav: Definition av hela det övergripande tekniska systemet och identifiering av ingående tekniska system och produkter, dels de som ska återanvändas, dels de som ska nyanskaffas.

Systemsäkerhetskrav

Tillämpa flertalet av de tekniska krav som kan användas vid nytt tekniskt system *6.5.6* liksom de verksamhetskrav som redovisas under *avsnitt 6.5.2*.

6.5.8 Krav avseende integrationsprodukt

Då befintligt tekniskt system avses tillföras nytt tekniskt delsystem/produkt (oavsett bakomliggande orsak) och detta nya delsystem är av liten omfattning, kan följande princip om ”integrationsprodukt” tillämpas, särskilt om samma produkt avses integreras i flera olika plattformar. Principen innebär att själva anskaffningen hanteras för sig och att integrationen utförs för en plattformstyp i taget, genom beställning till aktuell DesignA om att genomföra aktuell integration.

Det tillförda delsystemet/produkten kan utgöras av såväl särskild utvecklad materiel som köpt/tillhandahållen GOTS- eller COTS-materiel.

Krav avseende integrationsproduktens egenskaper

Generella förusättningar:

- Avsedd generell användning av integrationsprodukten
  - Krävd förmåga – hur och till vad integrationsprodukten ska kunna användas, respektive hur den inte avses kunna användas (båda avser generellt, inte plattformsspecifikt)
  - Krav på uthållighet (driftsprofil)
  - Vem som ska vara användare/operatör uttryckt i generella termer. Särskilda krav på användargränssnitt (HMI-krav) anges med hänsyn till avsedda lednings- och stridsförhållanden för operatör, antal operatörer och deras avsedda kompetens
  - Geografisk miljö/användningsmiljö

- Konfiguration

  Vilka plattformar/andra tekniska system integrationsprodukten ska kunna användas tillsammans med, ingå som tekniskt delsystem i, respektive samfungera med, vid till exempel internationell insats. Det förutsätts dock här att den särskilda anpassningen till plattformen åstadkoms genom att en särskild anpassningsutrustning tas fram för plattformen i en särskild integrationsbeställning. Integrationsprodukten avses härigenom på enklaste sätt kunna ”jackas” in i anpassningsutrustningen. Härigenom förblir integrationsprodukten identisk oavsett avsedd plattform.

Systemsäkerhetskrav

Krav ska ställas på tolerabel risknivå för person respektive ekonomisk skada. Använd kraven nr 2.656.02 och 2.656.03. (Anges i TTEM.)

Krav avseende integration på viss plattform

Generella krav:

- Krav på att utveckla en anpassningsutrustning som har egenskapen att kunna ”docka” integrationsprodukten och ”ta hand om” alla gränsytor mellan plattformen och integrationsprodukten. Anpassningsutrustningen bör utformas att utgöra en del av det tekniska system plattformen utgör.
- Specificera avsedd användning av integrationsprodukten på aktuell plattform
  - Krävd förmåga – hur och till vad integrationsprodukten ska kunna användas, respektive hur den inte avses kunna användas.
  - Krav på uthållighet (driftsprofil).
  - Vem som ska vara användare/operatör. Särskilda krav på användargränssnitt (HMI-krav) anges med hänsyn till avsedda lednings- och stridsförhållanden för operatör, antal operatörer och deras avsedda kompetens på aktuell plattformstyp.
  - Geografisk miljö/användningsmiljö.

- Konfiguration
  Inom aktuell plattform, vilka andra tekniska system som integrationsprodukten ska kunna användas tillsammans med, ingå som tekniskt delsystem respektive samfungera med, vid till exempel internationell insats.

Systemsäkerhetskrav

Krav ska ställas på tolerabel risknivå för person respektive ekonomisk skada. Använd kraven nr 2.656.02 och 2.656.03. (Anges i TTEM.)

6.5.9 Krav avseende fordon av standardkaraktär (COTS)

Fordon av standardkaraktär (COTS) som är godkänt att införas i MIFOR erfordrar inte särskild systemsäkerhetsverksamhet. Eventuellt beslut om användning kan, vad avser krav på systemsäkerhet, utfärdas på det underlag som ledde till registrering i MIFOR.

Om sådant fordon avses förses med militär tilläggsutrustning (radiostationer, beväpning med mera) ska systemsäkerhetsverksamhet genomföras för denna utrustning, samt ska särskild systemsäkerhetsverksamhet genomföras för integrationen. (Jämför *avsnitt 5.10.6* och krav enligt *6.5.8*.)

Följande krav kan användas vid uppdrag om anskaffning av civilt fordon som förekommer i handeln (COTS).

Systemsäkerhetskrav

2.659.01	Anskaffningen ska avse COTS-fordon. Fordonet ska vara godkänt genom registreringsbesiktning eller enskilt godkännande för att införas i MIFOR varför ingen särskild systemsäkerhetsverksamhet behöver utföras. (Anges i anskaffningsbeslut/ TTEM.)

6.5.10 Handvapen av civil standardkaraktär (COTS)

Vid uppdrag om anskaffning av civilt handvapen som förekommer i handeln (COTS) kan följande krav ställas:

Systemsäkerhetskrav

2.6510.01	Anskaffningen ska avse COTS-vapen. Vapnet ska vara CIP-märkt varför ingen särskild systemsäkerhetsverksamhet ska utföras. Vapnet ska inte klassas som krigsmateriel. (Anges i anskaffningsbeslut/TTEM.)
2.6510.02	Godkännande av vapnet ska inhämtas från Delegationen för folkrättslig granskning av vapenprojekt *[16]*. (Anges i anskaffningsbeslut/TTEM.) Kravet ställs enbart i det fall att det civila vapnet av Försvarsmakten avses användas för militärt ändamål (bekämpning av humanmål).

6.5.11 Krav avseende trivial materiel

Enkla produkter som används isolerat, såsom necessär, sportskor och som inte omfattas av lag eller författning med militärt undantag (jämför *avsnitt 1.2*) erfordrar inte heller någon systemsäkerhetsverksamhet. Inte heller ska något systemsäkerhetsbeslut tas fram.

I det särskilda fall att Försvarsmakten behöver fatta beslut om användning (BOA) för sådan enkel produkt, kan BOA, vad avser krav på CSSB, utfärdas på det underlag som möjliggjorde marknadsföring av den enkla produkten.

Skulle den enkla produkten behöva införlivas i ett tekniskt system, undersöks genom DesignA om principen ”Justerat tekniskt system” *avsnitt 5.6.4*, kan tillämpas, innan regelrätt systemsäkerhetsverksamhet initieras.

Systemsäkerhetskrav

2.6511.01	Anskaffningen ska avse COTS-produkt. Produkten ska vara CE-märkt varför ingen särskild systemsäkerhetsverksamhet ska utföras. (Anges i anskaffningsbeslut/TTEM.)

6.6 Förberedelse inför mottagning

Inför mottagning av leverans från DesignA förbereder ÄF för användning av levererat tekniskt system. Erforderliga förberedelser utgörs bland annat av att:

- instruktioner för hantering och skötsel samt erforderliga säkerhetsbestämmelser, tas fram och beslutas
- centralt systemsäkerhetsbeslut (CSSB) bereds och beslutas, varvid främst DesignA:s systemsäkerhetsgodkännande och övrig systemsäkerhetsdokumentation granskas (se vidare *avsnitt 7.2*)
- besluta hur olyckor och tillbud ska rapporteras. Tillse att det finns regler, rutiner och nödvändiga resurser för att omhänderta dessa rapporter, samt att det finns regler och rutiner för hur erforderliga riskreducerande åtgärder ska beredas och vidtas
- besluta om inrättande av gruppen SSWG-2 och ange organisation, personal, uppdrag, mandat och resurser. Ange också till vem gruppen ska rapportera.

  SSWG-2 utses på effektivast möjliga sätt:

  – Antingen enligt principen en SSWG-2 per tekniskt system/förbandstyp.
  – Alternativt kan en SSWG-2 tilldelas ansvar för flera (likartade) tekniska system/delsystem.

6.7 Försvarsmaktens mottagning av materielleverans

6.7.1 Systemsäkerhetsgodkännande

Försvarsmakten ska granska från DesignA erhållet systemsäkerhetsgodkännande, bland annat mot i beställning och TTEM/TEMU ställda krav, samt granska och acceptera detta, innan det kan utgöra underlag för Försvarsmaktens centrala systemsäkerhetsbeslut (CSSB), vilket sedan utgör ett nödvändigt delbeslut i Försvarsmaktens beslut om användning.

6.7.2 Materielleverans

Materielleverans från DesignA är av starkt skiftande karaktär vad gäller omfattning och komplexitet. Det kan avse allt från enstaka tekniskt system av okomplicerad natur till större materielsystem innehållande många tekniktyper och stödsystem. Därför måste även överlämningsprocedurens omfattning varieras utan att formalia åsidosätts. ÄFR genomför en så kallad överlämningsberedning inför varje specifik leverans. Där fastställs i samråd med DesignA överlämningsprocedurens omfattning.

Försvarsmaktens kravelementlista *[9]* upptar krav för olika slag av tekniska system och olika leveranstyper. Flera av kraven avser systemsäkerhet. Ett särskilt viktigt krav är att det ska tillsättas en SSWG-2 och att det till denna ska överlämnas ett komplett underlag avseende det tekniska systemets olycksrisker.

6.8 SSWG-2

6.8.1 Tillsättning

Arbetsgruppen för systemsäkerhet under vidmakthållandefasen, SSWG-2, beskrivs under aktiviteten SSWG i *H SystSäk del 2 avsnitt 5.8*.

SSWG-2 tillsätts av ÄF. Beslutet om SSWG-2 bör minst reglera följande punkter:

- ordförande
- personal
- ansvar och uppgifter
- resurser
- arbetsform (fristående arbetsgrupp eller sammanträdesform, med mera)
- befogenheter
- avrapportering (när, vad och till vem)
- från vilka aktörer (förband, TeK, FMV, FömedC, leverantörer, med flera) rapportering ska tas emot
- från vilka övriga källor (databaser med mera) som information bör inhämtas
- till vilka aktörer som stöd ska lämnas.

6.8.2 Inriktning av SSWG-2 arbete

SSWG-2 planerar sin verksamhet med utgångspunkt i erhållna förutsättningar enligt ovan och dokumenterar detta i en egen verksamhetsplan (SSPP/SSMP för aktuell SSWG-2):

- Inriktningen av SSWG-2 verksamhet ska vara att kontinuerligt följa verksamheten med det tekniska systemet ur ett systemsäkerhetsperspektiv. Syftet är att proaktivt identifiera förekommande säkerhetsbrister och föreslå erforderliga åtgärder för att eliminera/minska dessa och därigenom innehålla angiven tolerabel risknivå.
- SSWG-2 söker all möjlig information enligt principen ”medhörning”, det vill säga utan att ta administrativt ansvar för sluthantering med mera av rapporter.

