FÖRSVARSMAKTEN

Handbok

Handbok Systemsäkerhet

2022

Handbok Systemsäkerhet

H SYSTSÄK 2022

Bilder på omslaget: Framsida: /Försvarsmakten
Grafisk bearbetning: FMLOG/Försörjning, Grafisk produktion
Produktionsid: 220317036
M-nr: M7739-352022
Produktionsformat: InDesign, G5
Publikationsområde: C RPE PUBL
Tryck: Försvarsmakten, FMLOG

VIDAR-handling: **FM2021-9449:4**

Beslut om fastställande av Handbok Systemsäkerhet 2022

Handbok Systemsäkerhet (H SystSäk 2022) version 3.0 fastställs att gällafrån och med 2022-09-01.

Publikationens registrerade M-nr är M7739-352022.

Följande upphävs 2022-09-01:
M7739-352023 Handbok Systemsäkerhet 2011 del 2 – Metoder gällande från och med 2011-01-01.

M7739-352031 Handbook on System Safety 2011 part 1 – Commonmed gällande från och med 2012-01-01.

M7739-352032 Handbook on System Safety 2011 part 2 – Methods gällande från och med 2012-01-01.

Publikationen tillgängliggörs genom publicering på intranätet emilia och www.forsvarsmakten.se.

Publikationen distribueras och lagerhålls vid FMCL/FBF.

Detta beslut är fattat av brigadgeneral Jonas Lotsne. I den slutliga handläggningen har som föredragande deltagit överste Joakim Sellén.

Jonas Lotsne
Resursproduktionschef

Joakim Sellén

Ändringar

Version	Ändring nr	Datum för när versionen börjar gälla/ska tillämpas	Vidar-handlingsnr	Anmärkning
1.0	0	1996-11-01	14 910:72214	Utgivningsår 1996
2.0	1	2011-01-01	14 910:60224	Utgivningsår 2011
3.0	2	2022-09-01	FM2021-9449:4	Utgivningsår 2022

Förslag till förbättringar av Handbok Systemsäkerhet skickas till:

Försvarsmaktens Högkvarter
Materielproduktion
107 85 Stockholm

e-post: materielproduktion@mil.se; systemsakerhet.fmv@fmv.se
Skriv i ämnesraden: H SYSTSÄK 2022 – Ändringsförslag

Förord

Den här handboken innehåller anvisningar med förklaringar och beskrivningar med Försvarsmaktens krav på systemsäkerhetsverksamhet för grundläggande riskhantering, kravställning på tekniska system och produkter samt de aktiviteter, verktyg och beslut som ingår i Försvarsmaktens systemsäkerhetsmetodik.

Målgrupp för handboken är alla befattningshavare som är delaktiga inom Försvarsmaktens materielförsörjning.

Syftet med handboken är att bidra till att det militära försvarets behov av säker materiel, relaterad forskning, teknikutveckling och tjänster tillgodoses i alla beredskapsnivåer.

Det är medarbetare vid Försvarsmakten och FMV som tillsammans hanterar Försvarsmaktens materiel från idé till avveckling. Det innebär att alla inblandade i ett materielanskaffningsprojekt ska säkerställa att försvarsmateriel utformas och anpassas så att den passar i Försvarsmaktens olika miljöer och att den är säker att använda. Handboken ska utgöra ett naturligt stöd för alla befattningshavare som är delaktiga inom Försvarsmaktens materielförsörjning. Den redogör, förutom för försvarsmaktsperspektivet, även för andra aktörers bidrag till Försvarsmaktens systemsäkerhetsverksamhet.

Såväl utveckling av försvarsförmågor som vidmakthållande av dem bygger ett starkare försvar. Den materiella komponenten är en bärande del i tillväxten. Kortare leveranstider bör eftersträvas och forcerad anskaffning kan bli nödvändig. För att lyckas väl med dessa ansatser bör en strävan vara att bland annat begränsa mängden särkrav. Ett systematiskt kravarbete ska lägga grunden för en ändamålsenlig materielförsörjning.

Försvarsmaktens systemsäkerhetsarbete syftar till att olycksrisker i förbandsverksamheten vid utbildning, övning, insats, materielunderhåll, transport, förrådshållning samt avveckling, hålls så låga som möjligt. Detta sker dels genom ett systematiskt arbetsmiljöarbete för att öka säkerhetsmedvetandet hos den enskilde användaren, dels genom att ställa rätt systemsäkerhetskrav på den materiel som ska anskaffas eller modifieras.

Försvarsmaktens systemsäkerhetsarbete samverkar med flera olika kompetensområden. Miljöarbete, för att värna om vår yttre miljö. Användbarhet och genusperspektiv så att materielen utformas lämpligt för alla kvinnor och män.

För att uppfylla Försvarsmaktens krav på systemsäkerhet är det en förutsättning att samtliga aktörer, inom eller utom Försvarsmakten, under materielens samtliga livscykelskeden följer de principer som beskrivs i Handbok Systemsäkerhet 2022.

Handboken gäller i fred och hela konfliktskalan.

Innehållet i denna publikation omfattas inte av sekretess.

Läsanvisning

Handboken är dels strukturerad för att läsas i kapitelordning, dels indelad blockvis för genomförande av systemsäkerhetsverksamhet för tekniska system och produkter under alla livscykelskeden.

För den som är ny inom systemsäkerhetsområdet föreslås först kapitel 1–4 och därefter kapitel 5–9. För den som ska påbörja ett systemsäkerhetsarbete läses kapitel 10 och framåt.

Handboken är indelad enligt följande:

Kapitel 1–4	Syfte, systemsäkerhetsverksamhet samt roller och ansvar
Kapitel 5–9	Lagstiftning, standarder, Försvarsmaktens regelverk samt språk
Kapitel 10–12	Tekniska system, Vägvalsmodellen, val av systemsäkerhets-aktiviteter
Kapitel 13–16	Olycksmodellen, riskhanteringsmetodik och systemsäkerhets-värdering
Kapitel 17	Beslutssystem
Kapitel 18–19	Ändring (modifiering) samt avveckling
Bilaga 1	EU-rätt och svensk lagstiftning
Bilaga 2	Standarder
Bilaga 3	Systemsäkerhetsaktiviteter

Innehåll

1 Inledning

Syftet med detta kapitel är att beskriva systemsäkerhetsverksamhetens syfte, vision och grunder för tekniska system och produkter som anskaffas, genomgår ändring (modifiering) och som brukas av Försvarsmakten.

1.1 Syfte

Systemsäkerhetsverksamheten syftar till att säkerställa att de olycksrisker som identifieras hålls så låga som möjligt under det tekniska systemets eller produktens hela livslängd. Detta innefattar utveckling, användning (utbildning, övning och insats), underhåll, förrådshållning, transport, ändring (modifiering) och vid avveckling av materielen.

I första hand ska lagstiftningen uppfyllas utan att tillämpa undantag för militär materiel. Detta gäller under alla konfliktnivåer. Systemsäkerhetsmetodiken används för att komplettera lagstiftningen där undantag för militär materiel medges och är befogat eller där ytterligare säkerhetshöjande åtgärder erfordras för tekniska system och produkter.

Vision för systemsäkerhetsverksamheten

”Ingen person (soldat, sjöman, officer eller civil), egendom eller yttre miljö ska oavsiktligt skadas av Försvarsmaktens tekniska system.”

1.2 Bakgrund

Arbetsgruppen för Ammunitionssäkerhet (Ag SAM, 1970-09-28) med representanter från Försvarets materielverk (FMV), dåvarande Försvarets forskningsanstalt (FOA) och berörd svensk industri sammanställde i mitten av 1970-talet en handbok med erfarenheter från ammunitionsområdet, Handbok Ammunitionssäkerhet. I handboken, som sedan dess har utvecklats successivt, fanns ett särskilt avsnitt om säkerhetsmetodik. I början av 1990-talet beslutade Försvarsmakten att systemsäkerhetsmetodiken ska tillämpas på all materiel.

År 1996 fastställde ÖB den första utgåvan av Handbok Systemsäkerhet. Handbok Systemsäkerhet 2022 (H SystSäk 2022) är en vidareutveckling av tidigare utgåvor (H SystSäk 1996 och 2011) och innehåller Försvarsmaktens riktlinjer för genomförande av systemsäkerhetsverksamheten.

Denna utgåva av H Systsäk har utarbetats för att ge ett bättre stöd för systemsäkerhetsverksamheten i Försvarsmakten, presentera en utvecklad modell för systemsäkerhetsvärdering, beskriva roller och ansvar samt att delar av MIL-STD-882E är inarbetade.

1.3 Grunder

Försvarsmaktens huvuduppgift är att med militära medel försvara Sverige och främja samhällets säkerhet. För att nå framgång i strid krävs användning av materiel som kan sätta en motståndare ur spel. Användarna som brukar militär materiel måste känna tilltro till att materielen fungerar på avsett sätt och inte skadar dem själva. Detta gäller även för övrig personal som på olika sätt hanterar materielen, exempelvis vid underhåll eller transport.

Försvarsmakten har att hantera risker vid all verksamhet så att författningsenliga krav på arbetsmiljö och säkerhet för Försvarsmaktens personal, samt kraven på att säkerhet för tredje person, egendom och yttre miljö uppfylls. Försvarsmaktens arbete syftar till att olycksrisker i all verksamhet hålls så låga som möjligt. Detta sker dels genom ett systematiskt arbetsmiljöarbete för att reducera verksamhetens olycksrisker och öka säkerhetsmedvetandet hos all personal, dels genom att ställa krav på den materiel som används i verksamheten. Detta innebär i förlängningen att materielen både ska uppfylla lagstiftningen och ha erforderliga egenskaper för att skydda och försvara Sverige, men även för genomförande av organiserad väpnad strid. Systemsäkerhetsverksamheten är ett stöd så att Försvarsmakten kan ta sitt arbetsmiljö- och arbetsgivaransvar, samt att även förebygga och ta ansvar för risker som påverkar tredje person, egendom och yttre miljö.

Försvarsmakten eftersträvar att nå samhällets accepterade risknivåer för tekniska system och produkter genom att följa lagstiftningen med så få undantag som möjligt för militär materiel.

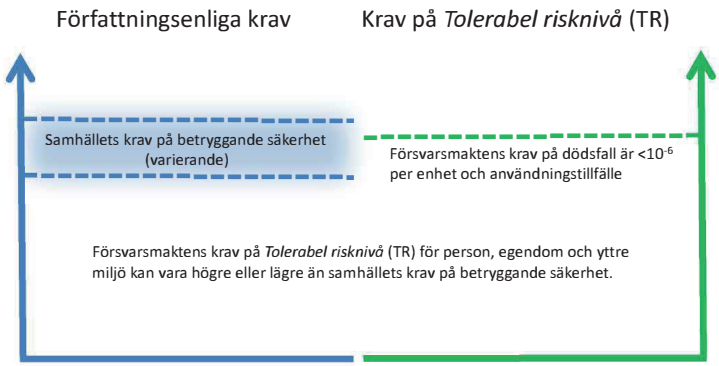
Försvarsmakten har tekniskt designansvar för all anskaffad materiel (ny eller modifierad) samt ansvarar för att leda systemsäkerhetsverksamheten så att materielen kan bibehålla betryggande säkerhet under hela dess livslängd. Innan materielen tas i bruk ska den därför ha genomgått erforderligt systemsäkerhetsarbete och beslutats vara tillräckligt säker för den tänkta (avsedda) användningen.

Försvarsmakten har även tekniskt designansvar för tekniska system och produkter som utvecklas i egen regi eller ändras (modifieras) inom egen organisation, exempelvis vid Försvarsmaktens verkstäder.

FMV har i sin roll som stödmyndighet till Försvarsmakten ett ansvar att överlämna tekniska system och produkter som uppfyller lagstiftningen och de av Försvarsmakten ställda systemsäkerhetskraven. De tjänster som FMV utför som stöd till Försvarsmakten ska också vara kvalitetssäkrade så att lagstiftning och ställda systemsäkerhetskrav uppfylls.

Lagstiftningen innehåller krav på vilka säkerhetsegenskaper olika typer av materiel (även utrustningar och förbrukningsmateriel), arbetslokaler med mera ska ha för att få överlämnas, tas i bruk respektive marknadsföras. Lagstiftningen lämnar i vissa fall undantag för militär materiel respektive militärt ändamål. Militärt ändamål kan innebära att Försvarsmakten behöver andra eller strängare systemsäkerhetskrav på materielen än vad lagstiftningen föreskriver. Detta kan exempelvis meddelas genom Försvarsmaktens interna bestämmelser (FIB), *Designregler* (DR) eller kravställning i målsättningar.

Betryggande säkerhet är samhällets accepterade risknivå och uppnås genom att följa lagstiftningen. *Tolerabel risknivå* (TR) är Försvarsmaktens accepterade risknivå för olycksrisker som behöver värderas i en riskmatris och där acceptansnivån kan vara både högre eller lägre än betryggande säkerhet.



Tabell 1.1 Samhällets krav på betryggande säkerhet kan skilja sig från Försvarsmaktens krav.

Försvarsmakten eftersträvar så få undantag som möjligt från lagstiftningen för så kallad militär materiel. Dels av systemsäkerhetskäl, dels av ekonomiska och tidsmässiga skäl vid anskaffning.

Vanligtvis använder Försvarsmakten tekniska system och produkter integrerat eller i samfunktion med andra tekniska system och då behöver ett kompletterande systemsäkerhetsarbete genomföras.

Tekniska system består ofta av flera olika produkter och komponenter. System-av-system består av flera tekniska system, vilket gör att systemsäkerhetsarbetet för helheten kan komma att bygga på underlag som tagits fram genom flera olika angreppssätt. Exempelvis kan olika tekniska eller systemsäkerhetsstandarder ha tillämpats i systemsäkerhetsarbetet för skilda delsystem. Vid ett uttalande om den samlade säkerheten för ett system-av-system behöver detta belysas.

Om systemsäkerhetsarbetet genomförs utifrån en annan etablerad systemsäkerhetsstandard än MIL-STD-882E, kan systemsäkerhetsarbetet dels behöva kompletteras med exempelvis de unika svenska aktiviteterna, dels med en korsreferenslista mellan de olika standarderna.

1.4 Begrepp inom systemsäkerhetsområdet

För systemsäkerhetsområdet används följande beskrivningar av olika begrepp:

- **Verksamhetssäkerhet** ur systemsäkerhetsperspektiv avser Försvarsmaktens förmåga att hantera olycksrisker vid all verksamhet så att de författningsenliga kraven på arbetsmiljö och säkerhet för Försvarsmaktens personal samt säkerhet för tredje person, egendom och yttre miljö uppfylls.
- **Systemsäkerhet** definieras av Försvarsmakten som:

> *”Egenskapen hos ett tekniskt system att inte oavsiktligt orsaka skada på person, egendom eller yttre miljö”*

Kommentar: Med att oavsiktligt orsaka personskada avses dödsfall, fysisk skada eller ohälsa på egen personal eller tredje person. Med att oavsiktligt orsaka egendomsskada avses skada på Försvarsmaktens egna tekniska system och anläggningar eller annans egendom såsom fastigheter, fordon och husdjur. Med att oavsiktligt orsaka skada på yttre miljö avses negativ påverkan på miljön, exempelvis förorenade vattentäkter eller störningar i ekosystemet. Med ”oavsiktligt orsaka” menas olyckshändelse.