Under vidmakthållandet koncentreras systemsäkerhetsaktiviteter till att:

- Bevaka att det tekniska systemets olycksrisker fortlöpande finns inom tillåten risknivå. Om viss risk överskrider tillåten nivå, identifierar SSWG-2 lämpliga åtgärder som kan leda till att den enskilda olycksrisken reduceras.
- Föreslå riskreducerande åtgärder.
- Granska och bevaka tillbud och olyckor samt hålla aktuellt tekniskt systems risklogg/risklista aktuell.
- Fortlöpande hålla SSWG-2 systemsäkerhetsplan aktuell. Planen utgör SSWG-2 programförklaring och arbetsplan.

Då förändringar i konstruktion, miljö eller avsedd användning planeras, ska aktuella systemsäkerhetsanalyser (de som påverkas av aktuella förändringar) granskas på nytt för att undersöka eventuella effekter på det tekniska systemets olycksrisker (nya såväl som tidigare hanterade).

6.8.3 Avvikelsehantering

När tekniskt system skapas och utvecklas identifieras det tekniska systemets olycksrisker. Samtliga olycksrisker kan dock sällan upptäckas (jämför *avsnitt 3.1*). Dessutom uppkommer vissa nya olycksrisker under användning av bland annat följande orsaker:

- annat användningssätt än avsett
- kortare utbildning än avsett
- mindre eller annat underhåll än avsett
- annan förslitning och åldring än förutsett
- obehörig ändring av tekniskt system.

Dessa olycksrisker kan göra sig påminda genom olika typer av avvikelser. Vissa är harmlösa, andra i form av olyckor. För att minska olycksrisken är det väsentligt att alla avvikelser rapporteras och analyseras så att riskreducerande åtgärder snarast kan tas fram och införas. Det är väsentligt att SSWG-2 upplyser aktuella operatörer om förhållandet att de tekniska systemen efter leverans, trots omfattande systemsäkerhetsverksamhet under utveckling och tillverkning, ändå kan förväntas innehålla flera okända olycksrisker. Därför är operatörens medverkan och uppmärksamhet viktig för att identifiera sådana olycksrisker innan de hunnit föranleda tillbud eller olycka.

6.9 Driftsättning

Som driftsförberedelse kontrolleras att:

- systemsäkerhetsavgörande utbildningsanvisningar har tillämpats
- grupp för systemsäkerhet, SSWG-2 har organiserats och fungerar (bemanning, uppgifter, resurser, se vidare *avsnitt 6.8*)
- beslut om användning (BOA) finns för det tekniskt system som avses tas i drift
- det finns rutin för hantering av avvikelser för det tekniska system som avses tas i drift
- användare och teknisk personal har fått rätt utbildning för sina uppgifter med det tekniska systemet.

6.10 Drift

Tekniskt system kan överlämnas till förband/skola för användning och utbildning.

ÄF kan fördela ansvar för att följa upp risker och föreslå/vidta riskreducerande åtgärder till lämplig organisation inom Försvarsmakten. Ansvaret avser visst tekniskt system och omfattar också att vidmakthålla samtlig riskdokumentation.

Det råder ett absolut förbud att genom lokala initiativ/beslut ändra/låta ändra sådan materiel. Inga som helst ingrepp får göras i materielen. Ingen materiel får läggas till eller användas tillsammans med det tekniska systemet, inga delar får avlägsnas, annat än vad som framgår av tillhörande dokumentation. Det tekniska systemet ska användas och underhållas i överensstämmelse med tillhörande dokumentation och tillämpliga säkerhetsbestämmelser.

Förslag om förändring kan inges till materielansvarig i Försvarsmaktens HKV. Vid utredning av förslaget, inför eventuellt beslut om införande, granskas bland annat:

- kostnader
- effekt

- tillkommande olycksrisker
- realiserbarhet.

Jämför också vad som anges under *avsnitt 5.11, Besluts- och produktdokument under insats*.

6.11 Modifiering

Med modifiering avses förändring av det tekniska systemet som påverkar av DesignA godkänd konfiguration.

Modifiering hanteras som ny anskaffning och kräver fullständigt systemsäkerhetsarbete. Detta arbete ska genomföras för hela förändringen inklusive alla gränsytor till oförändrade delar och funktioner hos grundsystemet. Se vidare *avsnitt 5.6*.

6.12 Avveckling

Generellt ska alla olycksrisker som är förknippade med avveckling, identifieras och omhändertas. Eftersom Försvarsmakten är ägarföreträdare för Statens försvarsmateriel, och militär materiel vanligtvis innehåller flera dolda/inbyggda riskkällor, så är det mycket viktigt att Försvarsmakten verkligen tar sitt ansvar för att identifiera (låta identifiera) de olycksrisker som finns i aktuell materiel. Det är Försvarsmaktens ansvar att upplysa (låta upplysa) den som förvärvar, alternativt tar emot materielen för destruering/skrotning om vilka dessa risker är och vilka egenskaper aktuella riskkällor har. Se vidare *H SystSäk del 2 avsnitt 5.34, Riskanalys inför avveckling av system (RADS) – S61*.

Vid avveckling av produkt ska Försvarsmakten först låta genomföra riskanalys inför avveckling och grundat på denna utforma uppdraget om avveckling så att detta sker på ett säkert sätt.

Avgränsning: Här berörs inte Försvarsmaktens rutiner för beslut om avveckling. Endast hur olycksrisker ska hanteras i anslutning till beredningen av avveckling.

6.13 Checklista för Försvarsmaktens krav till DesignA

Checklistan används vid Försvarsmaktens framtagning av krav i KB/TTEM. Krav i mörkblå fält är obligatoriska krav. Det tekniska systemets avsedda egenskaper utgör grund för att välja krav i övrigt.

Tabell 6:1 Systemsäkerhetskrav

Krav nr	Benämning	Tillämplighet för aktuellt tekniskt system			Kommentar
		Ja	Nej	N/A	
Krav om basresurser					
2.632.01	Specificera behov av basresurser				
Krav vid studier					
2.642.01	Identifiera systemrisker				
2.642.02	Identifiera systemsäkerhetsegenskaper/systemsäkerhetsåtgärder för att motverka identifierade systemrisker				
2.642.03	Identifiera risker i det framstuderade tekniska systemet				
2.642.04	Riskbedömning ska utföras med hjälp bifogad bedömningsmall				
Verksamhetskrav i KB					
2.652.01	Säkerställ att leverantör genomför systemsäkerhetsverksamhet				
2.652.02	Militärt undantag Säkerställ att leverantör begär komplettering avseende Försvarsmaktens krav på aktuella gränsvärden				
2.652.03	Leverera systemsäkerhetsgodkännande. Systemsäkerhetsgodkännandet ska också innehålla xx, yy, zz				
2.652.04	Leverera fullständig riskdokumentation				

Krav nr	Benämning	Tillämplighet för aktuellt tekniskt system			Kommentar
		Ja	Nej	N/A	
2.652.05	Leverera underlag för utbildning				
2.652.06	Leverera underlag till föreskrifter och anvisningar				
2.652.07	Avvikelsehanteringsrutiner ska tillämpa Försvarsmaktens avvikelsehanteringssystem XXXX				
2.652.08	Språk i tekniska systemets dokumentation				
2.652.09	Särskild granskning				
Krav i TTEM avseende systemrisker					
2.653.01	Identifiera systemrisker (olycksrisk på systemnivå)				
2.653.02	Systemsäkerhetsåtgärder för att motverka systemrisker				
Krav avseende militär ammunition					
2.654.01	Systemsäkerhetsgodkännande för militär ammunition avser dels ammunitionsobjekt och dels som fristående transport- och förvaringsobjekt				
2.654.02	H SystSäk och HVAS ska tillämpas				
2.654.03	Granskningsrapport från en oberoende granskningsfunktion				
2.654.04	Godkännande från MSB om säkerhet vid transport och förvaring				
Krav avseende civil ammunition					
2.654.05	COTS-ammunition ska vara CIP-märkt				
2.654.06	Förvaringskod (F-kod) ska inhämtas från FMV				

Krav nr	Benämning	Tillämplighet för aktuellt tekniskt system			Kommentar
		Ja	Nej	N/A	
2.654.07	Godkännande från Delegationen för folkrättslig granskning av vapenprojekt, om FM avser använda ammunitionen för militärt ändamål				
Tekniska krav i TTEM – strålningsemitterande utrustning					
2.655.01	Utrustning xx, yy, zz ska omfattas av systemsäkerhetsgodkännandet				
2.655.02	Förbandsutrustning mm, nn, pp ska omfattas av systemsäkerhetsgodkännandet				
Tekniska krav i TTEM avseende nytt tekniskt system					
2.656.01	Ammunition ska IM-egenskaper xx, yy, zz				
2.656.02	Olycksrisker för person enligt bifogad riskmatris för personskada				
2.656.03	Olycksrisker för ekonomisk skada enligt bifogad riskmatris för ekonomisk skada				
Krav avseende standardfordon, i anskafffningbeslut/TTEM					
2.659.01	Fordonet ska vara godkänt genom registreringsbesiktning eller enskilt godkännande				
Krav avseende civila handvapen, i anskafffningbeslut/TTEM					
2.6510.01	Vapnet ska vara CIP-märkt. Vapnet ska inte klassas som krigsmateriel				
2.6510.02	Godkännande från Delegationen för folkrättslig granskning av vapenprojekt, om FM avser använda vapnet för militärt ändamål				
Krav avseende trivial materiel, i anskafffningbeslut/TTEM					
2.6511.01	Produkten ska vara CE-märkt				

7 Designansvarigs systemsäkerhetsverksamhet

7.1 Försvarsmaktens övergripande krav på DesignA

7.1.1 DesignA:s organisation

DesignA ska i sin organisation peka ut minst en befattningshavare/rollinnehavare med ansvar för att styra och leda systemsäkerhetsverksamheten för den materiel/tjänst som DesignA producerar på Försvarsmaktens beställning. Denne befattningshavare/rollinnehavare undertecknar DesignA:s systemsäkerhetsgodkännande.

7.1.2 Leverans till Försvarsmakten

Det är Försvarsmaktens krav att DesignA före utsatt tid (vanligen i god tid innan leverans av det tekniska systemet) levererar en fullständig beskrivning av genomförd systemsäkerhetsverksamhet, med en utförlig redovisning av de risker som finns kvar i det tekniska systemet.

7.1.3 Medverkan i Försvarsmaktens systemsäkerhetsverksamhet

Försvarsmaktens krav på DesignA:s medverkan i Försvarsmaktens systemsäkerhetsverksamhet uttrycker Försvarsmakten i ömsesidiga samordningsavtal respektive genom beställning av tekniskt system eller av åtgärd avseende befintligt tekniskt system. Sådan medverkan avser att ta fram, använda, vidmakthålla samt avveckla Försvarsmaktens produkter och tekniska system men kan även avse direkt ledningsstöd.

7.1.4 Långsiktig planering av systemsäkerhetsverksamhet

Det är lämpligt att DesignA, i en särskild plan (SSMP) dokumenterar överväganden och beslut avseende organisation och delegeringar för DesignA:s systemsäkerhetsverksamhet. Det är också lämpligt att i planen redovisa analys av samordningsavtalet med Försvarsmakten avseende systemsäkerhet och de åtaganden DesignA har gjort. I planen bör även redovisas tagna beslut avseende arbetssätt, mallar med mera som ska tillämpas internt hos DesignA. (Se *H SystSäk del 2 avsnitt 5.1*.)

7.2 Försvarsmaktens krav på DesignA vid uppdrag

Försvarsmaktens systemsäkerhetskrav uttryckta i KB respektive TTEM rensas från motstridiga krav samt formuleras så att de är mätbara. Kraven omsätts till krav på leverantör och uttrycks i anbudsinfordran (RFP) och fastställs sedan i kontrakt genom beställning. (Se *H SystSäk del 2 avsnitt 5.4*.)

7.3 Systemsäkerhetsverksamhet

7.3.1 Mottagning av uppdrag

För mottaget uppdrag om anskaffning (i tillämpliga delar också vid studie, modifiering, renovering respektive avveckling) av visst tekniskt system, genomför DesignA systemarbete varvid behov av systemsäkerhetsverksamhet analyseras.

Nedanstående punkter tjänar som checklista vid denna analys:

- Genomför initial projektgenomgång med projektledaren. Här analyseras samtliga Försvarsmaktens systemsäkerhetskrav i beställningsunderlag; kundbeställning, TTEM samt övrig relevant dokumentation som beskriver förväntad prestation och produkt ur ett systemsäkerhetsperspektiv (se *avsnitt 5.3*). Till exempel krav avseende särskilt säkerhetsutförande för tekniskt system (produktkrav).

  Ta fram granskningsrapport över resultatet av utförd analys.

- Granskningsrapporten kommuniceras med Försvarsmakten för eventuell komplettering av KB och TTEM.
- Utforma krav avsedda dels för DesignA internt, dels för RFP till leverantör.
- Identifiera vad det tekniska systemet består av och identifiera möjlig uppdelning i lämpliga tekniska delsystem samt identifiera tänkbara leverabler.
- Besluta för varje nivå av systemintegrationen, inom ramen för ”hela det anskaffade tekniska systemet”, vem som ska ges ansvaret för denna integration samt hur integrationen ska verifieras. (Om integrationen inte beställs från leverantör, så kvarstår integrationsansvaret för helheten hos DesignA.)

7.3.2 Anbudsinfordran – beställning

Vid framtagning av anbudsinfordran (RFP) ska DesignA alltid genomföra följande systemsäkerhetsaktiviteter:

- Omforma identifierade systemsäkerhetskrav till krav i RFP. Utforma krav (tekniska krav och verksamhetskrav) för att kunna genomföra upphandling av respektive teknisk systemdel (med utgångspunkt i från Försvarsmakten erhållna mål och krav).
- Ställa krav på den verksamhet som leverantör ska genomföra (se *H SystSäk del 2 avsnitt 5.2.4* för exempel på krav).
- Ställa krav på att oberoende granskning ska utföras och anvisa funktion för detta (se *avsnitt 7.5*).
- Ställa krav på vilka säkerhetsgenomgångar som ska genomföras och när.
- Ange vem som har rätt att stänga risk på viss nivå, och hur detta ska rapporteras/förankras med DesignA.
- Ta fram anbudsinfordran, där ovan identifierade krav ställs på leverantören avseende systemsäkerhetsverksamhet, systemsäkerhetsdokumentation och systemsäkerhetsegenskaper hos det tekniska systemet.

- Värdera inkomna anbud mot ställda krav, med syfte att identifiera eventuella avvikelser.
- Tag fram rapport över genomförd utvärdering av anbud.

7.3.3 Styrning av projekt

DesignA styr projekts systemsäkerhetsverksamhet. Möjliga aktiviteter är bland annat följande:

- Planera DesignA:s systemsäkerhetsverksamhet för aktuellt uppdrag så att av Försvarsmaktens ställda krav på DesignA:s systemsäkerhetsverksamhet uppfylls. Dokumentera gjord planering i DesignA:s egen systemsäkerhetsplan, SSMP (Se *H SystSäk del 2 avsnitt 5.1*.).
- Tillsätta SSWG–1 som stöd för projektledaren (undantag kan göras för de allra enklaste anskaffningarna där projektledaren själv kan svara för aktuell verksamhet).
- Tilldela särskilt expertis.
- Ställa krav på att oberoende granskning ska utföras och anvisa funktion för detta (se *avsnitt 7.5*).

7.3.4 Styrning av leverantör

DesignA styr leverantörs systemsäkerhetsverksamhet genom att:

- genomföra säkerhetsgenomgångar med leverantören,
- fortlöpande granska leverantörens systemsäkerhetsverksamhet. Upprätta vid behov protokoll över iakttagna avvikelser samt
- fortlöpande granska systemsäkerhetsdokument som mottas från leverantör. Upprätta granskningsprotokoll (se avsnitt *avsnitt 5.12* och *7.5*).

7.3.5 Leverans till Försvarsmakten

Leverans (av tekniskt system, tjänst) ska åtföljas av beställd dokumentation. Följande åtgärder vidtas:

- Ta fram DesignA:s systemsäkerhetsgodkännande grundat på leverantörens systemsäkerhetsutlåtande, samtliga av DesignA:s framtagna granskningsrapporter samt övrig systemsäkerhetsverksamhet genomförd av DesignA. En sammanfattning av DesignA:s granskningsrapporter redovisas i systemsäkerhetsgodkännandets avsnitt ”Genomförd systemsäkerhetsverksamhet”.
- Ta fram granskningsrapport från oberoende granskningsfunktion (inom eller utom DesignA) i de fall Försvarsmakten har ställt detta krav, eller att det tekniska systemet utgörs av eller innehåller ammunition (Se *avsnitt 6.5.4*)
- Förbered och genomför överlämning till Försvarsmakten av anskaffad produkt/tekniskt delsystem/tekniskt system.

7.3.6 Anpassning

DesignA:s systemsäkerhetsverksamhet ska regelmässigt anpassas, jämför *H SystSäk del 2 avsnitt 3.2*. Grund för att anpassa systemsäkerhetsverksamheten för visst projekt är den förekomst av olycksrisker som DesignA bedömer kan komma att uppstå i aktuellt tekniskt system under utveckling/bedömer kunna finnas i tekniskt system som ska upphandlas, beroende på avsedd funktion, teknikinnehåll, komplexitet med mera. Anpassning av systemsäkerhetsverksamheten utförs genom att avväga och tilldela resurser, ställa särskilda krav på projektledarens systemsäkerhetsverksamhet och att ställa särskilda krav på leverantör.

7.3.7 Leverantör

DesignA ska kontrollera att anlitad leverantör uppfyller ställda krav.

I fall att leverantör (anbudsgivare) inte av egen kraft kan uppfylla samtliga av DesignA:s ställda krav kan denne genom att anlita underleverantör, likväl lämna anbud.

I det fall ingen anbudsgivare uppfyller samtliga ställda krav, kan DesignA likväl anlita en av dessa, förutsatt att DesignA själv säkerställer att kraven uppfylls.

7.3.8 Övrigt

Handboken reglerar inte DesignA:s interna delegeringar eller arbetssätt för systemsäkerhetsverksamhetens genomförande. (Det vill säga handboken styr *inte hur* verksamheten ska genomföras, däremot *vad* DesignA ska genomföra.)

7.4 SSWG-1

7.4.1 Beslut om SSWG-1

Arbetsgruppen för systemsäkerhet som stöd till anskaffningsprojekt, SSWG-1, beskrivs i *H SystSäk del 2 avsnitt 5.8*.

SSWG-1 inrättas av DesignA. Beslut om SSWG-1 bör minst reglera följande punkter:

- ordförande
- personal
- uppgifter
- resurser
- ansvar
- arbetsformer (kontaktytor, mötesfrekvens och omfattning, plats med mera)
- avrapportering (när, vad och till vem).

7.4.2 Inriktning av SSWG-1 arbete

SSWG-1 planerar sin verksamhet med utgångspunkt från erhållna förutsättningar enligt ovan och dokumenterar denna i en egen verksamhetsplan (SSPP för aktuell SSWG-1):

- Inriktningen av SSWG-1 verksamhet ska vara att kontinuerligt stödja projektledarens anskaffningsverksamhet med systemsäkerhetsverksamhet. Under aktuella aktiviteter med det tekniska systemet verkar SSWG-1 med inriktningen att proaktivt identifiera förekommande säkerhetsbrister och föreslå erforderliga åtgärder för att eliminera/reducera dessa för att uppnå och vidmakthålla en godtagbart säker nivå.
- SSWG-1 medverkar vid förekommande leverantörsredovisningar för projektet och utgör här systemsäkerhetsexpertis.
- Bevakar att det tekniska systemets olycksrisker fortlöpande under anskaffningstiden hålls inom tolerabel risknivå. Om viss olycksrisk överskrider tolerabel risknivå, bevakar SSWG-1 att leverantör identifierar och föreslår lämplig åtgärd som reducerar denna till tolerabel risknivå.
- Bevakar att leverantör fortlöpande uppdaterar tekniskt systems risklogg/risklista.
- Håller fortlöpande SSWG-1 systemsäkerhetsplan aktuell. Planen utgör SSWG-1 programförklaring och arbetsplan.

7.5 Oberoende granskning

7.5.1 Grunder

För grunder avseende granskning respektive oberoende granskning se *avsnitt 5.12* samt *6.5.4*.

7.5.2 Inriktning av och tidpunkt för oberoende granskning

Syfte med oberoende granskning är att säkerställa att erforderlig och kravställd systemsäkerhetsverksamhet genomförs för:

- tekniskt systems alla ingående tekniska system och tekniska delsystem
- övergripande systemrisker.

Oberoende granskning är främst en metod- och kvalitetsanalys, inte en särskild riskanalys. Syftet är att granska att systemsäkerhetsmetodiken har tillämpats på korrekt sätt samt har omfattat alla delar av tekniskt system.

Vad avser övergripande systemrisker är syftet med oberoende granskning att säkerställa att identifiering och vidare hantering av övergripande faror har genomförts och att resulterande systemrisker har hanterats på ett verkningsfullt sätt.

Oberoende granskning utförs principiellt i två olika faser och därvid delvis med olika inriktning:

- Inledningsvis (tidig fas) som stöd till projektledare innan fastställande sker av DesignA:s interna systemsäkerhetsplan.
- I senare delen av anskaffningsprojektet (sen fas) när det kan redovisas hur systemsäkerhetsverksamheten har genomförts och framtagna resultat kan demonstreras.

Tidig fas

Följande funktioner ska kontrolleras:

- Projektets aktuella systemsäkerhetsplan.
- Om uppgiften från Försvarsmakten innehåller en beskrivning av möjliga systemrisker och dessas upphov?
- Om projektet har en egen dokumenterad analys av möjliga systemrisker?
- Om det totala tekniska systemet har beskrivits korrekt?
- Om samtliga tekniska delsystem, direkt under det tekniska totalsystemets nivå, har beskrivits korrekt?