- **Säkerhetsmål** är den övergripande inriktningen avseende vilken tolerabel risk en verksamhet kan acceptera. Säkerhetsmålen definierar vilka risker organisationen och omgivningen utsätts för när tekniken inom en funktionskedja inte fungerar som avsett. Säkerhetsmål definieras utifrån de mest säkerhetskritiska funktionskedjorna inom respektive teknisk arena (armén, marinen, flyg, ledning och logistik) som Försvarsmakten behöver upprätthålla för att kunna genomföra de uppdrag som anges i förordningen med instruktion till Försvarsmakten.
- **Systemsäkerhetsmål** är de mål ett produktområde eller tekniskt system har för att uppfylla *Tolerabel risknivå* (TR) för att kunna uppfylla sin del i en funktionskedja. Systemsäkerhetskraven som följer blir då beroende av om produktområdet ingår i ett säkerhetsmål som definieras per arena.
- **Tekniskt designansvar** innebär att fastställd design för tillåtna konfigurationer av tekniska system (inklusive underhållslösningar) uppfyller lagkrav, fastställda målsättningar och övriga krav bland annat avseende prestanda, funktion, informations- och systemsäkerhet över hela livscykeln.

- **Militärt ändamål** ur systemsäkerhetsperspektiv är en militär verksamhet som endast är tillåten att genomföras av Försvarsmakten under övning och insats.
- **Militär materiel** ur systemsäkerhetsperspektiv har konstruerats och tillverkats (även genom integration till ett system-av-system) för militärt ändamål, där regelverk kan medge undantag eller där civila standarder saknas.

  Kommentar: Notera att det i vissa regelverk medges undantag för tekniska system och produkter som används av Försvarsmakten. I begreppet *militär materiel* inkluderas liknande termer som *militär utrustning* och *militär produkt.*
- **Militär materiel särskilt konstruerad och tillverkad för visst militärt ändamå**l ur systemsäkerhetsperspektiv är när ett tekniskt system har konstruerats och tillverkats (även genom integration till ett system-av-system) för att i sin militära funktion (organiserad väpnad strid) ha en direkt förstörelsebringande effekt.
- **Betryggande säkerhet** är samhällets accepterade risknivå och uppnås genom att följa lagstiftningen.
- **Tolerabel risknivå** är Försvarsmaktens accepterade risknivå för olycksrisker som behöver värderas i en riskmatris och där acceptansnivån kan vara både högre eller lägre än betryggande säkerhet.

1.5 Tillämpning

Syftet med detta avsnitt är att beskriva hur handboken ska tillämpas i relation till andra regelverk samt till andra myndigheter och organisationer.

1.5.1 Handbokens status

Handbok Systemsäkerhet redogör för Försvarsmaktens systemsäkerhetsverkssamhet, vilken ska genomföras under materielens hela livscykel.

Handboken innehåller anvisningar med förklaringar och beskrivningar avseende systemsäkerhetsverksamheten samt beskriver erforderlig administration och förvaltning. Handboken relaterar till EU-rätt, svensk lagstiftning, standarder, Försvarsmaktens regelverk och andra handböcker. Handboken innehåller även riktlinjer, processer, rutiner, råd och rekommendationer med bilder för tillämpning, vilka alltid bör följas om inte särskilda skäl föreligger att genomföra systemsäkerhetsverksamheten på annat sätt.

Handboken beskriver roller, metoder och beslutssystem. Vidare beskrivs tillämpning av systemsäkerhetsmetodiken, aktiviteter och verktyg samt hur resultaten kan dokumenteras. Val av aktiviteter och vilka dokument, beskrivna i handboken, som ska användas i det enskilda fallet måste alltid anpassas efter aktuellt tekniskt system, dess funktion, komplexitet, användning och bedömda riskinnehåll.

Om det vid tillämpning av systemsäkerhetsmetodiken enligt denna handbok uppstår konflikt med EU-rätt, svensk lagstiftning eller andra regelverk för mark-, sjö- eller flygsäkerhet, så äger dessa företräden.

1.5.2 Tillämpning mellan olika myndigheter

Handbok Systemsäkerhet kan dels tillämpas frivilligt, dels göras tvingande genom direktiv inom en myndighet. För att innehållet i handboken ska vara bindande mellan två eller flera aktörer krävs kontrakt, avtal eller överenskommelser mellan parterna som reglerar omfattningen av tillämpningen, inbördes ansvar och åtagande mm.

Försvarsmakten ställer krav på omfattningen av den systemsäkerhetsverksamhet som ska bedrivas tillsammans med olika myndigheter. Detta kan ske i samordningsöverenskommelser mellan Försvarsmakten och respektive myndighet eller direkt i en beställning.

Mellan Försvarsmakten och FMV finns en samordningsöverenskommelse (SAMO FM – FMV). Av denna framgår att FMV följer de föreskrifter och handböcker som Försvarsmakten fastställer inom systemsäkerhetsområdet samt ansvarar för att motsvarande verksamhet genomförs hos utvecklande industri och hos stödjande myndigheter i materielprojekt under de skeden när FMV är tekniskt designansvarig.

1.5.3 Tillämpning internationellt

Vid framtagning av denna handbok har hänsyn tagits till EU-rätt och etablerade standarder som används internationellt, varför handboken bedöms vara tillämplig i sin helhet även vid internationellt samarbete och anskaffning. Då utvecklingsuppdrag läggs hos en utländsk leverantör (industri eller stat) ska systemsäkerhetsverksamhet avtalas och genomföras enligt samma förfarande som hos industrier i Sverige.

2 Försvarsmaktens ledning av systemsäkerhet

Syftet med detta kapitel är att beskriva Försvarsmaktens ledning av systemsäkerhetsverksamheten så att tekniska system och produkter kan uppnå och bibehålla betryggande säkerhet över tid. Vidare beskrivs närliggande områden och hur dessa kan inverka vid genomförande av systemsäkerhetsarbete.

Systemsäkerhet

”Egenskapen hos ett tekniskt system att inte oavsiktligt orsaka skada på person, egendom eller yttre miljö.”

2.1 Säkerhetskultur och riskmedvetande

Försvarsmaktens huvuduppgift är att försvara Sverige mot ett väpnat angrepp och därmed hävda Sveriges territoriella integritet. Försvarsmakten ska kunna utföra sina uppgifter självständigt eller i samverkan med andra myndigheter, stater och organisationer. Försvarsmakten ska med myndighetens befintliga förmåga och resurser kunna främja samhällets säkerhet vid svåra påfrestningar.

Försvarsmakten genomför utbildning och övning, och för att under insats nå framgång krävs användning av materiel som kan innehålla stora mängder energi för att sätta en motståndare ur spel. Användarna måste känna tilltro till att materielen inte skadar dem själva. Detta gäller även för övrig personal som på olika sätt hanterar materielen, exempelvis vid underhåll, förrådshantering eller under transport.

Försvarsmakten ansvarar för verksamhetssäkerheten där delar av den har koppling till systemsäkerhetsverksamheten. Med verksamhetssäkerhet avses Försvarsmaktens förmåga att dels hantera risker vid all verksamhet så att författningsenliga krav på arbetsmiljö och säkerhet för Försvarsmaktens personal uppfylls, dels att krav på säkerhet för tredje person, egendom och yttre miljö beaktas. För detta ändamål finns säkerhetsmål och begreppet tolerabel risk för att kunna göra lämpliga avvägningar inför olika insatser. Verksamhetssäkerhetsarbete omfattar regelgivning, genomförande av verksamhet enligt uppsatta regelverk, samt uppföljning av att så sker.

Försvarsmaktens säkerhetsledning definieras som alla åtgärder olika organisatoriska enheter genomför, vilka syftar till att höja *säkerhetskulturen* och *riskmedvetandet* i organisationen. Säkerhetsledningen ska bland annat definiera policys, organisationens befogenheter och resurser, arbetsmetoder, kravställning, utbildning, förebyggande av olyckor, olycks- och tillbudsrapportering, uppföljning och korrigerande åtgärder samt tillsyn och inspektion.

Samhällets begrepp *säkerhetskultur* definieras som den samling av egenskaper och attityder i organisationen och hos individer som säkerställer att säkerhetsfrågor får den uppmärksamhet som behövs. Organisationen med sina medarbetare strävar ständigt efter så hög säkerhet som möjligt.

Försvarsmakten använder begreppet *riskmedvetande*. Ett högt riskmedvetande är en förutsättning för att Försvarsmakten säkerhetsledning efterlevs, samtidigt som en ansvarsfull tillämpning kan höja riskmedvetandet inom organisationen. För att ett högt riskmedvetande ska utvecklas krävs en atmosfär i vilken individer inte straffas eller anklagas, eller erhåller hot om detta, för sina oavsiktliga misstag. Dock ska en individ som gör sig skyldig till sabotage eller en medveten försummelse naturligtvis inte gå fri från sitt ansvar.

Ett högt riskmedvetande utmärks av berörd personals positiva engagemang och delaktighet. Endast genom ett gott riskmedvetande finns förutsättningar för ständiga förbättringar för att effektivt kunna ta hand om de olycksrisker som identifieras under verksamhetens genomförande, och åtgärda dessa redan innan de orsakar olyckor, tillbud eller avvikelser. En avgörande framgångsfaktor är att lära sig av olyckor, tillbud och misstag, istället för att utkräva ansvar.

Som exempel blev Försvarsmaktens flygsäkerhetsarbete internationellt erkänt för sin säkerhetskultur genom att fokusera på öppenhet, transparens och lärande istället för att primärt utkräva ansvar vid olyckor, tillbud och misstag.

2.2 Systemsäkerhetsverksamhet

Syftet med systemsäkerhetsverksamheten är att sträva efter att nå Försvarsmaktens vision för systemsäkerhet. Systemsäkerhetsverksamheten används för att inom lagstiftningens ramar se till att tekniska system och produkter erbjuder betryggande säkerhet. Detta sker genom att tillämpa systemsäkerhetsmetodiken för att

komplettera lagstiftningen där undantag för militär materiel medges eller där ytterligare säkerhetshöjande åtgärder erfordras på tekniska system och produkter.

Försvarsmaktens verksamhet omfattar såväl personal, tekniska system som organisation. Civilt brukar detta benämnas människa, teknik och organisation (MTO). Olycksrisker existerar om brister finns inom eller i interaktionen mellan dessa områden. Ett systematiskt systemsäkerhetsarbete för tekniska system kan eliminera eller minimera dessa olycksrisker.

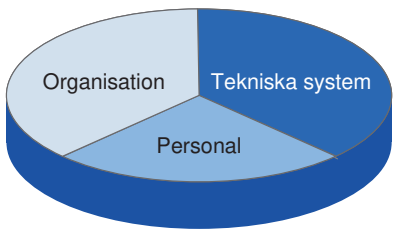


Bild 2.1 *Försvarsmaktens verksamhetssäkerhet innefattar organisation, personal samt tekniska system och produkter.*

Försvarsmaktens systemsäkerhetsverksamhet omfattar metodik för att uppnå och bibehålla betryggande säkerhet hos tekniska system och produkter samt i användningen av dessa i förbandsverksamheten.

Försvarsmakten ska utifrån verksamhetens behov och tidigare erfarenheter av liknande tekniska system, formulera systemsäkerhetskrav på nya eller ändrade (modifierade) tekniska system, eller för ändrat användningsområde. Desto tydligare och mer precisa krav som ställs på tänkt användning, ju mer heltäckande systemsäkerhetsarbete kan leverantören genomföra. Om tänkt användning inte är angiven eller är vagt beskriven, kommer leverantörens systemsäkerhetsarbete i huvudsak att bygga på den användning som leverantören antar att systemet ska få och Försvarsmakten behöver då genomföra ett mer omfattande verksamhetssäkerhetsarbete kopplat till användningen innan systemet kan tas i bruk.

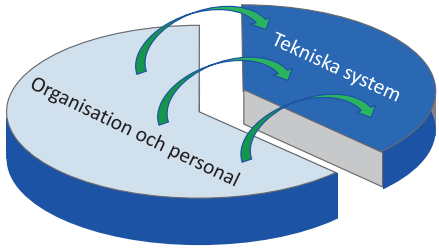


Bild 2.2 *Krav på tekniska system och systemsäkerhetsarbete från organisation och personal.*

Leverantörens systemsäkerhetsarbete kommer aldrig att vara mer heltäckande än det som beskrivits i olika målsättningsdokument. Det som inte har beskrivits riskerar därför att i slutänden skapa begränsningar som inskränker Försvarsmaktens tänkta användning. Försvarsmakten får hantera kvarvarande olycksrisker genom verksamhetsregler innan system kan tas i bruk. När tekniska system och produkter fallerar så är det organisationen och personalen som får kompensera dessa brister inom ramen för verksamhetssäkerheten.

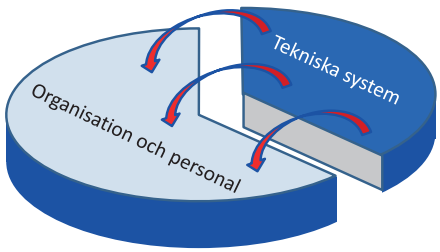


Bild 2.3 *Försvarsmakten får hantera kvarstående olycksrisker hos tekniska system och produkter genom verksamhetsregler.*

Säkerhetsmål ger övergripande krav avseende vilken tolerabel risk en verksamhet kan acceptera. Säkerhetsmålen definierar vilka risker organisationen och omgivningen utsätts för när tekniken inom en funktionskedja inte fungerar som avsett. Säkerhetsmål definieras utifrån de mest säkerhetskritiska funktionskedjorna inom respektive teknisk arena (armén, marinen, flyg, ledning och logistik) som Försvarsmakten behöver upprätthålla. Utifrån säkerhetsmålen kan specifika systemsäkerhetsmål för ett visst produktområde utarbetas och anges i *Systemsäkerhetsledningsplanen* (SSMP). För tekniska system och produkter ställs systemsäkerhetskrav i aktuell *Systemmålsättning* (SMS). Dessa systemsäkerhetsmål och systemsäkerhetskrav omsätts därefter i *Förfrågningsunderlag* (RFP).

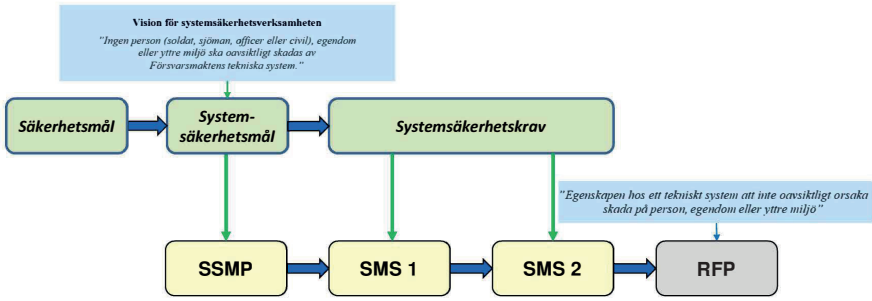


Bild 2.4 *Från säkerhetsmål till nedbrutna krav i Förfrågningsunderlag (RFP).*

2.3 Systemsäkerhetsarbete, krav- och beslutssystem

Försvarsmakten tillämpar ett krav- och beslutssystem för tekniska system och produkter. Alla aktörer i sina skilda roller deltar på olika sätt i systemsäkerhetsarbetet med nya eller ändrade (modifierade) tekniska system och produkter. I det gemensamma systemsäkerhetsarbetet eftersträvas att de kvarvarande olycksriskerna ska vara få till antalet samt vara tolerabla.