Sen fas

Följande funktioner ska kontrolleras för tekniskt system:

- Projektets systemsäkerhetsplan är genomförd.
- Riskloggen är korrekt utförd, bland annat att varje enskild olycksrisk är beslutad (=stängd).
- Systemsäkerhetsverksamheten för samtliga tekniska delsystem.
- Systemsäkerhetsverksamheten för interaktion mellan ingående tekniska delsystem.

Genomförande av oberoende granskning

Oberoende granskning av erforderliga projekt-/produktdokument genomförs som stöd till DesignA inför dennes beslut om systemsäkerhetsgodkännande.

För att kunna genomföra oberoende granskning krävs att följande aktiviteter vidtas och hålls uppdaterade:

- Särskild personal med erforderlig kompetens (expertfunktion) utses, bland annat granskningsledare.
- Rutiner utarbetas, bland annat för att identifiera vilket material som ska granskas, hur granskningsrapport ska utformas, beslutsordning för fastställande av granskningsrapport.
- Rutin för hur granskning ska gå till tas fram liksom mall för granskningsrapport.

7.6 Överlämning av tekniskt system till Försvarsmakten

7.6.1 Leverabler

Designansvarig ska för framtaget tekniskt system leverera följande systemsäkerhetsdokumentation:

- systemsäkerhetsgodkännande
- systemsäkerhetsutlåtande (SCA)
- systemsäkerhetsrapport (SAR)
- rapport från eventuellt utförd oberoende granskning
- risklogg med riskstatus för varje enskild olycksrisk.

7.7 DesignA:s mandat och ansvar för ändring

DesignA har på Försvarsmaktens uppdrag det fulla ansvaret för att ett tekniskt system är konstruerat på ett säkert sätt. Detta ansvar omfattar tekniskt systems hela livslängd. Det innebär att endast av Försvarsmakten anlitad DesignA (jämför avsnitt 5.2, Tekniskt designansvar) har rätt och skyldighet att besluta om ändring av tekniskt systems konfiguration.

Genom systemsäkerhetsgodkännande och centralt systemsäkerhetsbeslut (CSSB) är ett tekniskt system definierat till innehåll och användning.

- Grund för beslutsfattande framgår av avsnitt 5.6, Besluts- och produktdokument för tekniskt system.
- Det åligger av Försvarsmakten utsedd DesignA att i särskilt beslut reglera *vilken eventuell rätt ÄFR tilldelas att besluta om justering* av tekniskt system inom DesignA:s tilldelade ansvarsområde. Former och omfattning av sådant beslut ska regleras i beslutet. Här regleras även krav på återrapportering till DesignA samt hur konfigurationsledning och dokumentation härvid ska hanteras

- Notera att i det fall att Försvarsmakten vidtar ändring av tekniskt system utan samråd med DesignA så upphävs därmed av DesignA tidigare utfärdat systemsäkerhetsgodkännande vilket utgör grund för BOA, samt återgår ansvaret för det tekniska systemets systemsäkerhet till Försvarsmakten (jämför *avsnitt 5.1*, punkt *f*).

8 Systemsäkerhetsverksamhet vid förband/skola/centrum

8.1 Övergripande ansvar

Riskmedvetande måste alltid prägla verksamhet som avser brukande av tekniskt system i fred, i krig, under strid och vid internationell insats.

Förbandschefs ansvar avseende systemsäkerhetsverksamhet:

- Identifiera och genomföra alla de lokala åtgärder som möjliggör för förbandet att inom ramen för beslut om användning och ställda krav på enskild olycksrisk, använda det tekniska systemet.
- Utbilda befäl till krävda kunskaps- och färdighetsnivåer; särskilt beaktas kunskap om för det tekniska systemet gällande SäkI-bestämmelser samt eventuella restriktioner.
- Organisera och utbilda personalen i de särskilda hanteringsregler som krävs för att befintliga olycksrisker ska hållas på krävd nivå, samt utbilda på avvikelserapportering
- Identifiera och upprätthålla kontakt med aktuell SSWG-2.
- Säkerställ att tilldelade tekniska system inte utsätts för lokalt initierade/beslutade ändringar.

8.2 Övergripande mål

Utgående från Försvarsmaktens övergripande mål med systemsäkerhetsverksamhet; att ingen person (soldat, officer eller civil) ska skadas av tekniskt system som hanteras, åligger det förbandschef att övervaka och leda verksamheten vid förbandet så att detta mål uppnås.

8.3 Ledning

Förbandschef övervakar, som en del av sitt verksamhetssäkerhetsansvar att:

- endast tekniska system används för vilken det finns beslut om användning (BOA)
- tekniskt system används på det sätt som specificeras i BOA
- avvikelserapportering sker enligt fastställda regler.

Följande lokala åtgärder är tillåtna att utföra inom ramen för ett gällande CSSB och BOA:

- användning av andra godkända konfigurationer, till exempel last- eller beväpningsalternativ
- underhållsåtgärder som inte förändrar (av DesignA) tillåten konfiguration för tekniskt system.

9 Ansvar vid provning och försöksverksamhet

9.1 Bakgrund

Detta avsnitt tydliggör vad som gäller om skyddsansvar då personal inlånas/inhyrs från Försvarsmakten till leverantör/DesignA eller arbete sker på gemensam arbetsplats.

9.2 Arbetsmiljöansvar under provning och försöksverksamhet

9.2.1 Regelverk

Följande regelverk omfattar situationen då arbete sker på gemensam arbetsplats eller om Försvarsmakten tillhandahåller personal till leverantör eller DesignA och då dessa utför försök på Försvarsmaktens uppdrag:

- AML bland annat 3 kap 12 §, 7§, 2§, 3§ *[5]*
- Arbetsmiljöverkets föreskrifter
- RMS-G *[36]*
- SäkI G *[22]*.

9.3 Avtal

Ett avtal ska skrivas mellan Försvarsmakten och den leverantör/DesignA som lånar/hyr personal från Försvarsmakten eller då arbete sker på gemensam arbetsplats. Detta avtal kan omfatta:

- Avsedd verksamhet i stort.
- Vilken verksamhet Försvarsmaktens respektive DesignA:s personal får åläggas/medverka i.
- Tekniskt system, dess status, risker och säkerhetsbestämmelser.
- Eventuellt krav på att DesignA utfärdar ett säkerhetsintyg för aktuellt tekniskt system och avsedd användning och verksamhet.
- Krav på att Försvarsmaktens Säkerhetsinspektion ska teckna samråd på säkerhetsintyget före verksamhetens början.
- Tidsförhållanden.
- Aktuella personer och deras organisatoriska hemvist.

Anmärkning: Säkerhetsintyg avser tekniskt system fartyg. Motsvarande för övriga tekniska system benämns systemsäkerhetsgodkännande för provning (jämför *H SystSäk Del 2, avsnitt 5.31.2*)

9.4 Provturskommando

Provturskommando (PTK) regleras bland annat genom följande handlingar:

- RMS *[36]*
- Samordningsavtal mellan Försvarsmakten och FMV *[40]*
- Förtydligande av krav på systemsäkerhetsdokumentation vid fartygsutprovning *[23]*

Detaljer i övrigt framgår av *H SystSäk Del 2, avsnitt 5.31.2* (Systemsäkerhetsintyg för tekniskt system fartyg inför provturskommando).

Bilaga 1 Riskuppskattning

Denna bilaga syftar till att ge en fyllig beskrivning av verksamheten riskuppskattning och utgör en fördjupande komplettering till handbokens *avsnitt 4.2.3, Riskuppskattning*.

Grunder om enskild olycksrisk

Riskuppskattning inleds med att identifiera konsekvensen för varje känd olycksrisk. Principiellt kan olyckor anses ha ett oändligt antal olika skadeutfall (konsekvenser). Detta framgår tydligt vid studie av ett antal vanliga bilolyckor som inträffat under jämförbara förhållanden. Här kan då noteras en omfattande variation i antal döda och skadade av olika svårighetsgrad.

Denna stora variation utgör grund för den utmaning som verksamheten riskuppskattning ska hantera – det vill säga att kunna uppskatta vilken konsekvens som kan förväntas från en identifierad olycksrisk. Och göra detta innan ett större antal olyckor har inträffat.

I *tabell B1:1* nedan ges exempel på ett antal vanliga riskkällor och farliga tillstånd. För vardera av dessa anges exempel på möjlig vådahändelse, möjliga exponerade skyddsföremål, olyckshändelsens art samt vilka konsekvenser som kan förväntas. Exemplet visar hur en bedömning av värsta respektive mest sannolika eller troligaste konsekvens (”skadeutfall”) kan göras.

Om procentsatserna för riskdelarna ”värsta möjliga” respektive ”mest sannolika” i *tabell B1:1* summeras, framgår att för flera av exempelolyckorna, betydande delar av respektive olyckas konsekvens inte blir beaktad. Likaså inses att dödsfall sällan är den mest sannolika konsekvensen. Detta medför att riskanalytikern inte kan tillämpa en generell metod för val av viss utfallsdel.

Följden härav blir en ofullständig jämförelse mellan ett systems samtliga olycksrisker vilket försvårar ett effektivt riskreduceringsarbete.

Tabell B1:1 Exempel med vanligen använda skadeutfall

Riskkälla/farligt tillstånd	Vådahändelse	Exponerat	Olycka	Skadeutfall	
				Värsta möjliga	Mest sannolika
Lägesenergi hos föremål och is på radiomast	Föremål eller is faller från radiomast	Civilbefolkning eller anställda	Föremål eller is träffar person	Dödsfall 1%	Försumbar skada 70%
Klorgasbehållare	Klorgasutsläpp	Civilbefolkning och anställda	Människor förgiftas	Dödsfall 5%	Försumbar skada 65%
Kinetisk energi i bil och personer i bilen	Ouppmärksamhet	Bil med förare och passagerare	Kollision med föremål eller annan bil	Dödsfall 5%	Mindre allvarlig skada 50%
Kinetisk energi i flygplan och personer ombord	Förlust av radartäckning vid ledning av flygtrafik	Flygplan med besättning och passagerare	Kollision med mark eller annat flygplan	Dödsfall 90%	Dödsfall 90%
Eget vapen	Förvanskning av IFF-data (identifiering av vän eller motståndare)	Eget flyg	Egen/allierad personal beskjuts (friendly fire)	Dödsfall 70%	Dödsfall 70%

Vanliga sätt att värdera storlek på en viss olycksrisk är att försöka värdera sannolikheten för att olycka sker och resulterar i det värsta möjliga olycksutfallet; oftast dödsfall (engelskan använder termen ”worst credible event”) respektive att värdera sannolikheten för att olyckan sker och resulterar i det mest troliga olycksutfallet, (engelskan här använder termen ”most credible event”).