Genom en god säkerhetskultur och riskmedvetande vid Försvarsmakten finns erfarenheter som kan användas vid målsättningsarbete för att framtida tekniska system ska bli ännu säkrare att använda, underhålla, förrådshålla, transportera samt avveckla.

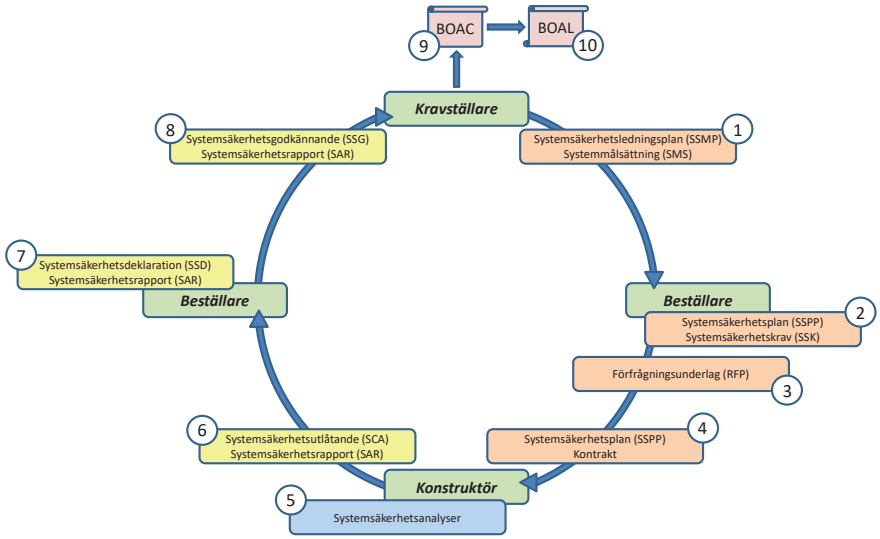


Bild 2.5 Försvarsmaktens krav- och beslutssystem för tekniska system och produkter.

Nedan förklaras de olika punkterna i bilden ovan.

1. Försvarsmakten i rollen som *kravställare* utarbetar en *Systemsäkerhetsledningsplan* (SSMP) för ett produktområde samt erforderligt antal *Systemmålsättningar* (SMS) för olika tekniska system och produkter. Systemsäkerhetskrav ska definieras i *Systemmålsättningen* (SMS).
2. Försvarsmakten eller FMV i rollen som *beställare* skriver en *Systemsäkerhetsplan (*SSPP) för det systemsäkerhetsarbete som denne behöver genomföra. Vidare genomförs *Systemsäkerhetskrav* (SSK) i syfte att identifiera EU-rätt, svensk lagstiftning, standarder, andra regelverk, *Designregler* (DR) samt konstruktionskrav.
3. Utifrån *Systemsäkerhetskrav* (SSK) formuleras tekniska krav och verksamhetsåtagandekrav, vilka fördelas till olika *Förfrågningsunderlag* (RFP).
4. Försvarsmakten eller industrin i rollen som *konstruktör* erhåller kontrakt (eller motsvarande) och utarbetar en *Systemsäkerhetsplan* (SSPP) som en del av avtalet.
5. *Konstruktör*en genomför systemsäkerhetsarbete och *beställaren* följer kontinuerligt upp *konstruktörens* systemsäkerhetsarbete.

6. *Konstruktören* utfärdar ett S*ystemsäkerhetsutlåtand*e (SCA) med erforderlig riskdokumentation, exempelvis *Systemsäkerhetsrapport (*SAR) och *Risklogg* (RL).
7. *Beställaren* granskar *konstruktörens Systemsäkerhetsutlåtande* (SCA). Därefter utfärdas en *Systemsäkerhetsdeklaration* (SSD) med erforderlig riskdokumentation, exempelvis S*ystemsäkerhetsrapport* (SAR) och *Risklogg* (RL).
8. *Kravställaren* granskar *beställarens Systemsäkerhetsdeklaration* (SSD). Därefter utfärdas ett *Systemsäkerhetsgodkännande* (SSG) med erforderlig riskdokumentation.
9. *Kravställarens Systemsäkerhetsgodkännande* (SSG) ingår i beslutsgrind *Beslut om användning, central nivå* (BOAC) och efter detta beslut kan det tekniska systemet eller produkten tas i bruk på central nivå.
10. *Chef för organisationsenhet* (C OrgE) fattar, om det är nödvändigt, *Beslut om användning, lokal nivå* (BOAL) och det tekniska systemet eller produkten kan därmed tas i bruk på lokal nivå.

2.4 Systemsäkerhetsarbete, tekniska system och produkter

Systemsäkerhetsarbete för tekniska system eller produkter syftar till att identifiera, analysera, värdera, klassificera och riskreducera identifierade olycksrisker. Dessa olycksrisker kan inledningsvis vara diffusa men genom ett strukturerat systemsäkerhetsarbete hos de olika aktörerna klarläggs olycksriskerna och riskreducerande åtgärder kan vidtas.

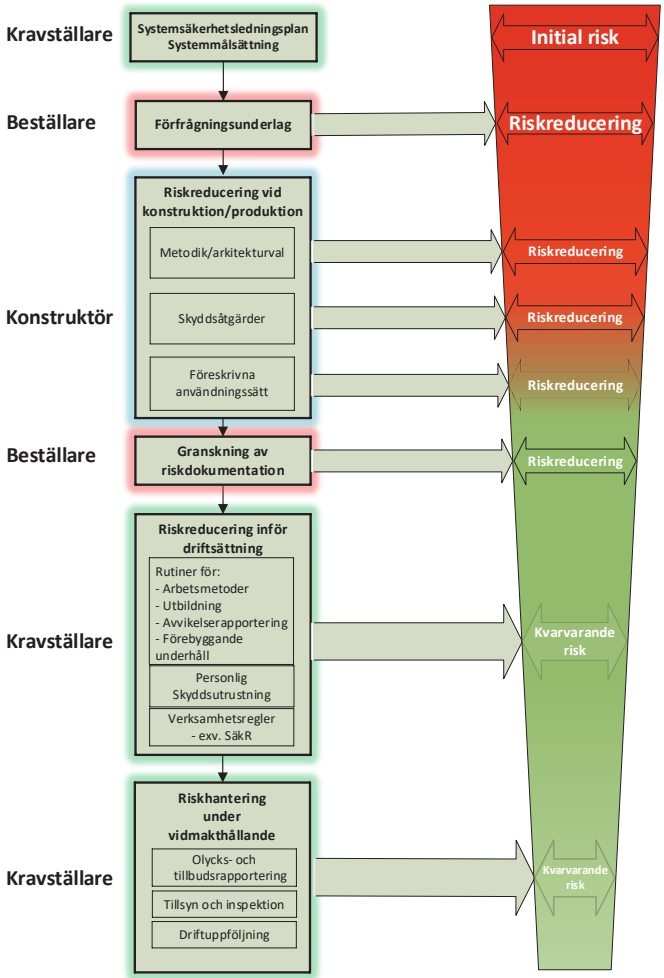


Bild 2.6 *Olika aktörers bidrag i arbetet med riskeliminering, riskreducering och hantering av kvarvarande olycksrisker.*

Försvarsmaktens befintliga och framtida tekniska system och produkter ingår i olika *Systemsäkerhetsledningsplaner* (SSMP) på produktområdesnivå. Dessa innehåller dels krav på systemsäkerhetsverksamhet, dels systemsäkerhetsmål för betryggande säkerhet utifrån EU-rätt/svensk lagstiftning, dels *Tolerabel risknivå* (TR) uttryckt i riskmatriser för tolerabla skador på person, egendom och graden av negativ påverkan på yttre miljö.

I *Systemmålsättningen* (SMS) refereras till aktuell *Systemsäkerhetsledningsplan* (SSMP). I *Systemmålsättningen* (SMS) ställs krav på systemsäkerhetsarbete samt specifika systemsäkerhetskrav på det aktuella tekniska systemet.

Systemsäkerhetskraven i *Systemmålsättningen* (SMS) realiseras till ett eller flera olika *Förfrågningsunderlag* (RFP). *Förfrågningsunderlag* (RFP) innehåller mätbara krav på det tekniska systemet, dess tänkta användning samt på förväntat systemsäkerhetsarbete och systemsäkerhetsdokumentation. Vidare ställs krav på betryggande säkerhet respektive *Tolerabel risknivå* (TR) som mått på acceptansnivå för eventuella kvarvarande olycksrisker.

Konstruktörens val av arkitektur, systemlösningar och riskkällor dimensionerar riskinnehållet i det tekniska systemet. Olyckliga eller ogenomtänkta val kan sällan kompenseras med olika typer av skyddsåtgärder eller föreskrivna användningssätt. *Konstruktören* använder med fördel olika typer av standarder och *Designregler* (DR) då dessa beskriver säkra konstruktionsprinciper.

Inför det att Försvarsmakten ska ta nya eller ändrade (modifierade) tekniska system i bruk behöver noggranna överväganden ske för varje identifierad kvarvarande olycksrisk. Detta innebär att varje sådan olycksrisk till sin art ska vara känd, vid behov åtgärdats och att acceptansbeslut är fattat. De kvarvarande olycksriskerna kan även omhändertas genom verksamhetsregler.

Verksamhetsregler kan exempelvis omfatta begränsningar i användningen, krav på utbildning av instruktörer och brukare samt påbud om användning av personlig skyddsutrustning (PPE). Vid användning av tekniska system i fredstid kan särskilda begränsningar gälla under utbildning och övning. Vid högre beredskapsnivåer kan begräsningar påverkas.

Antalet kända olycksrisker i ett tekniskt system är inte statiskt utan kan öka eller minska med tiden. Ökning kan bero på att nya användningssätt tillkommer, material- eller produktionsfel upptäcks, materielen åldras eller slits på ett oväntat sätt eller att underhåll genomförs felaktigt eller bristfälligt. Ökningen kan också bero på att utbildningen förändrats, förändrat användningssätt (normglidning), såväl människor som organisationer blir mindre vaksamma eller mer hemmablinda över tid, särskilt om inga olyckor eller tillbud har inträffat under en längre tid. Minskning kan bero på att säkerhetsbrister hos materielen omhändertagits genom ändring (modifiering).

Genom att arbeta förebyggande med ständiga förbättringar kan olyckor förebyggas. I all verksamhet uppkommer oundvikligen avvikelser från planerat genomförande såsom avsiktliga eller oavsiktliga avsteg från givna regler, variation i beteende hos användaren samt förändringar från förväntad prestanda hos materielen. I syfte att förebygga och säkerställa att betryggande säkerhet bibehålls samlar Försvarsmakten systematiskt in information under vidmakthållandeskedet från användning och underhåll. Informationen kan bestå av olycks- och tillbudsrapporter, signaler om förändrat användningssätt (normglidning), felutfall, prestandabrister eller tekniska statusundersökningar. Information kan även erhållas genom tillsyn och inspektion. Systemsäkerhetsaspekterna från insamlad data värderas och fakta som är av betydelse för systemsäkerheten analyseras så att korrekta åtgärder kan vidtas i verksamheten, genom ändring (modifiering) av tekniska system eller i dess användning.

2.5 Angränsade områden till systemsäkerhet

Systemsäkerhet har gemensamma intressen med andra verksamhetsområden. Nedan ges en beskrivning av vissa närliggande områden som normalt inte omfattas av systemsäkerhetsmetodiken. Information som skapas genom systemsäkerhetsarbete, eller av annat närliggande område, kan därför överföras och komma till användning inom eller mellan andra verksamhetsområden.

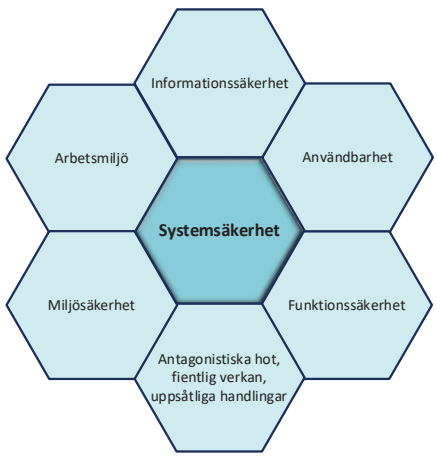


Bild 2.7 Exempel på angränsande och ibland överlappande områden till systemsäkerhet.

2.5.1 Informationssäkerhet

Med informationssäkerhet avses skydd för informationstillgångar så att informationen är korrekt och tillgänglig enbart för de personer, system eller processer som den är avsedd för. Syftet är att skydda dessa tillgångar mot oönskade händelser såsom fysiska eller digitala intrång. Skyddet kan bestå av teknisk säkerhet och/eller administrativ säkerhet. Utifrån verksamhetens karaktär kan en del av dessa tillgångar vara mer skyddsvärda än andra samt att skyddsvärdet för information kan variera över tid. Ur ett informationssäkerhetsperspektiv ska informationen vara:

- Riktig
- Skyddad (mot obehörig åtkomst)
- Tillgänglig (för den som vid en viss tidpunkt behöver informationen)
- Spårbar

Om skyddet av informationstillgången brister så att den blir otillgänglig, felaktig (korrupt) eller spridd till obehöriga (främmande makt) så kan detta även påverka systemsäkerheten och leda till konsekvenser i verksamheten för personal, materiel och anläggningar. Ett tekniskt system kan aldrig erbjuda betryggande säkerhet om inte informationssäkerheten är omhändertagen.

2.5.2 Användbarhet

Med användbarhet avses den grad i vilken en användare i ett givet sammanhang kan bruka ett system för att uppnå specifika mål på ett ändamålsenligt, effektivt och för användaren tillfredsställande sätt. De flesta tekniska och icke-tekniska system kommer på olika sätt att kommunicera med användare och underhållspersonal. Om människan kan öka eller minska sin förmåga i denna interaktion, har det betydelse för att system upplevs säkra och användbara.

Interaktionsdesign handlar om att forma system, tjänster och miljöer med särskilt fokus på deras brukskvalitéer, det vill säga hur de ska vara att använda. Vid utformning av användargränssnitt krävs därför kunskap om människans förutsättningar och förmågor, men även kunskap om människans fysiska och mentala begränsningar som användare och som en del av systemet. Insikt i hur psykologiska, fysiologiska, organisatoriska och tekniska aspekter interagerar i komplexa och påfrestande miljöer, skapar förutsättningar för att åstadkomma säkra och användbara system.

Om användbarheten brister, exempelvis genom en alltför komplex informationsvolym, återkommande falsklarm, ologiska manöverorgan eller val av färger, så kan detta även påverka systemsäkerheten och leda till konsekvenser i verksamheten för personal, materiel, miljö och anläggningar.

2.5.3 Arbetsmiljö

Med arbetsmiljö avses både den fysiska som den psykosociala arbetsmiljön. Arbetsmiljön innefattar biologiska, medicinska, fysiologiska, psykologiska, sociala och tekniska faktorer som i verksamheten eller i arbetsplatsens omgivning påverkar användaren. Vid framtagning av tekniska system och produkter är det den fysiska arbetsmiljön som användaren kan ställa krav på, vilket beror på att det finns utförliga regler och mätbara gränsvärden för hur vår fysiska arbetsmiljö ska utformas.

Ergonomi handlar om anpassning av arbete och miljö till människans behov och förutsättningar. Det kan ofta handla om hur arbetsplatsen och arbetsmiljön ska se ut rent tekniskt för att inte medföra skador eller ohälsa, exempelvis kroppshållning, arbetsställning, arbetshöjd, ljud, ljus, ventilation, strålning och klimat, men även att kroppen används på ett riktigt sätt, exempelvis genom att skjuta, dra, lyfta eller bära.

En god och sund arbetsmiljö höjer stridsvärdet hos användaren och ger vare sig akut eller på sikt negativ påverkan på hälsan. Långsiktig hälsopåverkan hanteras genom begränsningar angivna i lagstiftningen samt med stöd av metoder inom arbetsmiljöområdet.

2.5.4 Funktionssäkerhet

Med funktionssäkerhet avses förmågan hos ett system att utföra en krävd funktion under givna förhållanden under ett visst tidsintervall. Funktionssäkerhet på en systemnivå kan vara systemsäkerhet på en annan systemnivå. Funktionsfel kan både vara en bidragande orsak eller en utlösande faktor till att en olycka inträffar.

Funktionssäkerhet är en delmängd av driftsäkerhet och ett sätt att mäta den är genom felintensitet. Felintensiteten kan som funktion av tid, vara avtagande, konstant, eller ökande.

Om de berörda komponenterna som ska leverera sin funktion inte har rätt funktionssäkerhet kan olyckor och tillbud inträffa. Det är dock viktigt att skilja

på systemfel som har inverkan på säkerheten och systemfel som påverkar eller begränsar funktion och prestanda. De senare kan i förlängningen, som en konsekvens av otillräcklig funktion eller prestanda, orsaka skador på person, egendom eller yttre miljö. Dessa hanteras dock som ett prestanda- eller kvalitetsproblem.

Funktionssäkerheten kan bibehållas genom förebyggande underhåll och/eller förtida utbyte av säkerhetskritiska komponenter alternativt genom ändring (modifiering) av det tekniska systemet.

2.5.5 Miljösäkerhet

Med miljösäkerhet kopplat till tekniska system avses hantering av aspekter som har negativ påverkan på den yttre miljön. Miljöarbetet omhändertar exempelvis emissioner och buller från ett tekniskt system vid normal drift och som utgör en belastning på den yttre miljön. Emissioner kan exempelvis vara farliga ämnen, luftpartiklar, ljus eller strålning.

I systemsäkerhetsarbetet ingår att identifiera och hantera potentiella olycksrisker, således enskilda oavsiktliga händelser som frångår normal drift och som kan ha både lång- och kortsiktiga miljö- och hälsoeffekter. Möjliga orsaker till olyckor eller tillbud utreds och tänkbara konsekvenser redovisas inom ramen för systemsäkerhetsarbetet. Exempel på sådana händelser kan vara tankbilsläckage eller bortfall av bullerskydd. Den faktiska miljöpåverkan som är betingad av aktuell fysisk plats faller dock utanför systemsäkerhetsarbetet och hanteras genom begränsningar angivna i lagstiftningen samt med stöd av andra metoder inom miljöområdet.

Resultat från systemsäkerhetsanalyser såsom uppmätt buller eller emissioner kan även användas i miljöarbetet, exempelvis vid ansökan om koncession för tillståndspliktig verksamhet.

2.5.6 Antagonistiska hot, fientlig verkan, uppsåtliga handlingar

Med fientlig vapenverkan avses främmande makts användning av militära medel direkt riktade mot ett förbands skyddsvärda tillgångar såsom personal, materiel och anläggningar. Systemsäkerhetsverksamheten hanterar inte skador som orsakats av fientlig vapenverkan mot egna tekniska system eller personal. Undantaget

är tekniska system för ammunitions- eller minröjning vid internationell insats respektive svensk nationell ammunitionsröjning i fred. Olycksrisker till följd av sådana riskkällor omhändertas inom ramen för systemsäkerhetsarbetet, eftersom det tekniska systemets huvudsakliga uppgift är att röja ammunition eller minor.

Med antagonistiska hot avses angrepp utan konventionella vapen, men riktade mot ett förbands skyddsvärda informationstillgångar, exempelvis genom IT-attacker. Systemsäkerhetsverksamheten hanterar inte skador som orsakats av antagonistiska attacker mot egna tekniska system eller personal.

Systemsäkerhetsverksamheten omfattar heller inte medvetet sabotage eller uppsåtliga handlingar från egen personal i syfte att skada egen personal eller medvetet förstöra tekniska system och produkter.

3 Systemsäkerhetsverksamhet i livscykeln

Syftet med detta kapitel är att beskriva Försvarsmaktens livscykelmodell för tekniska system och produkter ur ett systemsäkerhetsperspektiv.

3.1 Forskning och teknikutveckling

Med verksamheten Forskning och teknikutveckling (FoT) menas det arbete som genomförs innan ett tekniskt system ska realiseras. Verksamheten Forskning och teknikutveckling (FoT) styrs vanligen av Försvarsmaktens framtida behov av nya förmågor för att möta kommande militära hot. Syftet med arbetet är dels att utveckla ny plattformsoberoende teknik, dels att analysera vilka möjligheter och hot som kan uppstå utifrån ny teknik, dels att identifiera nya användningsområden för redan känd teknik. Målet med systemsäkerhetsarbetet inom verksamheten Forskning och teknikutveckling (FoT) är att skaffa tillräcklig kunskap om olika tekniker och dess potentiella användningsområden, för att en *Systemsäkerhetsbedömning* (SSB) av olika alternativ ska vara möjlig att genomföra.

3.2 Försvarsmaktens livscykelmodell

Försvarsmaktens livscykel- och beslutsmodell för tekniska system och produkter bygger på standarden ISO/IEC/IEEE 15288, *Systems and software engineering – System life cycle processes.*

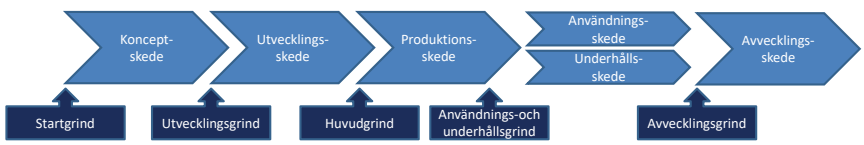


Bild 3.1 Försvarsmaktens livscykelmodell med beslutsgrindar.

Försvarsvarsmaktens nyttjande av livscykelmodellen med tillhörande beslutsgrindar beskrivs primärt i materielproduktionsprocessen. I *Samordningsöverenskommelsen (SAMO FM – FMV)* används både skeden och faser, vilka nedan är

kursiverade. Skeden används för att beskriva ett tekniskt systems livscykel och faser härrör från Regeringens direktiv för investeringsplanering. För att beskriva vilket systemsäkerhetsarbete som behöver genomföras inom ramen för de olika livscykelskedena används istället begreppet ”arbete”.

- Konceptarbete *(Konceptskede, Konceptfas)*
- Utvecklingsarbete *(Utvecklingsskede)*
  - Förberedelsearbete *(Förberedelsefas)*
  - Anskaffningsarbete *(Anskaffningsfas)*
- Produktionsarbete inklusive arbete inför BOAC/BOAL *(Produktionsskede)*
- Vidmakthållandearbete *(Vidmakthållandeskede, Användningsskede/Underhållsskede)*
- Avvecklingsarbete *(Avvecklingsskede)*

Bilden nedan visar systemsäkerhetsarbete i förhållande till Försvarsmaktens beslutsgrindar. För att förflytta ett tekniskt system eller produkt mellan livscykelskeden krävs bland annat erforderlig systemsäkerhetsdokumentation.

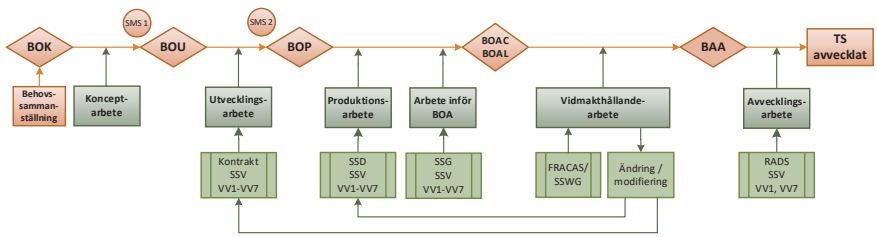


Bild 3.2 Systemsäkerhetsarbete i förhållande till Försvarsmaktens beslutsgrindar.

3.3 Aktörernas livscykelskeden

Försvarsmaktens och de övriga aktörernas livscykelskeden är förskjutna gentemot varandra. *Kravställarens* Koncept- och Utvecklingsskede genomförs innan *beställaren* kan påbörja sitt arbete. Försvarsmaktens Beslutsgrind BOP (*Beslut om produktion)* frisläpper medel för att påbörja serieanskaffning, vilket innebär att *beställaren* först då kan påbörja anskaffning av tekniska system. I de fallen *beställarens* offert till *kravställaren* ska vila på ett bindande anbud från *konstruktören* så påbörjas *beställarens* anskaffningsarbete redan under Försvarsmaktens Utvecklingsskede. *Konstruktörens* arbete påbörjas så snart som ett kontrakt har slutits med *beställaren*.

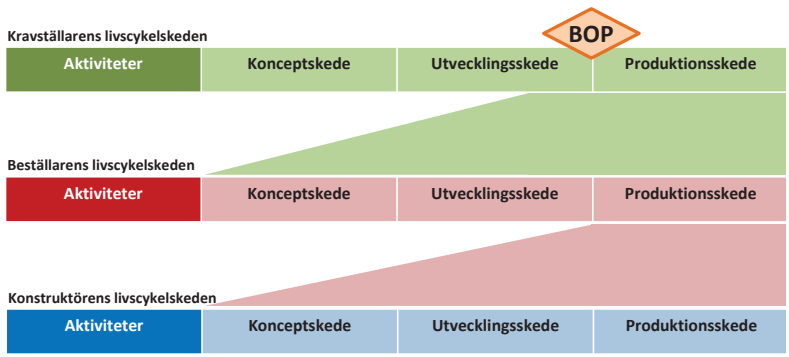


Bild 3.3 De olika aktörernas förskjutna livscykelskeden.

3.4 Behovssammanställning

Aktiviteten *Behovssammanställning* innebär att Försvarsmakten i rollen som *kravställare* tar fram underlag såsom rapporter utarbetade under Forskning och Teknikutveckling (FoT), Perspektivplanering (PerP), omvärldsbevakning, marknadsanalys och erfarenheter från tidigare tekniska system. Styrningar och ingångsvärden som ska ligga till grund för att kunna beskriva förmågor, funktioner, nytta, egenskaper och begränsningar inhämtas. Information om intressenter till det tänkta tekniska systemet och beroenden till andra system och verksamheter, samt underlag om vilka befintliga tekniska system som är tänkta att ersättas tas fram.

I aktiviteten Behovssammanställning genomförs inget systemsäkerhetsarbete.

3.5 Konceptarbete

Försvarsmaktens Konceptskede initieras genom Beslutsgrind BOK (*Beslut om koncept*) som normalt tas på militärstrategisk nivå. Syftet med Konceptskedet är att Försvarsmakten i rollen som *kravställare* undersöker olika alternativa möjligheter att tillgodose behov av funktionalitet i framtida tekniska system. Denna funktionalitet kan realiseras genom ändring (modifiering) av befintlig materiel eller genom anskaffning av nya tekniska system eller produkter eller en kombination av ny materiel, befintlig materiel och ändrad (modifierad) materiel. Konceptarbetet utgår från Behovssammanställningen.

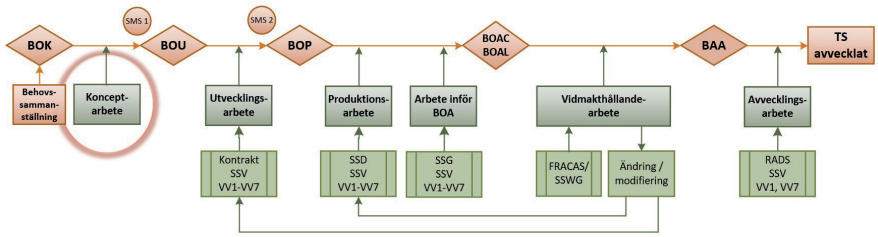


Bild 3.4 Systemsäkerhetsarbete i Försvarsmaktens Konceptskede.

Konceptskedet behöver inte genomföras om den lämpligaste produkten kan identifieras utan djupare analys. I de fallen utarbetas inte *Systemmålsättning* (SMS 1).

I de fallen en given försörjningslösning saknas behöver en *Systemmålsättning* (SMS 1) utarbetas. Alternativa försörjningslösningar utreds och värderas utifrån olika aspekter såsom systemsäkerhet, informationssäkerhet, internationellt samarbete, användningsmiljö och kommersiella aspekter. Vidare behöver förhållningssätt till anläggningar och dess basresurser beskrivas. I Konceptskedet sker en kontroll av att det tänkta tekniska systemet faller inom ramen för aktuella lagar för militär materiel, om inte så måste konceptet omarbetas.

Systemsäkerhetsarbetet fokuserar på till vilken grad det går att basera det tänkta tekniska systemet på samhällets krav och godkännanden genom vägval (VV1), på annan stats godkännande vägval (VV2) eller om det är ett beprövat system vägval (VV6). Dessa vägval är att föredra då det innebär att man kan använda sig av redan genomfört systemsäkerhetsarbete. Om det tekniska systemet avses ändras (modifieras) eller användas på annat sätt än det som förutsätts för vägval (VV1, 2, 6) behöver andra vägval också tillämpas.

Med godkännande utgivet av annan stat enligt vägval (VV2) avses främst en utländsk försvarsmyndighet. I *Systemmålsättningen* (SMS 1) bör förutsättningarna anges för att kunna acceptera andra staters godkännanden och om möjligt även vilka staters godkännanden som kan accepteras.

Med beprövat system enligt vägval (VV6) innebär det att man utgår ifrån ett tekniskt system som redan används och är välkänt. Förutsättningen för att kunna förlita sig på att det tekniska systemet är beprövat är att dess utförande eller användning inte förändras.

3.6 Utvecklingsarbete

Försvarsmaktens Utvecklingsskede initieras genom Beslutsgrind BOU *(Beslut om utveckling)* och genomförs av Försvarsmakten i rollen som *kravställare*. Syftet med Utvecklingsskedet är att i en *Systemmålsättning* (SMS 2) beskriva en systemlösning som uppfyller Försvarsmaktens behov för ett framtida tekniskt system.