Med hänsyn till den stora spridningen i olyckors utfall behöver ett fåtal standardiserade skadeklasser definieras för att möjliggöra analys av en olyckas hela skadeutfall.

Följande skadeklasser ska tillämpas för personskada:

- dödsfall
- allvarlig personskada
- mindre allvarlig personskada
- försumbar personskada.

En motsvarande fördelning används i Räddningsverkets ”Värdering av risk” *[48]*.

Nedan ges en total beskrivning av hur ett olycksutfall kan göras. I *tabell B1:1* ovan utgörs det översta exemplet av ”Lägesenergi hos föremål eller is på radiomast”. Exemplet utvidgas nu enligt följande.

Det finns i landet ett stort antal fasta radiomaster. Olika föremål kan lossna och falla från masten, dels i samband med underhållsarbete, dels som följd av väderpåverkan. Dessutom är möjligheten av isbildning på master och deras staglinor väl känd, och medför en icke försumbar risk för personer och egendom i närheten av mast. En sådan olyckas allvarlighet beror på hur hög radiomasten är och vad som faller.

Bild B1:1 Varningsskylt

Grundat på dessa faktorer kan en bedömning göras avseende hur konsekvensen kan komma att fördelas på de fyra skadeklasserna. Där så är möjligt, bör denna typ av bedömningar baseras på tillgänglig olycksstatistik från aktuellt eller närliggande område.

Mastinnehavarens riskreducerande åtgärd består bland annat av att bestämma riskområde och sätta upp varningsskyltar enligt *bild B1:1*.

Med dessa tillägg görs nu en bedömning av en olyckas hela skadeutfall uttryckt i de fyra skadeklasserna. Se vidare exemplet i *tabell B1:2* nedan.

Tabell B1:2 Exempel på en olycksrisk fördelad på skadeklasser

Fördelning av sannolikheter för en viss konsekvens	Skadeklass	Riskandel för aktuell skadeklass
I ett fall av 10 inträffar	Dödsfall	1%
I två fall av 10 inträffar	Förlust av kroppsfunktion (t. ex amputerat ben, förlust av syn eller hörsel)	5%
I två fall av 10 inträffar	Brutet ben	24%
I fem fall av 10 inträffar	Försumbar skada	70%
	Summa riskandel	100%

Genom exemplet i *tabell B1:2* påvisas möjligheten för och nödvändigheten av att för varje enskild olycka bedöma/beräkna olyckans hela skadeutfall, och grovt fördela detta på de skadeklasser som tidigare redovisats. (Det förtjänar ånyo att upprepas att dessa skadeklasser är en mycket grov, men nödvändig förenkling av verkligheten.)

Nedan i *tabell B1:3* visas med tidigare exempel (från *tabell B1:2*) hur skadeutfallet kan vara fördelat på de olika skadeklasserna.

I *tabell B1:3* har nu fullständigt redovisats samtliga ingående utfallsdelar (det vill säga 100% är redovisade). Men i de siffror som finns i *tabell B1:1* redovisas enbart en fördelning av bedömt skadeutfall på riskklasser, givet att olyckan verkligen inträffar. Här finns ingen bedömning av sannolikheten för att en olycka verkligen ska inträffa. För att kunna identifiera en olyckas riskvärde erfordras också en skattning av hur sannolik själva olyckan är, det vill säga, hur ofta kommer den att inträffa i förhållande till systemets livslängd eller annat lämpligt intervall (till exempel per år, per 100 skott, per 1000 flygtimmar). Bedöms olyckan inträffa mindre än en gång per valt intervall är den korrekta benämningen ”sannolikhet” för olycka. Kan olyckan inträffa mer än en gång under valt intervall är den korrekta benämningen olycks-”frekvens”. Matematisk är det ingen skillnad att hantera detta.

Ett olycksriskvärde uttryckt per skott kan räknas om till olycksrisk per år genom att i driftsprofilen identifiera hur många skott som avses skjutas per år och sedan multiplicera.

Tabell B1:3 Exempel med vanligen använda skadeutfall

Riskkälla/farligt tillstånd	Vådahändelse	Exponerat	Olycka	Utfallsdelar
Lägesenergi hos föremål eller is på radiomast	Lägesenergi hos föremål eller is på radiomast	Civilbefolkning eller anställda	Föremål eller is träffar person	0,01 död 0,05 allvarligt skadad 0,24 mindre allvarligt skadad 0,7 försumbar skada
Klorgasbehållare	Klorgasutsläpp	Civilbefolkning och anställda	Människor förgiftas	0,05 död 0,1 allvarligt skadad 0,2 mindre allvarligt skadad 0,65 försumbar skada
Kinetisk energi i bil och personer i bilen	Ouppmärksamhet	Bil med förare och passagerare	Kollision med föremål eller annan bil	0,05 död 0,1 allvarligt skadad 0,5 mindre allvarligt skadad 0,35 försumbar skada
Kinetisk energi i flygplan och personer ombord	Förlust av radartäckning vid ledning av flygtrafik	Flygplan med besättning och passagerare	Kollision med mark eller annat flygplan	0,9 död 0,1 allvarligt skadad 0,0 mindre allvarligt skadad 0,0 försumbar skada
Eget vapen	Förvanskning av IFF-data (identifiering av vän eller motståndare)	Eget flyg	Egen/allierad personal beskjuts (friendly fire)	0,7 död 0,1 allvarligt skadad 0,1 mindre allvarligt skadad 0,1 försumbar skada

Grundat på första exemplet i *tabell B1:1* ”Föremål eller is på radiomast”, görs här en ytterligare utvidgning för att beskriva relevanta delar av denna olycka, nödvändiga för att identifiera hur ofta en sådan olycka kan komma att inträffa.

Tidigare har omnämnts mastens höjd, föremålens och isens utformning (storlek, form, med mera). Utifrån dessa faktorer gjordes en bedömning avseende konsekvenser.

Nu erfordras data som beskriver, dels hur ofta riskkällan förväntas förekomma (jämför *tabell B1:2*), och hur ofta den kan komma att utlösas av en ”bidragande orsak” och dess ”utlösare” respektive hur ofta ett farligt tillstånd kan förekomma.

Exemplet avser en fast radiomast ute i naturen. Olika föremål (vilka därmed utgör riskkälla/farligt tillstånd) kan under hela året lossna från masten och falla. Exponerat är personer och egendom under masten och dess staglinor.

Dessutom kan eventuellt förekommande is lossna från masten och dess staglinor och falla.

Antaganden om olyckan

Redovisade siffror är mycket grova antaganden och avser ge underlag för hur problemet kan ställas upp, bedömas och beräknas. (Se *avsnitt 4.2.1.*):

- föremål bryts loss från masten av väderfenomen eller tappas i samband med underhåll, cirka en gång per år
- is finns på masten under 20 dagar per år och faller i genomsnitt var fjärde dag.
- person bedöms finnas under masten totalt en dag per år
- radiomasten bedöms inte kunna skada yttre miljön nämnvärt
- skyddsvärd egendom bedöms finnas under masten totalt en halv dag per år.

Kalkyl avseende personskada

1 + (20 × 25%) = föremål och is faller sex gånger per år

Som antagits ovan exponeras en person en dag per år.

Sannolikhet för olycka med skada på person blir därmed:

$6/365 \times 1/365 = 5 \times 10^{-5}$, per radiomast och år.

Det vill säga det inträffar en olycka per 20 000 år och radiomast, med risk för viss personskada.

Observera dock att det här redovisade exemplet, dels inte gör anspråk på att vara siffermässigt representativt, dels avser att belysa resultatet av en riskanalys avseende den faktiska risken för personskada, **innan någon som helst riskreducerande åtgärd har vidtagits!**

Uppskattning av personrisk

För den enskilda olyckan ”Någon blir exponerad för fallande föremål eller is”, leder resonemanget närmast ovan fram till en siffra på sannolikheten för att olyckan inträffar. Enligt beräkningen ovan inträffar det en olycka med någon form av personskada, per år och mast med sannolikheten ($p = 5 \times 10^{-5}$).

Ur *tabell B1:2* hämtas den uppskattade fördelningen i procent av olyckans fyra olika standardiserade skadeklasser, det vill säga ett bedömt värde på hur sannolikheten för att skador, motsvarande vardera av de fyra olika skadorna skulle kunna uppkomma, givet att en olycka inträffar.

I *tabell B1:4* nedan redovisas hur en olycka med sannolikheten (p=0,00005) för personskada fördelas per skadeklass (kallas också delrisk) då underlag enligt *tabell B1:2* används.

Tabell B1:4 Exempel på fullständigt skadeutfall fördelat på skadeklasser

Skadeklass	Bedömning av skadeklassens andel av det totala utfallet	Sannolikhet för visst skadeutfall. fördelat per skadeklass, per radiomast och år (=delrisk)
Dödsfall	Inträffar i ett fall av 100 = 1%	$5\times10^{-5}\times0{,}01 = 5\times10^{-7}$ dödsfall
Allvarlig skada	Inträffar i fem fall av 100 = 5%	$5\times10^{-5}\times0{,}05 = 2{,}5\times10^{-6}$ allvarlig skada
Mindre allvarlig skada	Inträffar i 24 fall av 100 = 24%	$5\times10^{-5}\times0{,}24 = 1{,}2\times10^{-5}$ mindre allvarlig skada
Försumbar skada	Inträffar i 70 fall av 100 = 70%	$5\times10^{-5}\times0{,}70 = 3{,}5\times10^{-5}$ person med försumbar skada

Genomsnittlig användning

För att kunna identifiera vilka olycksrisker som kan förekomma med ett visst tekniskt system måste användningsmiljö och avsedd nyttjandegrad anges. När Försvarsmakten anskaffar ett visst tekniskt system måste Försvarsmakten också ange avsedd driftsprofil. Det är mot denna driftsprofil som konstruktören ska konstruera det tekniska systemet.

Om istället Försvarsmakten vid viss utländsk insats använder tekniskt system som är framtaget med driftsprofil för invasionsförsvar (regelbunden utbildning och ett tidsbegränsat krig) så kan de olycksrisker som uppstår under kontinuerlig användning under ett helt år, förväntas ha annan karaktär samt möjligen kunna inträffa med annan frekvens/sannolikhet. I värsta fall kommer detta att inträffa oftare och med allvarligare konsekvenser än vad som tidigare har bedömts. Problemet hanteras genom att ta fram ett nytt systemsäkerhetsbeslut för avsedd användning.

Uppskattning av miljörisk

Risk för skada på yttre miljö kan resultera i reparabla skador respektive skador som helt utplånar en djurart eller permanent förstör ett visst fysiskt område. Risker med reparabla konsekvenser kan uppskattas i ekonomiska termer. Olycksrisk som bedöms kunna leda till kvarstående miljökonsekvenser erfordrar i varje enskilt fall, alltid Försvarsmaktens särskilda beslut, se vidare *avsnitt 4.2.3*.

Kalkyl avseende ekonomiska skada

1 + (20 × 25%) = föremål och is faller sex gånger per år.