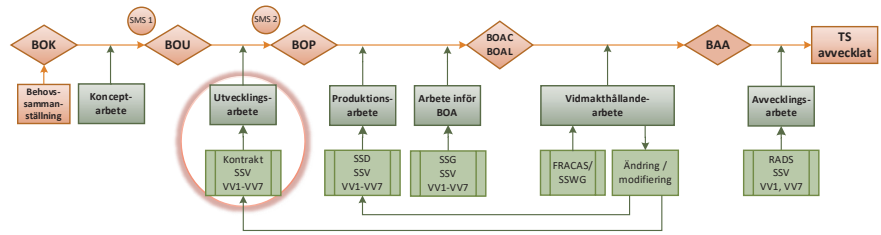


Bild 3.5 Systemsäkerhetsarbete i Försvarsmaktens Utvecklingsskede.

3.6.1 Försvarsmaktens utvecklingsskede som kravställare

Om befintlig *Systemsäkerhetsledningsplan* (SSMP) och *Systemmålsättning* (SMS 2) är giltiga och tillräckliga finns det inte något behov av att genomföra ett Utvecklingsskede.

För nya tekniska system kan *Systemsäkerhetsledningsplanen* (SSMP) behöva uppdateras. *Systemsäkerhetsledningsplanen* (SSMP) utgår från säkerhetsmålen och Försvarsmaktens vision för systemsäkerhet, vilka omsätts till systemsäkerhetsmål. I *Systemmålsättningen* (SMS 2) anges systemsäkerhetskraven.

I de fallen en tillämplig systemmålsättning saknas behöver en *Systemmålsättning* (SMS 2) utarbetas. Om *Systemmålsättning* (SMS 1) finns utgör den underlag för utarbetandet av en ny *Systemmålsättning* (SMS 2).

Det nya tekniska systemet, eller det uppdaterade, kan skapas genom ändring (modifiering) av befintlig materiel, genom anskaffning av nya tekniska system eller produkter, eller en kombination av ny materiel, befintlig materiel och ändrad (modifierad) materiel. Alternativa systemlösningar utreds och värderas utifrån olika aspekter såsom systemsäkerhet, informationssäkerhet, internationellt samarbete, användningsmiljö och kommersiella aspekter. Vidare behöver förhållningssätt till anläggningar och dess basresurser beskrivas.

I arkitekturen för systemlösningen identifieras hur ett system-av-system lämpligast byggs upp av olika systemelement (tekniska system, delsystem, produkter och integrationsprodukter). Systemarkitekturen på övergripande nivå definieras så långt man behöver, till exempel med hänsyn till anpassning till organisation eller användning av befintlig materiel.

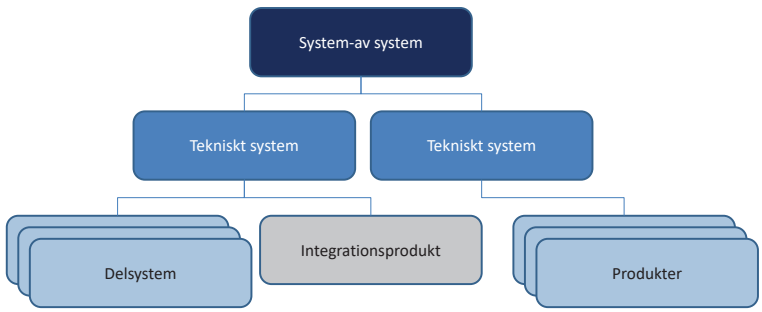


Bild 3.6 *System-av-system kan bestå av valfria kombinationer av tekniska system, delsystem, produkter och integrationsprodukter.*

Vart och en av dessa systemelement kan uppvisa betryggande säkerhet genom olika vägval (VV). De olika systemelementen ska bidra med underlag för att hela det tekniska systemet ska kunna visa på betryggande säkerhet och även i förekommande fall, som ett av systemen i ett system-av-system.

Ett systemsäkerhetsarbete genomförs för det tekniska systemet i syfte att klarlägga värsta trovärdiga konsekvenser vid olyckor för person, egendom och yttre miljö. Detta görs för att kunna bestämma vilka vägval (VV) som kan vara aktuella i det

kommande arbetet. Med stöd av systemsäkerhetsarbetet tillämpas *Vägvalsmodellen* (VVM) med inriktning mot vägvalen (VV1 – 6):

- Vägval 1 – Författningsenliga krav
- Vägval 2 – Godkänd av annan stat
- Vägval 3 – Godkänd av annan part
- Vägval 4 – Övriga standarder
- Vägval 5 – Designregler
- Vägval 6 – Beprövat system

3.6.2 Försvarsmaktens eller FMV:s utvecklingsarbete som beställare

Försvarsmakten eller FMV i rollen som *beställare* tar fram en *Systemsäkerhetsplan* (SSPP) som beskriver hur det interna systemsäkerhetsarbetet ska genomföras. Vidare beskrivs hur systemsäkerhetskraven mot *kravställaren* ska uppfyllas samt vilka systemsäkerhetskrav som ska ställas på *konstruktören*.

I *beställarens* systemsäkerhetsarbete fastläggs de dimensionerande olycksriskerna vilka utgör underlag för utarbetande av *Förfrågningsunderlag* (RFP). Systemlösningen anpassas för att möjliggöra lämpliga vägval också på lägre systemnivåer och för att ge möjlighet till olika anskaffningar. *Beställaren* säkerställer samfunktion för det sammanhållna tekniska systemet med dess delsystem och produkter från olika *konstruktörer*, det vill säga gör en lämplig fördelning mellan olika leverantörer utifrån olika aspekter. Utifrån systemsäkerhetsarbetet fastställs acceptanskriterierna för de angivna vägvalen. I *Förfrågningsunderlaget* (RFP) kan även krav ställas på principiella konstruktionslösningar på det tekniska systemet eller produkten.

I *Förfrågningsunderlaget* (RFP) anges kriterierna för att kunna använda sig av vägvalen (VV1 – VV7) i efterföljande systemsäkerhetsvärderingar under produktionsarbetet:

- VV1: Vilka författningsenliga krav ska tillämpas?
- VV2: Vilket underlag ska redovisas för att kunna acceptera ett godkännande från en annan stat?
- VV3: Vilket underlag ska redovisas för att kunna acceptera ett godkännande från en annan part?
- VV4: Vilka etablerade standarder inom teknikområdet kan tillämpas?

- VV5: Vilka *Designregler* (DR) och *Tekniska handlingsregler* (THR) kan tillämpas?
- VV6: Vilka kriterier och krav kan accepteras för ett beprövat system?
- VV7: Vilken *Tolerabel risknivå* (TR) inklusive riskmatriser ska tillämpas?

3.6.3 Industrins utvecklingsarbete som konstruktör

Då industrin i rollen som *konstruktör* erhållit kontrakt utarbetar *konstruktören* dels ett förslag till *Systemsäkerhetsplan* (SSPP), dels tas ett mer detaljerat koncept för det tänkta tekniska systemet fram. *Konstruktören* redogör i sin *Systemsäkerhetsplan* (SSPP) för hur vägvalen kommer att tillämpas för systemet med dess ingående delsystem och produkter samt utifrån alla förekommande olycksrisker för person, egendom och yttre miljö. *Konstruktören* föreslår hur vägvalen kan tillämpas för det detaljerade konceptet för att kunna uppnå betryggande säkerhet för det tänkta tekniska systemet. Detta utgör underlag för kontraktsgenomgången.

Vid kontraktsgenomgången finns det möjligheter för *beställaren* att ge alternativa förslag på konstruktion och vägval. *Beställaren* och *konstruktören* kan komma överens om förändringar av de föreslagna vägvalen inom ramen för kontraktet. Detta dokumenteras i ett protokoll och överförs därefter till den kontrakterade *Systemsäkerhetsplanen* (SSPP). Avstämningar med *beställaren* sker under konstruktionsarbetet så att *Systemsäkerhetsplanen* (SSPP) efterlevs.

Under utvecklingsarbetet kan prototyper behöva tas fram för att kunna utvärdera olika tekniklösningar vid provning respektive försök. Prototyper tas normalt fram av *konstruktören*. Vid prototypframtagning ska *konstruktören* redovisa att de vidtagna tekniska konstruktionsåtgärderna tillsammans med bruksanvisningar med eventuella restriktioner, ger betryggande säkerhet för den avsedda provningen eller försöken.

Efter genomfört systemsäkerhetsarbete sammanställer *konstruktören* riskdokumentationen genom att göra en systemsäkerhetsvärdering för det tekniska systemet. Vidare utfärdas ett *Systemsäkerhetsutlåtande* (SCA) med *Systemsäkerhetsrapport* (SAR) och *Risklogg* (RL).

3.7 Produktionsarbete

Försvarsmaktens Produktionsskede initieras genom Beslutsgrind BOP *(Beslut om produktion)* och genomförs av Försvarsmakten i rollen som *kravställare*. Beslutsgrind (BOP) innebär att *Systemmålsättning* (SMS 2) fastställs och att *beställaren* därmed kan påbörja sin anskaffning. Syftet med Produktionsskedet är att anskaffa, verifiera och validera (VoV) samt driftsätta tekniska system och produkter i förbandsverksamheten.

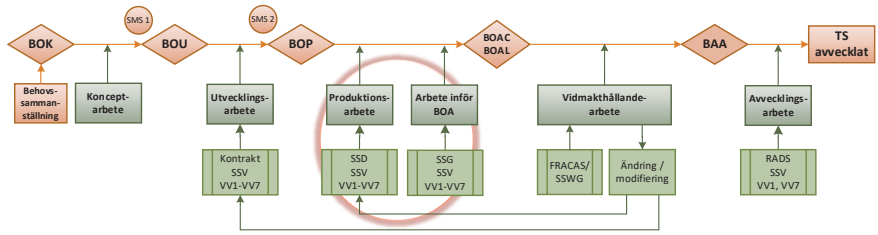


Bild 3.7 *Systemsäkerhetsarbete i Försvarsmaktens Produktionsskede.*

Kravställaren följer upp att Försvarsmakten eller FMV i rollen *beställare* har omhändertagit och tolkat kraven i *Systemsäkerhetsledningsplanen* (SSMP) och *Systemmålsättningen* (SMS 2). Detta arbete kan samordnas, överenskommas och kvalitetssäkras i *Arbetsgrupp för systemsäkerhe*t (SSWG).

Beställaren genomför anskaffning i enlighet med de styrningar som utarbetats i de föregående livscykelskedena. Styrningar avseende systemsäkerhet återfinns i *Systemmålsättning* (SMS 2) och i denna refererad *Systemsäkerhetsledningsplan* (SSMP).

Beställaren säkerställer att *konstruktören* arbetar i enlighet med kontraktet och den avtalade S*ystemsäkerhetsplanen* (SSPP). *Beställaren* granskar *konstruktörens* arbete innan leverans sker. *Konstruktören* utfärdar ett *Systemsäkerhetsutlåtande* (SCA) med *Systemsäkerhetsrapport* (SAR) och *Risklogg* (RL).

Beställaren genomför verifiering och validering (VoV), vilket innebär att överenstämmelse med *Systemmålsättningen* (SMS 2) kan visas med tillräckligt konfidens. Oberoende granskning som interngranskning genomförs och vid behov inhämtas värdering från FMV:s Rådgivningsgrupper inom Vapen-

och ammunitionssäkerhet innan systemöverlämning (SÖL) kan genomföras. *Beställaren* ska genom sin systemsäkerhetsvärdering kunna visa att betryggande säkerhet uppnåtts för hela det tekniska systemet. Om ett redan existerande tekniskt system används kan dess systemsäkerhetsunderlag behöva omvärderas och i nödvändig omfattning omarbetas utifrån förändringar i den tänkta användningen av det tekniska systemet och i samverkan med andra delsystem och produkter. *Beställaren* utfärdar en *Systemsäkerhetsdeklaration* (SSD) med tillhörande systemsäkerhetsdokumentation.

3.7.1 Systemsäkerhetsgodkännande (SSG)

Genom *Systemsäkerhetsgodkännandet* (SSG) bekräftas att det tekniska systemet uppfyller kraven i *Systemsäkerhetsledningsplanen* (SSMP) och *Systemmålsättning* (SMS) för avsedd användning. Vidare intygas att nödvändiga verksamhetsregler finns för hanterade olycksrisker samt att eventuella förslag till restriktioner för kvarstående olycksrisker är rimliga och att det tekniska systemet därmed kan föras in i verksamheten på ett tillfredsställande sätt.

3.7.2 Beslutsgrind B0AC

I *Beslut om användning, central nivå* (BOAC) säkerställs ur systemsäkerhetsperspektiv att det tekniska systemet så som det verkligen är beskaffat, uppfyller visionen för systemsäkerhet och att förutsättningar finns för att ta det tekniska systemet i bruk vid Försvarsmakten.

I *Beslut om användning, central nivå* (BOAC) styrs vad som ska omhändertas i *Beslut om användning, lokal nivå* (BOAL). Om *Beslut om användning, lokal nivå* (BOAL) inte är nödvändigt ska motsvarande underlag och ställningstaganden finnas redovisat i *Beslut om användning, central nivå* (BOAC).

3.7.3 Beslutsgrind B0AL

I *Beslut om användning, lokal nivå* (BOAL) redovisas att samtliga punkter är hanterade som åligger C OrgE enligt *Beslut om användning, central nivå* (BOAC).

3.8 Vidmakthållandearbete

Försvarsmaktens Vidmakthållandeskede genomförs av Försvarsmakten i rollen som *kravställare*. Syftet med systemsäkerhetsarbetet under Vidmakthållandeskedet är att identifiera förhållanden i användningen av det tekniska systemet och

dess funktion som innebär att systemsäkerhetsvärderingen i *Systemsäkerhetsgodkännandet* (SSG) som ligger till grund för *Beslut om användning, central nivå* (BOAC), kan behöva kompletteras eller göras om i tillämpliga delar. Detta kan också föranledas av förändringar i gällande lagstiftning, regelverk eller ändrade förutsättningar för de tidigare gjorda vägvalen (VV).

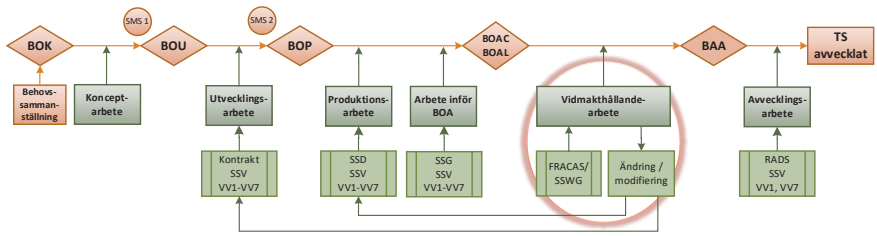


Bild 3.8 *Systemsäkerhetsarbete i Försvarsmaktens Vidmakthållandeskede.*

Information samlas systematiskt in från användning, underhåll och förrådshållning (transport). Informationen kan bestå av olycks- och tillbudsrapporter, brukarerfarenheter, felutfall, prestandabrister eller tekniska statusundersökningar. Systemsäkerhetsaspekterna från insamlad data under aktiviteten *Felrapporteringssystem* (FRACAS) värderas av *Arbetsgrupp för systemsäkerhet* (SSWG). FMV eller industrin kan ges i uppgift att genomföra mer detaljerade analyser i den omfattning som behövs.