Som antagits ovan exponeras värdeföremål en halv dag per år.

Sannolikhet för olycka med skada på egendom blir därmed:

$6/365 \times 0{,}5/365 = 2 \times 10^{-5}$, per radiomast och år.

Det vill säga det inträffar en olycka per 50 000 år och radiomast, med risk för viss ekonomisk skada.

Observera också här att det redovisade exemplet, dels inte gör anspråk på att vara siffermässigt representativt, dels avser att belysa resultatet av en riskanalys avseende den faktiska risken för ekonomisk skada, **innan någon som helst riskreducerande åtgärd har vidtagits!**

Uppskattning av ekonomisk risk

Risk för ekonomisk förlust anses i denna handbok utgöras av:

- direkt skada på eller förlust av materiel, delsystem, system
- skada på annans egendom
- kostnad för sanering av skada på yttre miljö som Försvarsmakten har orsakat genom sin verksamhet med aktuellt system.

På samma sätt som ett personrelaterat olycksutfall till alla sina delar behöver kunna identifieras och sorteras in i olika skadeklasser, behöver motsvarande kunna göras också avseende ekonomisk skada.

Ekonomiska skadeklasser definieras genom att först identifiera värsta möjliga utfall. Därefter fördelas det totala utfallsutrymmet i fyra likvärdiga skadeklasser (se i exempel nedan hur tilldelning av värden utförs till de fyra skadeklasserna).

För exemplet föremål och is som faller från radiomast skulle värsta möjliga skada kunna bedömas hamna i storleksordningen några hundra tusen kronor, varvid de fyra skadeklasserna tilldelas följande värden:

- mer än ett hundra tusen kronor ($\geq 10^5$)
- tio tusen till hundra tusen kronor (10^4–10^5)
- ett tusen till tio tusen kronor (10^3–10^4)
- mindre än tusen kronor ($\leq 10^3$).

För ett annat exempel där riktigt svåra olyckor bedöms kunna inträffa skulle värsta möjliga skada kunna hamna i miljardklassen (egendomsskador, skadestånd relaterat till tredje man samt kostnader för att städa upp och återställa den yttre miljön), varvid de fyra skadeklasserna tilldelas följande värden:

- mer än en miljard kronor ($\geq 10^9$)
- tio miljoner till en miljard kronor (10^7-10^9)
- etthundratusen till tio miljoner kronor (10^5-10^7)
- mindre än tusen kronor ($\leq 10^3$).

(Princip: Kvoten mellan två närliggande skadeklasser är alltid konstant.)

Dessa skadeklasser används på ena axeln tillsammans med samma olyckssannolikheter på andra axeln som för personskador.

Tabell B1:5 Exempel på skadeutfall för ekonomiska skada

Skade-klass	Skada uttryckt i kronor	Bedömning av skadeklas-sens del av totala utfallet	Sannolikhet för visst skade-utfall, fördelat per skade-klass per mast och livs-längd
I	1 000 000 SEK	Inträffar i ett fall av 100 = 1%	$2\times10^{-5}\times0{,}01 = 2\times10^{-7}$ för ska-da (på en miljon)
II	100 000 SEK	Inträffar i fem fall av 100 = 5%	$2\times10^{-5}\times0{,}05 = 10^{-6}$ för skada (på ett hundra tusen)
III	10 000 SEK	Inträffar i 20 fall av 100 = 20%	$2\times10^{-5}\times0{,}2 = 4\times10^{-6}$ för skada (på tio tusen)
IV	1 000 SEK	Inträffar i 740 fall av 10 = 74%	$2\times10^{-5}\times0{,}74 = 1{,}5\times10^{-5}$ för skada (på nivån ett tusen)

Det är värt att understryka att siffrorna i exemplet ovan är antaganden och avser situationen innan riskreduce-rande åtgärder är vidtagna.

Metoder för riskuppskattning

Empirisk uppskattning

Tillvägagångssätt

Erfarenhetsdata från liknande (befintligt eget/befintligt annans/ avvecklat) system med liknande användning, anpassas och tillämpas.

Nackdelar

Kan vara svårt att hitta data från liknande system enligt ovan.

Transformering och anpassning av data är svårt.

Fördelar

Om tillförlitliga och lämpliga data finns så är detta en enkel metod.

Beräkning

Tillvägagångssätt

Utgående från detaljerade kunskap om systemet beräknas varje enskild olycksrisk, bland annat med hjälp av felträd.

Nackdelar

Felträd är ofta komplicerade och kräver omfattande kännedom om ingående komponenters och delsystem interna relationer, varför denna metod ofta är omständlig att tillämpa.

Fördelar

Metoden är ofta tillämpbar och ger bra värden för väl känt tekniskt system, under förutsättning att detta är relativt litet. Yttre faktorer som handhavande och användningsmiljö kan på ett åskådligt sätt byggas in i felträdet, åsättas uppskattade sannolikheter och resulterar i en sammanfattande siffra på det tekniska systemets olycksrisk.

Vid riskreducerande åtgärd återanvänds samliga parametrar, utom för den egenskap som förbättrats, vilket tillsammans leder till tillförlitligare bedömningar.

Expertuppskattning

Tillvägagångssätt

Person med mycket ingående kunskap om systemets egenskaper och dess användning gör uppskattningarna och ansätter siffervärden.

Nackdelar

Svårt att hitta experter med goda kunskaper. Svårt att upprepa gjord uppskattning då den tenderar att bli relativt personberoende. Ibland svårt att säkerställa en ensad dokumentation då också denna tenderar att bli relativt personberoende.

Fördelar

Enkel och snabb metod med god trovärdighet och relevans.

Modellering/Simulering

Tillvägagångssätt

Modellering och simulering innebär att aktuellt system åskådliggörs med en modell där olika funktioner åsätts siffervärden.

Nackdelar

Det är att notera att alla bedömningar är förutsägelser om framtiden, de utgör inte sanningar (jämför *4.2.1*). Och att bedömningar som uttrycks med siffror fortfarande bara är förutsägelser.

Alla modeller (till exempel avseenden en viss risk) är per definition fel eftersom de fokuserar på de väsentligaste sammanhangen som beskriver en viss olycka. Alla andra faktorer som kan finnas runt en möjlig olyckshändelse avgränsas. Skälet härtill är att modellen annars blir för svår att hantera och bedöma. Men en del modeller är faktiskt korrekta och beskriver verkligheten väl. Det är dock svårt att veta vilken modell som råkar vara exakt innan just den olyckan har inträffat.

Fördelar

Fördelen med modellering och simulering består i att man kan teoretiskt upprepa olycksförlopp oändligt antal gånger varvid olika riskreducerande åtgärder prövas i syfte att hitta den åtgärd som ger bäst riskreducering till lägst kostnad. Om en skicklig konstruktör utför aktiviteten redan tidigt under konstruktionsfasen kan god kvalitet erhållas på riskreduceringseffekten av gjord förändring. Samtidigt blir det högre kvalitet på såväl riskanalys som bedömning av värdet av olika riskreducerande åtgärder. Och eftersom simuleringen genomförs tidigt under projektet så är åtgärden relativt sett billig och därmed effektiv.

Med fördel kan också såväl tidigare erfarenheter från tidigare system, felträd och expertuppskattning användas tillsammans med modellering och simulering för att därigenom ge bättre indata till modelleringen.

Bilaga 2 Risklogg

Bakgrund

MIL-STD-882C har omfattande brister vad avser anvisning om hur dokumentation av olycksrisk ska utföras, samt exemplifiering av lämplig struktur för utformning av lämpligt dokument. Likväl förutsätter standarden en fullvärdig riskanalys. Enda ledning härvid utgörs av en generell hänvisning till i USA på 90-talet kända dokumentmallar.

För att stödja och skapa stadga åt riskanalysarbete ges i H SystSäk ett handfast verktyg i form av en särskilt framtagen Risklogg som:

- utgör grund för projekt vid utformning av projektspecifik risklogg
- beskrivs i respektive avsnitt nedan vid samtidig redovisning av aktuell verksamhet
- är utförd i Excel och tillhandahålls på H SystSäk CDR
- ger stöd under genomförande av systemsäkerhetsverksamhet
- ansluter till handbokens modell för riskhantering
- underlättar ett systematiskt genomförande av riskhanteringen
- underlättar noggrann uppföljning av genomförd riskhantering.

Allmänt

Risklogg är ett sätt att fullständigt dokumentera uppgifter om alla enskilda risker. Riskloggen börjar föras när riskidentifiering för viss tekniskt system inleds. Riskloggen vidmakthålls och uppdateras så länge som det tekniska systemet används och vidmakthålls. I detta avsnitt presenteras en enkel men komplett risklogg som omfattar utrymme för att registrera ett grundbehov av data. Varje utvecklingsprojekt väljer att utöka riskloggen efter de behov som uppkommer. Exemplet bygger på att Excel används, vilket ger fördelar som beräkningshjälp och enkel expansion genom att kopiera och klistra in. Det är också möjligt att använda modellen med valfria hjälpmedel, där papper och penna är det allra enklaste.

Här presenterad mall till risklogg finns som fil på H SystSäk CDR.

Riskloggens grundmall innehåller fyra flikar. Den första för personskada och ekonomisk skada (egendom och miljösanering). Den andra fliken används vid olycksrisk som ger bestående miljöskada. Notera att olycksrisk som ger bestående miljöskada alltid ska hanteras som RÖD, med innebörd att denna endast kan stängas av Försvarsmakten (jämför *avsnitt 4.3.2*).

Vardera fliken omfattar initialt utrymme för endast två risker. Avsikten är att användaren själv utökar riskloggen efter behov, genom att kopiera raderna för en risk.

Nedan beskrivs riskloggens hantering med avseende på personskada (beskrivningen också tillämpbar för ekonomisk skada och viss miljöskada, se *avsnitt 4.2.3*).

Den tredje fliken Anvisningar innehåller några enkla anvisningar om hur riskloggen är avsedd att hanteras.

Tillämpning

Observera att den fjärde fliken ”Krav på risk” visar de riskmatriser som återfinns i handbokens kapitel 4. De värden som finns där ska alltid ersättas med krav från TTEM för visst utvecklings-/anskaffningsprojekt.

Översikt av risklogg

Nedan visas en starkt förminskad bild av riskloggen. Syftet är att skapa en insikt hos användaren om utseende och sammanhang. Detaljer redovisas nedan i respektive avsnitt där avsedd hantering presenteras närmare.

Riskidentifiering					
Riskid	Risknamn	Delsystem	Fara	Egenskap	Möjlig vådahändelse eller farligt tillstånd
01-001	Fall fr stege	Stege	Höjd över omgivande mark	Hög lägesenergi	Fall
					Stegen skadar byggnad
01-002	Fall fr stege	Stege	Höjd över omgivande mark	Hög lägesenergi	Fall

Riskidentifiering

Läs *avsnitt 4.2.2, Identifiering av olycksrisk* här i del 1.

Studera aktiviteterna *PHL* och *PHA* som finns beskrivna i del 2.

Riskanalysen börjar med riskidentifiering. Här gäller det att försöka hitta alla risker som det tekniska systemet innehåller eller kan ge upphov till. Börja med att leta faror genom att fundera över dels vilka riskkällor som finns och dels över vilka farliga tillstånd som finns. Identifiera den farliga egenskapen som har möjlighet (potential) att vålla skada. Definiera vilken möjlig vådahändelse som skulle kunna utlösas av den farliga egenskapen eller vilket farligt tillstånd som kan inträffa.

Om faran hör till visst delsystem är det lämpligt att ange detta.

Varje identifierad risk ges också en entydig identitet, lämpligen ett nummer. Ofta används ett tvådelat nummer där första delen anger vilket delsystem som berörs och den andra delen är ett löpnummer inom respektive grupp. För att förenkla kommunikation bör varje risk även ha ett namn som helst ska vara både kort och dessutom beskriva vad risken består av.

Riskidentifiering					
Riskid	Risknamn	Delsystem	Fara	Egenskap	Möjlig vådahändelse eller farligt tillstånd
01-001	Fall fr stege	Stege	Höjd över omgivande mark	Hög lägesenergi	Fall
					Stegen skadar byggnad
01-002	Fall fr stege	Stege	Höjd över omgivande mark	Hög lägesenergi	Fall

Behöver mallen utvidgas så måste cellerna där det står riskidentifiering delas upp innan nya kolumner kan läggas till. När detta är gjort kan översta radens celler sammanfogas igen.

Riskuppskattning

Läs *avsnitt 4.2.3, Riskuppskattning* här i del 1.

Studera aktiviteterna *PHA* och alla analysaktiviteter (SSHA, SHA, O&SHA, HHA, EHA, FHA) som finns beskrivna i del 2.

Riskuppskattningen innebär att riskernas storlek ska uppskattas. Det är en mycket svår uppgift som kräver att alla möjliga hjälpmedel och metoder används. Några metoder finns beskrivna i *bilaga 1*.

Först bedöms sannolikhet för att vådahändelsen ska inträffa och sedan bedöms sannolikheten för exponering. Sannolikheten för olycka beräknas därefter enligt formel av Excel. De rutor som är orangefärgade är alla sådana som innehåller en beräkningsformel.

Därefter ska olyckans skadeutfall bedömas. Detta görs genom att ange en procentuell fördelning mellan de fyra olika skadeutfallen. Observera att summan av de procentuella andelarna alltid ska vara 100.

Riskuppskattning				
Före åtgärd				
Sannolikhet för vådahändelse	Sannolikhet för exponering	Sannolikhet för olycka	Skadeklass	Procentuell andel
		PERSON	Dödsfall	0,1
			Allvarlig	0,9
			Mindre allvarlig	20
1,0E-02	8,0E-02	8,0E-04	Försumbar	79
		EKONOMI	$> 10^9$	0
			$10^7 – 10^9$	0
			$10^5 – 10^7$	2
1,0E-02	5,0E-06	5,0E-08	$< 10^5$	98
		PERSON	Dödsfall	
			Allvarlig	
			Mindre allvarlig	
		0,0E+00	Försumbar	
		EKONOMI	$> 10^9$	
			$10^7 – 10^9$	
			$10^5 – 10^7$	
		0,0E+00	$< 10^5$	

Riskvärdering

Läs *avsnitt 4.3, Riskvärdering*.

Riskens beräknade värde ska nu jämföras med ställt krav på individuell risk.

Identifiera för aktuell olycksrisk de fyra riskdelarnas sannolikhet. Avläs i riskmatrisen vardera riskdels placering och färg. Färgen avgör om storleken av aktuell delolycksrisk kan tolereras eller inte. Om någon de fyra riskdelarna har hamnat inom rött (gult) område, betraktas hela olycksrisken som ej tolerabel (begränsat tolerabel), och riskreducering krävs.

Beroende på vilken risknivå som risken hamnar på gäller:

- Röd risknivå = ej tolerabel

  Riskreducering måste göras för att om möjligt komma ner till grön risknivå.
- Gul risknivå = begränsat tolerabel

  Riskreducering bör göras för att om möjligt komma ner till grön risknivå
- Grön risknivå = tolerabel

  Riskreducering är inte nödvändig. Om det finns enkla riskreduceringar att göra ska de dock övervägas.

	Riskvärdering	
	Riskmatris	
Riskid (kopierad)	p för olycka med viss skadeklass	Risknivå
01-001	8,0E-07	
	7,2E-06	
	1,6E-04	
	6,3E-04	
	0,0E+00	
	0,0E+00	
	1,0E-09	
	4,9E-08	
01-002	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	

Riskreducering

Läs *avsnitt 4.3.3, Analys av alternativ*.

Alla riskreducerande åtgärder har ett pris. En del kostar mycket att genomföra, andra kanske leder till mindre bra lösningar i något avseende. Ibland kan det finnas både en kortsiktig och en långsiktig lösning.

Det finns alltid anledning att försöka skapa samt överväga alternativa åtgärder för att hitta de riskreducerande åtgärder som ger störst/bäst riskreduktion till lägst kostnad. Ibland kan kombination av flera åtgärder ge det effektivaste slutresultatet. En fullvärdig riskanalys möjliggör en sådan effektivitet.

Riskreducering	
ill åtgärd	Kostnad för åtgärd
Köp in livlina till varje exemplar av det tekniska systemet. Säkerställ att denna används (föreskrift)	50 000

Övervakning

Läs *avsnitt 4.4.3, Övervakning*.

Förväntad riskreducering av viss riskreducerande åtgärd måste verifieras. Detta kan ske genom provning eller beräkning eller en kombination av dessa.

Förnyad riskuppskattning

Den förnyade riskuppskattningen utförs för att se vad en föreslagen riskreduceringsåtgärd ger för förbättringar avseende riskvärde. Alla ingående värden kan vara förändrade efter en utförd åtgärd. Både sannolikhet för vådahändelse, sannolikhet för exponering och fördelning på skadeklasser kan ha påverkats. Riskuppskattningen utförs på samma sätt som förut.

Förnyad riskuppskattning				
Efter åtgärd				
Sannolikhet för vådahändelse	Sannolikhet för exponering	Sannolikhet för olycka	Skadeklass	Procentuell andel
		PERSON	Dödsfall	0
			Allvarlig	1
			Mindre allvarlig	10
1,0E-02	8,0E-02	**8,00E-04**	Försumbar	89
		EKONOMI	> 10^9	
			$10^7 – 10^9$	
			$10^5 – 10^7$	
		0,00E+00	< 10^5	
		PERSON	Dödsfall	
			Allvarlig	
			Mindre allvarlig	
		0,00E+00	Försumbar	
		EKONOMI	> 10^9	
			$10^7 – 10^9$	
			$10^5 – 10^7$	
		0,00E+00	< 10^5	

Förnyad riskvärdering

Riskvärderingen görs nu om med de nya förutsättningarna från den förnyade riskuppskattningen. Nu visar det sig om den verifierade riskreduceringen har lett till tillräcklig förbättring så att risknivåerna blivit gröna = tolerabla. Om förbättringen inte är tillräcklig behöver kanske ytterligare åtgärder övervägas.

När den förnyade riskvärderingen visar att verifierade riskreduceringen har lett till tillräcklig förbättring är det dags att besluta om att åtgärden ska utföras.

	Förnyad riskvärdering	
	Riskmatris	
Riskid (kopierad)	p för olycka med viss skadeklass	Risknivå
	0,0E+00	
	8,0E-06	
	8,0E-05	
01-001	7,1E-04	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
01-002	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	
	0,0E+00	

Acceptansbeslut

Acceptansbeslut innebär att risken anses vara färdighanterad för tillfället. Det finns ingen som helst begränsning i möjligheten att väcka upp en risk på nytt om nya uppgifter visar/tyder på att gjord uppskattning inte är korrekt.

En grön risk stängs/accepteras av leverantör efter kommunikation med DesignA.

En gul risk stängs/accepteras av DesignA efter förslag från leverantör. Då ska också visas att ytterligare riskreducering inte är möjlig med rimlig insats.

En röd risk kan endast stängas/accepteras av Försvarsmakten efter förslag från DesignA. Då ska det tydlig framgå att ytterligare riskreduktion inte är möjlig eller vad kostnaden skulle bli för ytterligare riskreducering.

Acceptansbeslut		
Anm	Status	Beslut

Risklogg miljö

Den andra fliken innehåller mall för riskhantering av miljörisker som leder till bestående skada. Här återfinns stora delar av fälten från den vanliga riskloggen. Riskidentifiering görs på exakt samma sätt. Riskuppskattningen är förenklad enligt nedan.

Riskuppskattning		
Före åtgärd		
Sannolikhet för vådahändelse	Sannolikhet för exponering	Sannolikhet för olycka

		MILJÖ
1,0E-07	1,0E+00	1,0E-07
		MILJÖ
		0,0E+00

Här stannar beräkningen med en sannolikhet för olycka. Därefter görs riskreducering enligt ovan varefter en förnyad riskuppskattning görs.

En miljörisk ses alltid som en röd risk och en röd risk kan endast stängas/accepteras av Försvarsmakten efter förslag från DesignA.

Bilaga 3 Övriga säkerhetsformer för tekniska system

Nedan redovisas några tillämpningsområden (för produkter/materiel/system) med dess särskilda regelverk som används för att styra genomförandet av tillhörande säkerhetsverksamhet. Angivna dokumentbeteckningar var de som var aktuella vid handbokens färdigställande. Om viss referens behöver tillämpas rekommenderas att förekomsten av senare utgåva kontrolleras.