Fakta som är av betydelse för systemsäkerheten analyseras och nya systemsäkerhetsvärderingar genomförs som syftar till att säkerställa att betryggande säkerhet fortsatt innehålls. Detta kan dels innebära behov av ändringar (modifieringar), dels förändringar i handhavande inklusive normglidning, dels underhåll. Ändringar som påverkar tidigare gjorda systemsäkerhetsvärderingar innebär att systemsäkerhetsarbete ska genomföras i enlighet med utvecklings- och/eller produktionsskedet. Baserat på sådana fakta kan *Arbetsgrupp för systemsäkerhet* (SSWG) lämna underlag till nya systemsäkerhetsbeslut.

I *Arbetsgrupp för systemsäkerhet* (SSWG) kan det vara svårt att identifiera normglidning från de data som samlas in och därför måste detta bevakas särskilt. Normglidning innebär att det sker förändringar i användning som inte baserats på förnyad analys eller ställningstaganden. Det är ett vanligt fenomen som inträffar då materiel använts under längre tid och utan upplevda större problem. Normglidning är problematisk eftersom erfarenheten inte självklart är tillämplig

på den förändrade användningen. Det kan också vara så att konstruktionen varken formellt eller i verkligheten är avsedd för eller uppfyller kraven för den förändrade användningen. Det här måste kontinuerligt bevakas och förändringar i användning måste föregås av systemsäkerhetsarbete och medvetna beslut. Annars kan materielen komma att användas utanför vad den visats vara säker för vilket kan innebära icke-tolerabla olycksrisker.

3.9 Avvecklingsarbete

Försvarsmaktens Avvecklingsskede initieras genom Beslutsgrind BAA (*Beslut av avveckling*) och genomförs av Försvarsmakten i rollen som *kravställare*. Syftet med systemsäkerhetsarbetet under Avvecklingsskedet är att identifiera olycksrisker som kan inträffa under den fysiska kvittblivningen av det tekniska systemet.

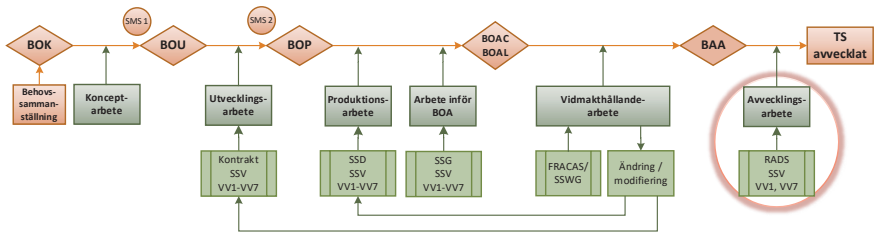


Bild 3.9 *Systemsäkerhetsarbete i Försvarsmaktens Avvecklingsskede.*

Avveckling kan bland annat föranledas av att systemets tekniska livslängd är förbrukad eller för att det inte längre finns behov av systemet. I vissa fall kan en identifierad säkerhetsbrist i det tekniska systemet eller produkten föranleda avveckling.

Avvecklingsarbetet syftar till att undersöka olika möjligheter att bli kvitt tekniska system och produkter på ett säkert och hållbart sätt enligt gällande miljölagstiftning. Eventuellt kan producentansvar åberopas med stöd av kontrakt eller lagstiftning. Ny lagstiftning, bestämmelser eller regelverk som inte fanns under produktionsskedet kan exempelvis påverka hanteringen av farliga ämnen.

Avvecklingsmetoder som överlåtelse, återanvändning, försäljning och destruktion utvärderas. I avvecklingsarbetet behöver även ekonomiska, juridiska och praktiska aspekter omhändertas. Avvecklingsmetoder beslutas av Försvarsmakten.

Avvecklingen behöver beaktas under materielens hela livscykel. Inför fysisk avveckling av tekniska system och produkter ska den under produktionsskedet framtagna *Riskanalys inför avveckling av system* (RADS) analyseras och vid behov revideras. Den förnyade systemsäkerhetsanalysen ska identifiera nya olycksrisker och vid behov omvärdera de tidigare identifierade som kan inträffa under den fysiska avvecklingen. Det är viktigt att även reservmateriel, underhållsutrustningar, stödsystem samt Grund- och förvaltningsdata (GoF) och information oavsett i vilken form och hos vilken aktör omfattas av avvecklingen för att undvika att det uppstår oklara ansvarsförhållanden vad avser systemsäkerhetsstatusen för berörd materiel och information.

Återrapportering av att det tekniska systemet eller produkterna är fysiskt avvecklade och att förvaltningsdata tagits bort sker utifrån tillämpningsbeslut enligt Avvecklingsskrivelsen.

4 Aktörer, roller och ansvar

Syftet med detta kapitel är att beskriva de olika aktörernas roller och ansvar. De olika organisationerna såsom Försvarsmakten, FMV, Fortifikationsverket och industrin har alla olika ansvar, uppgifter och funktioner inom systemsäkerhetsverksamheten.

4.1 Beskrivning av roller

Ur Försvarsmaktens perspektiv beskrivs nedan ett fåtal principiella roller som genomför systemsäkerhetsverksamhet. Respektive aktör kan inneha ytterligare roller men dessa hanteras inom egen organisation utifrån de huvudsakliga beskrivningarna nedan.

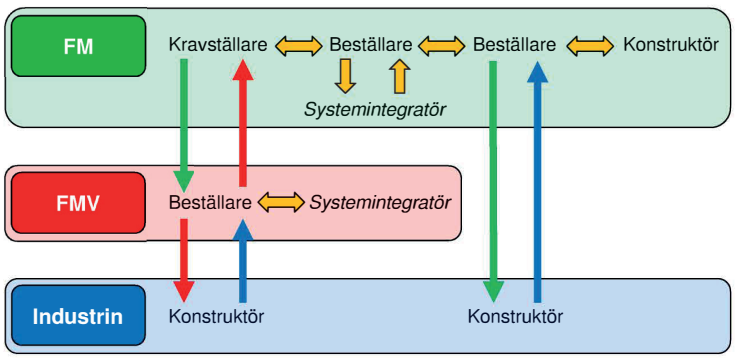


Bild 4.10 De olika aktörernas roller med order-/beställnings- och leveransvägar.

Kravställaren är den som utifrån behov av förmågor och funktioner ställer krav på materiel (system-av-system, tekniska system eller produkter). Vidare utfärdar *Kravställaren Systemsäkerhetsgodkännanden* (SSG), följer upp materielen under vidmakthållandeskedet samt avvecklar densamma.

Beställaren är den som utifrån *Systemmålsättningar* (SMS) ställer krav på samt beställer konstruktion och tillverkning av den eller de som utför realiseringen av tekniska system eller produkter, alternativt ger en särskild uppgift till en *Systemintegratör*. Vidare utfärdar *Beställaren Systemsäkerhetsdeklarationer* (SSD) samt genomför efterfrågade uppgifter under vidmakthållande- och avvecklingsskedena.

Konstruktören är den som utifrån kontrakt realiserar, konstruerar och utformar tekniska system eller produkter. Vidare utfärdar *Konstruktören Systemsäkerhets-utlåtand*e (SCA).

Systemintegratören är den som säkerställer samfunktion mellan tekniska system till ett system-av-system och som därmed ger efterfrågad förmåga eller funktionalitet i de fallen sekretess föreligger eller att en *konstruktör* inte kan ta detta ansvar.

4.2 Försvarsmaktens roller

Försvarsmakten förfogar över hela spektrumet av roller inom systemsäkerhetsverksamheten, och kan således utföra uppgifter i de fyra rollerna *Kravställare, Beställare, Systemintegratör* och *Konstruktör*.

Försvarsmakten innehar rollerna *Kravställare, Beställare, Systemintegratör* och *Konstruktör.*

4.2.1 Försvarsmakten i rollen som kravställare

Försvarsmakten i rollen som *kravställare* har att ansvara för och fatta beslut om:

- Designregler (DR) och Tekniska handlingsregler (THR)
- Systemsäkerhetsledningsplan (SSMP)
- Systemmålsättning (SMS)
- Systemsäkerhetsgodkännande (SSG)
- Beslut om användning, central nivå (BOAC)
- Beslut om användning, lokal nivå (BOAL)
- Arbetsgrupp för systemsäkerhet (SSWG)
- Riskanalys inför avveckling av system (RADS)

Försvarsmakten har tekniskt designansvar för all materiel och ställer verksamhets- och systemsäkerhetskrav på förband, funktionskedjor, tekniska system och produkter som ska ingå i krigsorganisationen och som därmed ska användas för utbildning, övning och insats. Detta görs genom utarbetande och fastställande av *Systemmålsättningar* (SMS) på olika nivåer. Dessa innehåller bland annat systemsäkerhetskrav. Motsvarande gäller även för materiel som används inom övrig verksamhet.

Designansvarig (DesignA) är en roll i Försvarsmakten som bär tekniskt designansvar inom tilldelat produktområde. Detta innebär att samordna och styra design i de skeden av materielens livscykel där Försvarsmakten bär tekniskt designansvar. Rollen DesignA finns på olika nivåer och inom olika delar av Försvarsmaktens verksamhet. Exempel på olika nivåer av rollen DesignA är Teknisk direktör och Teknisk chef. Rollen tilldelas ansvar, uppgifter och mandat genom myndighetens arbetsordningar (ArbO) inklusive beslutsdelegeringar, direktiv och övriga beslut.

Försvarsmaktens Tekniska direktör ansvarar för gemensamma *Designregler* (DR) och *Tekniska handlingsregler* (THR) och leder Försvarsmaktens tekniska designverksamhet genom att identifiera, definiera, och fördela ansvar för alla nivåer av tekniska system och deras samfunktion (system-av-system) samt fattar övergripande designbeslut. *Teknisk chef* (TC) ansvarar för *Designregler* (DR) och *Tekniska handlingsregler* (THR) inom eget verksamhetsområde och leder den tekniska designverksamheten genom att identifiera, definiera och fördela uppgifter och mandat för underliggande nivåer av tekniska system och deras samfunktion (system-av-system) samt fattar designbeslut inom eget verksamhetsområde.

Utsedda befattningshavare i enlighet med Försvarsmaktens arbets- och delegeringsordningar (ArbO) fastställer övergripande riktlinjer som styr systemsäkerhetsverksamheten som beskrivs i olika *Systemsäkerhetsledningsplaner* (SSMP). Dessa riktlinjer kan finnas på olika nivåer i verksamheten såsom arena, sammansatta systemnivåer samt enskild systemnivå.

Teknisk chef är tekniskt designansvarig för tilldelad produktportfölj. Uppgifter och mandat för underliggande områden inom produktportföljen kan via delegering fördelas till olika nivåer och befattningshavare. Teknisk chef fastställer *Systemsäkerhetsledningsplaner* (SSMP) för produktområde (eller visst tekniskt system) samt fastställer *Systemsäkerhetsgodkännanden* (SSG) inom egen produktportfölj.

SÄKINSP respektive FLYGI genomför tillsyn. SÄKINSP tecknar samråd på *Systemsäkerhetsgodkännanden* (SSG) och FLYGI gör detta vid behov.

Behörig chef fattar *Beslut om användning, central nivå* (BOAC).

C OrgE har arbetsgivar- och delegerad arbetsmiljöuppgift och har därmed ansvar för all verksamhet som bedrivs lokalt och för all materiel som används i

den verksamheten. C OrgE fattar *Beslut om användning, lokal nivå* (BOAL) samt ansvarar för att återrapportera drifterfarenheter såsom olyckor, tillbud och avvikelser.

4.2.2 Försvarsmakten i rollen som beställare

Försvarsmakten i rollen som *beställare* har att ansvara för och fatta beslut om:

– Kontrakt (eller motsvarande) gällande anskaffning eller ändring (modifiering) av tekniska system eller produkter.

Försvarsmakten följer upp systemsäkerhetsarbetet genom att kontrollera kravuppfyllnad mot kontrakt (eller motsvarande) utifrån *Systemsäkerhetsledningsplaner* (SSMP) och *Systemmålsättningar* (SMS). Vidare granskas mottagen systemsäkerhetsdokumentation från *konstruktör* eller *systemintegratör* samt bereder *Systemsäkerhetsgodkännande* (SSG) för beslut.

4.2.3 Försvarsmakten i rollen som systemintegratör

Försvarsmakten i rollen som *systemintegratör* genomför systemsäkerhetsarbete för att säkerställer samfunktion mellan tekniska system till ett system-av-system. Ett system-av-system ger efterfrågad förmåga eller funktionalitet genom nya kombinationer av fysiska produkter eller programvaror. Systemsäkerhetsarbetet dokumenteras i en *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL).

4.2.4 Försvarsmakten i rollen som konstruktör

Försvarsmakten i rollen som *konstruktör* har att ansvara för och fatta beslut om:

– Systemsäkerhetsplan (SSPP)
– Systemsäkerhetsutlåtande (SCA)

Försvarsmakten i rollen som *konstruktör* motsvarar i princip industrins roll nedan, vilket innebär konstruktions- och produktionsansvar. *Konstruktören* svarar på interna *Förfrågningsunderlag* (RFP) genom att ta fram en *Systemsäkerhetsplan* (SSPP) för systemsäkerhetsarbetet. Vidare utfärdar *konstruktören* ett *systemsäkerhetsutlåtande* (SCA) med *Systemsäkerhetsrapport* (SAR) och *Risklogg* (RL).

4.3 FMV:s roller

FMV anskaffar tekniska system och produkter från olika aktörer (leverantörer) såsom utvecklande industrin, annan stat, Försvarsmaktens verkstäder eller Fortifikationsverket.

FMV innehar rollerna *Beställare* och *Systemintegratör*.

FMV utövar det tekniska designansvaret fram till dess att godkänd överlämning skett till Försvarsmakten. Vidare kan FMV efter beställning medverka i Försvarsmaktens utvecklings-, vidmakthållande- och avvecklingsskeden, exempelvis genom att medverka i Försvarsmaktens *Arbetsgrupp för systemsäkerhet* (SSWG).

FMV i rollen som *beställare* tar fram en *systemsäkerhetsplan* (SSPP) som beskriver det systemsäkerhetsarbete som ska genomföras för aktuellt tekniskt system eller produkt. FMV utformar utifrån *Systemmålsättning* (SMS 2) ett *Förfrågningsunderlag* (RFP) för anskaffning. *Förfrågningsunderlaget* (RFP) omfattar nödvändiga tekniska systemsäkerhetskrav och krav på systemsäkerhetsverksamhet. I samband med systemöverlämning (SÖL) överlämnas *Systemsäkerhetsdeklaration* (SSD) med *Systemsäkerhetsrapport* (SAR) och *Risklogg* (RL).

FMV i rollen som *systemintegratör* genomför det systemsäkerhetsarbete som behöver genomföras för att säkerställa samfunktion mellan tekniska system till ett system-av-system. Systemsäkerhetsarbetet dokumenteras i en *Systemsäkerhetsrapport* (SAR) som överlämnas till *beställaren*. I samband med systemöverlämning (SÖL) överlämnar *Beställaren Systemsäkerhetsdeklaration* (SSD) med S*ystemsäkerhetsrapport* (SAR) och *Risklogg* (RL).

4.4 Fortifikationsverkets roller

Fortifikationsverket uppför och vidmakthåller anläggningar av olika slag för Försvarsmaktens behov. Anläggningar kan utgöra den miljö där tekniska system installeras, ansluts, förrådshålls eller brukas. Anläggningar kan, förutom skydd, även tillhandahålla vissa anläggningstekniska basresurser såsom el, kraft, värme, kyla, ventilation, vatten och avlopp. Framtagning av denna typ av resurser

hanteras genom beställning från Försvarsmakten till Fortifikationsverket, alternativt genom beställning från FMV. Fortifikationsverket överlämnar anläggningsdokumentation.

I de fallen Fortifikationsverket installerar tekniska system och produkter såsom datorutrustning eller larmanordningar i anläggningar ställs samma krav på systemsäkerhetsbeslut och systemsäkerhetsdokumentation som om FMV hade genomfört motsvarande arbete.

4.5 Industrins roll

Industrins huvudsakliga roll är *konstruktör*. I rollen *konstruktör* ingår även andra roller som får hanteras inom egen organisation.

Industrin innehar rollen som *Konstruktör*.

Industri som utvecklar, konstruerar och tillverkar tekniska system och produkter tar produktsäkerhets- och produktansvar (om det är juridiskt tillämpligt). Industrin svarar på *Förfrågningsunderlag* (RFP) genom att ta fram en *Systemsäkerhetsplan* (SSPP). Vid leverans överlämnas *Systemsäkerhetsutlåtande* (SCA) med *Systemsäkerhetsrapport* (SAR) och *Risklogg* (RL).

Industri som enbart utför serietillverkning överlämnar Leveranscertifikat (LC) som intygar att man följt tillverkningsunderlag och verifierat detta genom kvalitetsdokument.

En ekonomisk aktör såsom distributör inom EES-området, ansvarar för att enbart lagliga produkter köps in och säljs. En importör i EES-området, ansvarar för att enbart lagliga produkter importeras från tillverkare utanför EES-området, för att släppas ut på marknaden. Importören har en större del i produktsäkerhetsansvaret jämfört med distributören.

5 EU-rätt och svensk lagstiftning

Syftet med detta kapitel är att redovisa EU-rätt och svensk lagstiftning, vilka ställer krav på de systemsäkerhetsegenskaper som tekniska system och produkter ska ha för att inte oavsiktligt orsaka skada på person, egendom eller yttre miljö.

5.1 Bakgrund

Försvarsmakten har i sin egenskap som arbetsgivare ett juridiskt ansvar för sina anställdas säkerhet, men även för de som tillhör Hemvärnet, officersaspiranter, rekryter under utbildning, värnpliktiga och för de som ingår i en frivillig försvarsorganisation. Försvarsmakten har också ett juridiskt ansvar för tredje persons säkerhet och egendom i samband med den verksamhet Försvarsmakten bedriver. Försvarsmaktens uppgifter måste lösas inom ramen för gällande lagstiftning.

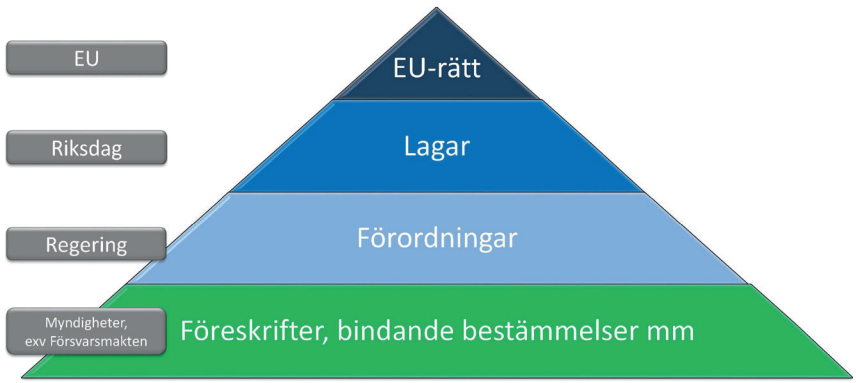


Bild 5.1 Hierarki över EU-rätt, lagar, förordningar, föreskrifter mm.

Ett tekniskt system kan bestå av flera olika delsystem och produkter. Det gäller att identifiera vilka regler som är tillämpliga för respektive teknikområde. Vissa regler styr konstruktionen och tekniska egenskaper såsom tryck, energi eller elektriska spänningsnivåer. I andra fall kan funktion/påverkan eller avsedd användning styra om reglerna är tillämpliga eller inte.

Tillverkare eller *systemintegratör* måste säkerställa att samfunktionen mellan olika delsystem och produkter (även vid system-av-system) analyseras fullt ut vad

gäller tillämplig EU-rätt och svensk lagstiftning för det totala tekniska systemet. Noteras bör att reglerna oftast lägger ansvar på legal/juridisk tillverkare, det vill säga den aktör som släpper ut en ny produkt på marknaden i sitt namn.

Formuleringar i EU-rätt och svensk lagstiftning är ofta skrivna teknikneutralt, vilket innebär att kraven uttrycks på sådant sätt att det inte spelar någon roll vilken teknik systemen byggs med. Säkra funktioner kan realiseras med olika tekniker såsom mekanik, pneumatik, hydraulik, pyroteknik, elektriska kretsar, elektronik, radiokommunikation eller programvara. Det viktiga är att tillverkaren har genomfört ett systemsäkerhetsarbete och sedan använt tekniker och metoder för att undvika fel vid konstruktion och tillverkning, det vill säga fel som kan leda till olyckor eller tillbud. I detta arbete ingår också att hantera olycksrisker under användning och underhåll.

I handboken redovisade referenser och dokumentbeteckningar är de som var aktuella vid handbokens färdigställande. I de fallen som referenserna behöver tillämpas rekommenderas att använda den gällande utgåvan av referensen.

5.2 EU-förordningar, EU-direktiv och harmoniserad standard

Inom den europeiska unionen (EES-området avseende friheten gemensam inre marknad) eftersträvas att harmoniera lagstiftningen inom flera områden för att möjliggöra rörlighet på den inre marknaden utan ytterligare tvingande krav och samtidigt garantera en hög nivå av säkerhet. Därför utfärdas EU/EG-direktiv/förordningar vilka riktar sig till medlemsstaterna respektive till berörda parter. EU-direktiv ska införlivas i respektive medlemsstats lagstiftning. I Sverige sker det oftast genom lag, förordning och föreskrifter.

Handboken använder i fortsättningen begreppet EU-direktiv när ett EU/EG-direktivs svenska överföringar till lag, förordning och föreskrifter egentligen avses. EU-direktiv används som begrepp även om rättsakten är en EU-förordning.

Ett EU-direktiv är bindande med avseende på det resultat som ska uppnås, men överlåter åt medlemslandet att bestämma tillvägagångssättet för överförandet. En EU-förordning verkar däremot direkt i varje medlemsland.

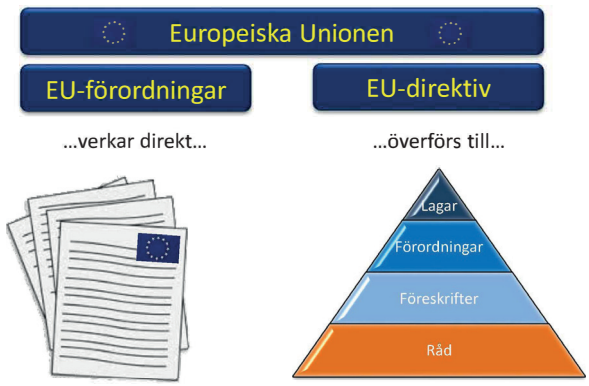


Bild 5.2 Införlivande av EU-förordningar respektive EU-direktiv i Sverige.

EU-direktiv och EU-förordningar anger grundläggande hälso- och säkerhetskrav på konstruktion och tillverkning, till skydd för person, husdjur, miljö och i viss mån egendom. De grundläggande hälso- och säkerhetskraven är minimikrav som måste uppfyllas för att produkterna ska få säljas/distribueras/användas inom EU/EES. Ofta finns krav på genomförande av riskanalys. Produkterna ska även motstå rimlig förutsebar felaktig användning utan att bli farliga. Kraven ska uppfyllas av varje enskild produkt för att den ska få släppas ut på den gemensamma inre marknaden *(placing on the market)* med avsikt att tas i bruk/användas *(put into service/to be used)* på denna marknad, exempelvis i Sverige.

Detaljerade krav kring teknisk utformning hänskjuts i praktiken till harmoniserade standarder. Dessa ställer krav på verifiering enligt angivna provmetoder. Ibland ställs krav på teknisk konstruktion, men principen är att en harmoniserad standard inte får låsa fast en konstruktionslösning eller vara utvecklingshämmande. Detta arbetssätt innebär att EU-direktiven och EU-förordningarna blir stabila och inte behöver ändras i samma takt som dagens tekniknivå ändras.

Respektive EU-direktivs tillämpningsområde varierar avseende hur och när det ska tillämpas på olika produkter.

För vissa teknikområden utfärdas EU-förordningar som verkar direkt i EU:s medlemsstater. De överförs således inte till svenska föreskrifter även om de ofta kompletteras av en förordning från Regeringen eller myndigheters föreskrifter. Exempel är EU-förordningar för vägfordon, personlig skyddsutrustning (PPE) samt medicintekniska produkter (MTP).

EU-förordningar är en del av svensk lagstiftning och vissa förordningar kan träda ikraft redan 20 dagar efter att de har offentliggjorts inom EU. EU-direktiv ska normalt införlivas samt tillämpas i svensk lagstiftning inom 18 månader från utgivandet. EU-direktiven innehåller krav på CE-märkning av produkterna varigenom tillverkaren visar och intygar att produkten överensstämmer med de lagstadgade kraven på säkerhet, hälsa och miljö.

Bild 5.3 Exempel på CE-märkning.

Standarder kan innehålla både normativa och informativa delar. De normativa delarna utgör fordringarna eller kraven i standarden. Det är de normativa delarna som ska efterlevas för att en produkt kan anses överensstämma med standarden. De informativa delarna kan utgöras av anmärkningar och förklarande bilagor till de normativa delarna.

En *beställare* kan ställa högre eller mer precisa krav på säkerhet än vad som anges i ett visst EU-direktiv eller viss harmoniserad standard utifrån den användningsmiljö och under de betingelser produkten ska användas i. Sådana högre krav ställs i *Förfrågningsunderlaget* (RFP) och hanteras genom CE-märkning.

Harmoniserade standarder är europastandarder utarbetade enligt riktlinjer som överenskommits mellan EU-kommissionen och de europeiska standardiseringsorganen och som följer ett mandat från Kommissionen. När en produkt uppfyller de normativa kraven i listade (dvs aktuella) harmoniserade standarder, antas produkten också uppfylla de motsvarande grundläggande säkerhetskraven i aktuellt EU-direktiv för produkten enligt den så kallade presumtionsprincipen.

Vilka harmoniserade standarder som ger presumtion anges i Kommissionens beslut som publiceras i europeiska unionens officiella tidning (EGT), *Official Journal* (OJ). Här anges även ifall det finns restriktioner till standarden respektive när den harmoniserade standardens presumtion upphör att gälla. I några speciella fall finns det kvar standarder som är tvingande, exempelvis inom vägfordonsområdet.

En harmoniserad standard är frivillig att följa. Flera, men mycket sällan alla, av EU-direktivets krav täcks av en (1) harmoniserad standard. Oftast behöver flera standarder tillämpas. Vilka krav i EU-direktivet som standarden anses uppfylla anges i ett Annex Z/ZA i respektive standard. Notera att de krav i ett EU-direktiv som den harmoniserade standardens presumtion inte täcker, måste tillverkaren ta hand om separat. Om tillverkaren inte följer harmoniserad standard som ger presumtion, blir det dock svårare och mer omständligt att verifiera att de grundläggande hälso- och säkerhetskraven är uppfyllda.

En fördel med gemensamma regler för produktsäkerhetsansvar och produktansvar är att en produkt kan släppas ut på marknaden i flera medlemsländer i ett och samma utförande, utan en upprepad godkännandeprocedur i varje enskilt medlemsland. De grundläggande hälso- och säkerhetsföreskrifterna är desamma i EU:s alla medlemsstater. Kraven i den nationella lagstiftning som överför direktiven är obligatoriska och måste uppfyllas för att produkten ska få släppas ut på marknaden. För produkter med måttliga olycksrisker förlitar sig EU-direktiven på tillverkarens egen verifiering att säkerhetskraven är uppfyllda. För produkter med större risker tillkommer krav på certifiering av tredje part, så kallat Anmält organ (Notified Body).

5.3 Arbetsmiljölagstiftning

Arbetsmiljölagens ändamål är att förebygga ohälsa och olycksfall i arbetet samt att även i övrigt uppnå en god arbetsmiljö. Arbetsmiljölagen reglerar såväl arbetsgivarens som arbetstagarens skyldigheter. Med arbetstagare i Försvarsmakten avses all personal, det vill säga anställd personal, de som tillhör Hemvärnet, officersaspiranter, rekryter under utbildning, värnpliktiga och för de som ingår i en frivillig försvarsorganisation, då dessa deltar i verksamhet inom Försvarsmakten.

5.3.1 Grunder

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

Enligt Arbetsmiljölagen 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.

5.3.2 Arbetsgivarens generella ansvar

Arbetsgivarens ansvar innebär att denne ska vidta alla åtgärder som behövs för att förebygga att arbetstagaren utsätts för ohälsa eller olycksfall. Arbetsgivaren ska systematiskt planera, leda och kontrollera verksamheten på ett sätt som leder till att arbetsmiljön uppfyller föreskrivna krav på en god arbetsmiljö. Arbetstagaren ska inte bara veta vilka olycksrisker som kan finnas, utan också ha kunskap om hur man kan undvika dem. Vidare ska arbetsskador utredas, olycksriskerna i verksamheten fortlöpande undersökas och åtgärder som föranleds av detta vidtas. När ändringar i verksamheten planeras, ska arbetsgivaren bedöma om ändringarna medför nya olycksrisker för ohälsa eller olycksfall som kan behöva åtgärdas.

Teknik, arbetsorganisation och arbetsinnehåll ska utformas så att arbetstagaren inte utsätts för fysiska eller psykiska belastningar som kan medföra ohälsa eller olycksfall. Även förläggning av arbetstid behöver beaktas. Starkt styrt eller bundet arbete bör undvikas eller begränsas. Maskiner, redskap och andra tekniska anordningar ska vara så beskaffade och placerade samt brukas på sådant sätt, att betryggande säkerhet ges mot ohälsa och olycksfall.

5.3.3 Leverantörens generella ansvar

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. Bruksanvisningar för anordningens montering, installation, användning och underhåll 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 för anordningen.

Den som tillverkar, importerar eller överlåter ett ämne, som kan föranleda ohälsa eller olycksfall, ska vidta de åtgärder som behövs för att hindra eller motverka att ämnet vid avsedd användning innebär risk från skyddssynpunkt. Produktinformation ska medfölja vid avlämnandet genom tydlig märkning, i form av handlingar eller på annat sätt.