Tillämpnings-område	Avser	Dokumentation
Ammunition och explosiva varor	Försvarsmaktens instruktion för förvaring och transport av ammunition och övriga explosiva varor	IFTEX *[21]*
Ammunitionssäkerhet	Säkerhet hos ammunition	Lagen om Brandfarliga och explosiva varor *[28]* FMV handbok för vapen- och ammunitionssäkerhet, H VAS *[11]*
Brand- och explosionsfara	Försvarsmaktens gemensamma bestämmelser för åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor med mera	BVKF
Elsäkerhet	Säkerhet mot skada på person eller egendom genom direkt eller indirekt inverkan av elektrisk ström	Ellagen *[8]* Handbok elsäkerhet, H Elsäk *[30]*
Flygsäkerhet för markbaserade system för flygtrafik- och flygstridsledning	Ledningssystemets påverkan på luftfarten/luftfartyg	LFS 2008:14 FMV AK Led Flygsäkerhetsprocess

Tillämpnings-område	Avser	Dokumentation
Fordonssäkerhet	Säkerhet hos fordon	Fordonslagen (2002:547) Fordonsförordningen (2009:211) Militärtrafikförordningen (2009:212) Vägverkets författningssamling (2003:22) FMV Handbok fordonssäkerhet *[10]*
Luftvärdighet	Säkerhet hos flygmateriel/ luftfartyg	RML, Försvarsmaktens regler för militär luftfart *[34]*
Medicinteknisk säkerhet	Medicinteknisk utrustning	Lag (1993:584) om medicintekniska produkter. Förordning (1993:876) om medicintekniska produkter
Programvara	Programvara i säkerhetskritiska tillämpningar	Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk, 2001 *[20]*
Sjövärdighet	Arbetsmiljö samt säkerhet för fartyg och dess utrustning	RMS, Försvarsmaktens regler för militär sjöfart *[36]*
Strålskydd	Radioaktiva material Materiel som förorsakar: elektromagnetisk strålning/ fält (radar), laser	Strålsäkerhetsmyndighetens regler avseende joniserande och icke joniserande strålning
Säkerhet hos förbindelsemateriel	Säkerhet hos broar och färjor med mera	För ny bromateriel Boverkets konstruktionsregler BKR: 94 (utgiven som BFS 1993:58 med ändringar BFS 1995:18) som innehåller föreskrifter och allmänna råd till Plan- och bygglagen 1987:10 För äldre bromateriel tillämpas Vägverkets publikation 1991:210 ”Bärighetsklassning av broar”. För färjor tillämpas Försvarsmaktens regler för sjövärdighet
Vapensäkerhet	Säkerhet hos vapenmateriel	FMV handbok för vapen- och ammunitionssäkerhet, H VAS *[11]*

Det finns ytterligare tillämpningsområden, vilka dock inte berörs i handboken.

Exempel är

- CBRN-materiel
- läkemedel
- master
- lyftredskap
- tryckkärl
- arbetsutrustningar.

Definitioner

För att underlätta förståelsen av i handboken använda begrepp och akronymer lämnas nedan 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, t ex befästning, kasernetablissement, basområde, förbindelser med mera. Med anläggning avses även de truppbefästningar som behövs för att lösa uppgiften. Till anläggning hänförs även anläggningsbundna förnödenheter *[32]*.
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 angiven risknivå.
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 *[18]*.
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 även *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) *[27]*.
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 *[21]*.
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 uppkomst av fel.
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 övergår systemet till 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 luftfartmyndighet.
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 *[43]*).
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 *Lifetime, 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 väpnad strid.
Militär materiel *Military equipment*	Tekniskt system som särskilt har konstruerats och tillverkats (även genom integration) för att genomföra väpnad strid.
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*	Framtida 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, inte 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, se vidare *avsnitt 4.3.1*). 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*) *[27]*.
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*	Nytt 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 exempelljud/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 *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 enligt gällande riskmatris.
System *System*	Se *Tekniskt system*.

Begrepp	Förklaring
System av system *System of systems*	Förmåga som skapas genom återanvändning 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 ohälsa. 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 6.5*.
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 inte 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. Se även *Systemsäkerhet*.

Begrepp	Förklaring
Säkerhet *Security*	Frånvaro av förhållanden som innebär spioneri, 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 requirement*	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) *[40]*] *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) *[40]* *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	Betydelse
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
BVKF	Försvarsmaktens instruktion för åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor m m
BT	Begränsat tolerabel risknivå
CAA	Civil Aviation Authority, Storbritannien
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	Le 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	Betydelse
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
EASA	Europeiska flygsäkerhetsbyrån
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 Analysis)
FLYGI	Militära flyginspektionen
FM	Försvarsmakten
FM ArbO	Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten (FFS 2009:2 med ändring FFS 2009:3)
FMEA	Feleffektanalys (Fault Modes and Effects Analysis)

Akronym/Förkortning	Betydelse
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 *[10]*
H Mål	Handbok för Försvarsmaktens framtagning av målsättningar för förband, förnödenheter och anläggningar för krigsorganisationens behov
H VAS	Handbok för 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
HTM	Halvtidsmodifiering
HTRR	Hazard Tracking and Risk Resolution
IEC	International Electrotechnical Commission

Akronym/Förkortning	Betydelse
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
MIFOR	Militära fordonsregistret
MIL-STD	Amerikansk militär standard (Military Standard)
MOTS	Militär hyllvara, färdig produkt utvecklad för militärt ändamål (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)
OHHA	Operating and Health Hazard Analysis
OPR	Office of Primary Responsibility
OPS	Offentlig privat samverkan /PPP Private-Public Partnership

Akronym/Förkortning	Betydelse
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	Produktledare
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
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

Akronym/Förkortning	Betydelse
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
SEMP	Safety and Environmental Programme Plan
SHA	Säkerhetsanalys för system (System Hazard Analysis)
SHK	Statens haverikommission
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 Safetey Evaluation)
SSHA	Säkerhetsanalys för delsystem (Sub System Hazard Analysis)
SSI	Safety Significant Item
SSMP	System Safety Management Plan
SSP	Systemsäkerhetsprogram (System Safety Program)
SSPP	Systemsäkerhetsplan (System Safety Program Plan)

Akronym/Förkortning	Betydelse
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
US	United States
UTEMU	Utkast till Teknisk-Ekonomisk Målsättning för Utbildningsmateriel

Akronym/Förkortning	Betydelse
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 är ett Europa-gemensamt regelverk för transport av farligt gods på landsväg. Den svenska versionen av regelverket heter ADR-S och ges ut av Myndigheten för samhällsskydd och beredskap (MSB). Innan MSB bildades 1 januari 2009 gavs ADR-S ut av Räddningsverket.
2	AFS 2001:1, Arbetsmiljöverkets föreskrifter om systematiskt arbetsmiljöarbete.
3	An introduction to System Safety Management and Assurance, UK MOD 2002.
4	AOP-39, Guidance on the Development, Assessment and Testing of Insensitive Munition (IM).
5	Arbetsmiljölagen (AML) (1977:1160). Lagen ändras frekvent. Regeringen har utfärdat en Arbetsmiljöförordning (1977:1066) med vissa kompletterande regler. AML ger ramen för Arbetsmiljöverkets föreskrifter (AFS). De anger mer i detalj krav och skyldigheter beträffande arbetsmiljön.
6	CE-märkning och produktsäkerhet, Arbetsmiljöverket, ADI 468.
7	Dependability management. Part 3: Application guide, section 9: Risk analysis of technological systems, International Electrotechnical Commission, 1995, IEC 60300-3-9.
8	Ellagen, SFS 1997:857 Med föreskrifterna • Starkströmsförordningen, SFS 1957:601 • Elinstallatörsförordningen, SFS 1990:806 • Elmaterielförordningen, SFS 1993:1068 • Förordningen om elektromagnetisk kompatibilitet, SFS 1993:1067.
9	Fastställande av rutin avseende leveranser av produkter från Försvarets materielverk till Försvarsmakten, fastställd med Försvarsmaktens skrivelse 14 760:900947, 2008-12-19.
10	FMV Handbok fordonssäkerhet, M7762-000511.
11	FMV Handbok för Vapen- och ammunitionssäkerhet 2000, M7762-000212, FMV H VAS (revideras vart 7:e år).

Ref nr	Titel
12	Fordonsförordningen, SFS 2009:211.
13	Fordonslagen, SFS 2002:574.
14	Förordning om brandfarliga och explosiva varor (FBE), SFS 2010:1075.
15	Förordning om medicintekniska produkter, SFS 1993:876.
16	Förordning (2007:936) om folkrättslig granskning av vapenprojekt.
17	Försvarsmakten och FMV Ändringsstyrningsprocess.
18	Försvarsmaktens föreskrifter med arbetsordning för Försvarsmakten FM ArbO), FFS 2009:2.
19	Försvarsmaktens gemensamma riskhanteringsmodell. Fastställd med Försvarsmaktens skrivelse 01 310:900666, 2008-12-12.
20	Försvarsmaktens handbok för programvara i säkerhetskritiska tillämpningar, M7762-000531 H ProgSäk, 2001.
21	Försvarsmaktens instruktion för förvaring och transport av ammunition och övriga explosiva varor, IFTEX.
22	Försvarsmaktens säkerhetsinstruktion för vapen och ammunition med mera (SäkI), Gemensam del.
23	Förtydligande av krav på systemsäkerhetsdokumentation vid fartygsutprovning, Försvarsmaktens skrivelse 14 910:75564, 2003-10-17.
24	Handbok Materielförvaltning Sjö (HMS), remitterad med HKV skr 14 600:53495, 2010-03-22.
25	HMÅL, Försvarsmaktens Handbok för målsättningsarbete, fastställd med FM skrivelse 2006-06-16, 09 100:69399.
26	Instruktion om Försvarsmaktens handbok Systemsäkerhet, beslutad med FM HKV 14 910:60223, 2010-06-08.
27	Handbok för Riskanalys, Statens Räddningsverk 2003, ISBN 91-7253-178-9.
28	Lag om brandfarliga och explosiva varor (LBE), SFS 2010:1011.
29	Lag om medicintekniska produkter, SFS 1993:584.
30	Handbok Elsäkerhet i Försvarsmakten • M7739-352015 avsedd för distribution och tillämpning inom Försvarsmakten och innehållande licensierad SS-EN standard. Versionen ska tillämpas inom Försvarsmakten av Försvarsmaktens personal. • M7739-355002 är avsedd för distribution och tillämpning utanför Försvarsmakten och innehåller inte SS-EN standard.
31	Militärtrafikförordningen, SFS 2009:212.
32	Nomen F 97 Militärhögskolan BEGREPPSKATALOG.

Ref nr	Titel
33	Plan- och bygglagen, (SFS 1987:10).
34	Regler för militär luftfart, framtagen av Försvarsmakten, RML.
35	Regler för militär markverksamhet, framtagen av Försvarsmakten, RMM.
36	Regler för militär sjöfart, framtagen av Försvarsmakten, RMS.
37	Reliability, Maintainability and Risk. David J Smith Butterworth Heinemann.
38	RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification Requirements.
39	Safety Management Requirements for Defence Systems, UK DEF STAN 00-56.
40	Samordningsavtal mellan Försvarsmakten och FMV. Samordningsavtal mellan Försvarsmakten och FOI respektive FORTV med tillkommande överenskommelser om systemsäkerhetsverksamhet (uppdateras med viss regelbundenhet och diarieförs under nr 03 200 som skrivelser).
41	Sjölagen, SFS 1994:1009.
42	Sprängämnesinspektionens föreskrifter (SÄIFS 1997:5) om import och om överföring av explosiva varor med ändringar i SÄIFS 1999:3.
43	STANAG 2418, Procedures for Expedient Repair including Battle Damage Repair.
44	STANAG 4439, Policy for Introduction and Testing for Insensitive Munition (IM).
45	Standard best practices for system safety program development and execution, ISO/GEIA-STD-0010.
46	System Safety Program Requirements, MIL-STD-882C.
47	The Tolerability of Risk from Nuclear Power Stations. UK HMSO 1992.
48	Värdering av risk, Räddningsverket Karlstad 1997, ISBN 91-88890-82-1.

Bildförteckning

Tabellförteckning

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