Den som överlåter eller upplåter en förpackad produkt ska se till att förpackningen inte innebär olycksrisk för ohälsa eller olycksfall.

5.3.4 Föreskrifter utgivna med stöd av Arbetsmiljölagen

Arbetsmiljölagen är en ramlag som ger regeringen rätt att uppdra åt vissa myndigheter, i detta fall Arbetsmiljöverket och Transportstyrelsen, att vid behov utge kompletterande föreskrifter till lagen, vilket görs fortlöpande.

Arbetsmiljöverket har utfärdat ett antal föreskrifter med detaljerade krav och regler. Majoriteten av dessa är generella och gäller alltid. Arbetsmiljöverkets föreskrifter (AFS) ska vara väl kända och tillämpas hos den som mottar uppdrag avseende framtagning av materiel till Försvarsmakten. Arbetsmiljöverkets föreskrifter AFS 2008:3 om Maskiner, vilka överför EU-direktiv 2006/42/EU, är centrala då mycket materiel faller in under dessa regler.

I vissa av Arbetsmiljöverkets föreskrifter (AFS) finns specificerade gränsvärden för till exempel luftföroreningar (hygieniska gränsvärden) samt för buller och vibrationer. Dessa gränsvärden ska speciellt beaktas.

5.3.5 Undantag för militär användning och militär materiel

Vissa föreskrifter medger vissa undantag för militär användning och/eller militär materiel. Exempel på sådana föreskrifter är AFS 2020:1 Arbetsplatsens utformning, Radioutrustningsdirektivet (RED) genom Post- och telestyrelsen föreskrifter om krav med mera på radioutrustning PTSFS 2016:5, respektive AFS 2008:3 Maskiner. Om produkten (eller en liknande produkt) kan ha dubbla

användningsområden *(dual use)*, det vill säga kan användas både civilt respektive militärt, så kan militärt undantag inte åberopas utan produkten ska CE-märkas.

Genom undantaget för militär användning avser lagstiftaren att ge Försvarsmakten viss handlingsfrihet att utforma tekniska system enligt ”krigets krav”, men med fortsatt innehållande av grundkravet som ställs på arbetsgivaren i Arbetsmiljölagen. För att kunna använda handlingsfriheten på ett ansvarsfullt sätt behöver Försvarsmakten ta fram egna *Designregler* (DR), tillämpningsanvisningar med riktlinjer, gränsvärden med mera, som Försvarsmakten definierar som tolerabla för svensk militär personal.

Arbetsmiljöverkets föreskrifter AFS 2008:3 Maskiner, undantar maskiner som är *särskilt* konstruerade och tillverkade för *militära* eller polisiära *ändamål.* Bakgrunden till detta undantag för viss militär materiel är att visst militärt ändamål ställer krav på avancerad materiel, ofta grundad på ny teknik respektive särskilda applikationer vilka om möjligt inte ska delges potentiell motståndare. Om sådana teknologier eller applikationer är säkerhetsskyddsklassificerade uppgifter (försvarssekretess) kan CE-märkning inte genomföras.

Om lagstiftningen medger undantag för viss militär materiel respektive militär användning och eventuellt 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 2020:1 Arbetsplatsens utformning).

Att ett regelverk medger undantag för viss militär materiel hindrar inte att regelverkets krav ändå tillämpas i den utsträckning det är möjligt.

6 Standarder

Syftet med detta kapitel är att beskriva civil och militär standardisering samt att presentera de vanligast förekommande internationella standardiseringsorganen.

6.1 Allmän beskrivning av standarder

Standardisering sker såväl civilt som inom försvarsområdet, både nationellt och internationellt. I Lagen om offentlig upphandling (LOU) samt i Lagen om offentlig upphandling inom försvarsområdet (LUFS) finns en prioriteringsordning som bestämmer i vilken ordning standarder ska användas. Om undantag behöver göras ska de vara proportionerliga och skälen behöver vara väl beskrivna. Prioriteringen är framtagen för att så långt som möjligt undvika nationella särkrav mellan de olika medlemsländerna inom EU.

Det är frivilligt att följa en standard till dess att någon hänvisar till att den ska uppfyllas, exempelvis i föreskrifter eller i ett kontrakt, men kravet från en myndighet måste i båda fallen enligt Lagen om offentlig upphandling (LOU) alltid följas av orden ”…*eller likvärdig*”. Undantag från detta krav får hanteras från fall till fall.

Det är frivilligt att följa en standard till dess att någon hänvisar till att den ska uppfyllas. I de flesta fall behöver man ändå följa standarder då det i praktiken inte finns några andra alternativ till att uppfylla regelverkets säkerhetskrav.

Det finns många vinster med att använda standarder såsom interoperabilitet, funktionalitet, tekniksamordning, gemensamma komponenter, säkerhet, driftsäkerhet, tillförlitlighet, kompatibilitet med generella logistiksystem, total ägandekostnad och andra liknande försvarsrelaterade krav.

Med standard i denna handbok menas både formellt fastställda standarder utgivna av standardiseringsorgan och standardliknande dokument i form av vägledningar (guidelines) och manualer (manuals) utgivna av branschorganisationer.

Användaren av en viss standard bör alltid införskaffa den från utgivaren. Dels för att ha tillgång till den senaste utgåvan, dels på grund av eventuell upphovsrätt.

6.2 Civila standarder

Civila standarder används av både militära och civila myndigheter, andra tekniska organisationer samt av utvecklande industri.

Sverige deltar i internationell standardisering genom de tre av staten erkända standardiseringsorganen:

- Svensk Elstandard (SEK)
- Svenska institutet för standarder (SIS)
- Svenska Informations- och Telekommunikationsstandardiseringen (ITS)

SEK är medlem i de internationella standardiseringsorganisationerna CENELEC (europeisk) och IEC (global), SIS är medlem i CEN och ISO samt ITS är medlem i ETSI.

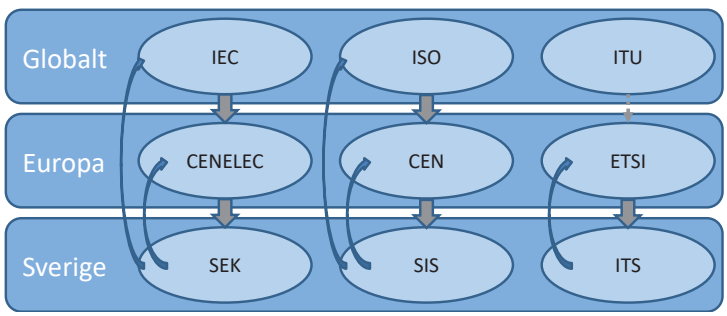


Bild 6.1 Förenklad bild över relationen mellan olika erkända standardiseringsorgan.

6.3 Försvarsstandarder

Försvarsstandarder används av både militära och civila myndigheter, andra tekniska organisationer samt av utvecklande industri. Försvarsstandarder har

olika informationssäkerhetsklasser vilket behöver beaktas vid kravställning mellan olika aktörer, då vissa omfattas av försvarssekretess.

Försvarsstandarder kan generellt delas in i operativa standarder, förmågestandarder samt tekniska standarder. NATO:s standarder bedöms inofficiellt av både EU och FN som internationella försvarsstandarder. Dessa standarder används frivilligt av NATO:s medlemsländer och partners. Dock kan användning av NATO-standarder påverkas av överenskomna partnerskapsmål inom ramen för *Partnership for Peace Planning and Review Process* (PARP). NATO anvisar användning av de standarder som partnerländer ska implementera vid samverkan med NATO-förband.

De tekniska standarderna är mer nationsspecifika och omfattar till exempel standarder för färg, ballistiskt skydd och elkvalitet för vapen på fartyg. Det finns ett stort antal myndigheter och statliga organisationer som på olika sätt skapar försvarsstandarder oberoende av varandra.

6.4 Funktionen för Försvarsstandardisering organiserad vid FMV

Försvarsstandardisering etablerades 1944, då Försvarets standardiseringsdelegation bildades för myndighetsgemensam standardisering. År 1976 upphävde regeringen Försvarets standardiseringsdelegation och beslöt att ansvaret för standardisering inom specifika områden skulle fördelas på respektive myndighet under Försvarsdepartementet. Vidare beslöt regeringen att FMV skulle hålla samman gemensamma standardiseringsfrågor och tillhandahålla myndighetsgemensamma sekretariatsfunktioner i samråd med myndigheterna under Försvarsdepartementet. Dessutom skulle FMV ansvara för de nationella försvarsstandarderna (FSD).

FMV håller samman frågor om standarder inom försvarsområdet genom Försvarsstandardisering (FSD). FSD har till uppgift att administrera och tillhandahålla såväl internationella som nationella försvarsstandarder samt

tillhandahålla civila standarder till de ingående myndigheterna. FSD tillhandahåller även tjänster inom myndighetsgemensam standardisering till myndigheterna under Försvarsdepartementet och deras leverantörer. Anställda inom försvarsmyndigheter hittar fakta om FSD på deras hemsida. De myndigheter som idag omfattas är:

- Försvarsmakten (FM)
- Försvarets materielverk (FMV)
- Försvarets radioanstalt (FRA)
- Kustbevakningen (KBV)
- Myndigheten för samhällsskydd och beredskap (MSB)
- Totalförsvarets forskningsinstitut (FOI)
- Försvarshögskolan (FHS)

Även andra myndigheter, statliga affärsverk såsom LFV samt utvecklande industri tillämpar vissa svenska försvarsstandarder (FSD) i sin verksamhet.

7 Försvarsmaktens regelverk

Syftet med detta kapitel är att beskriva Försvarsmaktens interna regelverk och handböcker. Dessa behöver beaktas vid kravställning då interna regelverk, jämfört med motsvarande civila krav, kan skilja sig åt eller att kraven i de interna regelverken är mer detaljerade.

7.1 Försvarsmaktens författningssamling (FFS) och Försvarsmaktens interna bestämmelser (FIB)

Försvarsmakten beslutar om föreskrifter i form av författningar som kungörs i Försvarets författningssamling (FFS) och i Försvarsmaktens interna bestämmelser (FIB). Vidare finns Försvarsmaktens allmänna råd (FAR). FFS, FIB och FAR beslutas av ÖB eller av denne bemyndigad. Vissa FFS beslutas av Försvarsinspektören för hälsa och miljö (FIHM).

FFS innehåller bestämmelser som även riktar sig till andra myndigheter såsom Fortifikationsverket, Totalförsvarets forskningsinstitut (FOI) och FMV, men även till företag eller enskilda. Detta beror på vilket bemyndigande Försvarsmakten har att utfärda bestämmelser inom ett visst område, exempelvis Regler för militär luftfart (RML).

FIB innehåller bestämmelser som kan omfatta regelkrav som måste uppfyllas för att ett tekniskt system eller produkt ska få användas i Försvarsmakten. I *Systemmålsättnin*g (SMS 2) behöver samtliga tillämpbara FIB anges, exempelvis de inom Regler för militär sjöfart (RMS).

Innehållet i FIB och FAR kan behöva överföras till krav i *Förfrågningsunderlaget* (RFP).

7.2 Regler för militär luftfart (RML)

Enligt Luftfartslagen (SFS 2010:500) är all verksamhet som anses som luftfartsverksamhet tillståndspliktig. Försvarsmakten har i enlighet med Luftfartsförordningen (SFS 2010:770) bemyndigats att utfärda föreskrifter och utöva tillsyn över militär luftfart. Försvarsmakten reglerar detta genom Försvarsmaktens föreskrifter om militär luftfart FFS 2019:10, FFS 2020:4 och där utpekade reglementen, handböcker samt tillämpningsbestämmelser SE-EMAR *(European Military Airworthiness Requirements)*, samlat benämnt Regler för militär luftfart (RML). 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-kommissionen, genom EASA *(European Aviation Safety Agency)*, ansvarar för reglering och tillsyn av de viktigare delarna av civil luftfart. Inom militär luftfart samarbetar EU-länder inom ramen för EDA *(European Defence Agency)* och har skapat gemensamma krav för luftvärdighet med mera i form av EMAR *(European Military Airworthiness Requirements)* vilket omsatts till nationella tillämpningsbestämmelser SE EMAR.

Det militära luftfartssystemet omfattar verksamhet för flygdrift, flygplatser och flygbaser samt för luftrum. De tre systemen omfattar, inom respektive delområde, verksamhetsutövare inklusive personal, flygmaterielsystem och övriga luftfartsprodukter, system för flygplatser och flygbaser, mark, anläggningar och lokaler, luftfartsrelaterade anordningar och utrustning ombord på sjögående fartyg och andra installationer samt det luftrum som tillgodoser behovet för luftfartygens manövrering.

Försvarsmakten ska bedriva militär luftfart utifrån en tolerabel risk som kan variera beroende på aktuella förhållanden och uppgifter. Överbefälhavaren, eller den överbefälhavaren bestämmer, avgör vad som är tolerabel risk. Detta tillämpas inom Försvarsmakten (Reglemente Ledning av Militär Luftfart, R LML) i form av flygsäkerhetsrisk som omfattar det som påverkar flygning, det vill säga alla de olika tjänster och verksamheter som inverkar. Begreppet tolerabel risk är därmed inte överensstämmande med begreppet *Tolerabel risknivå* (TR) inom systemsäkerhet.

Regler för luftfartyg finns, genom RML, i tillämpningsbestämmelser SE EMAR och avser luftvärdighet, vilket innebär att människa och egendom inte ska skadas vid, eller i direkt anslutning till flygning. Detta innebär att kompletterande systemsäkerhetskrav behöver ställas på tekniska system som omfattar luftfartyg eller andra luftfartsprodukter för att uppnå betryggande säkerhet för hela det tekniska systemet.

7.3 Regler för militär sjöfart (RMS)

Försvarsmakten reglerar militär sjösäkerhet genom Regler för militär sjöfart (RMS). RMS kommer allt eftersom att ersättas av Försvarsmaktens interna bestämmelser (FIB) för militär sjöfart. I begreppet militär sjösäkerhet ingår både fartygssäkerhet och dyksäkerhet.

För att ett örlogsfartyg ska få användas i Försvarsmakten ska det finnas ett giltigt sjövärdighetsbevis. För dyksystem ska det finnas ett giltigt dyksäkerhetsbevis. Sådana bevis, tillsammans med övriga certifikat och dokument som regleras i Regler för militär sjöfart (RMS) och andra gällande föreskrifter, styrker att gällande regelverk är uppfyllda.

Regler för militär sjöfart (RMS) omfattar regler för bland annat tillsyn, sjösäkerhetssystem, bemanning och behörighet, konstruktions- och utrustningskrav (för både örlogsfartyg och dyksystem) samt åtgärder mot förorening. Detta innebär i praktiken att Försvarsmakten genom den militära sjösäkerhetsinspektionen (SJÖI) dels utformar Regler för militär sjöfart (RMS), dels utövar Försvarsmaktens interna tillsyn av att dessa regler följs.

7.4 Försvarsmaktens Reglemente Verksamhetssäkerhet (SäkR)

Försvarsmaktens Reglemente Verksamhetssäkerhet (SäkR) innehåller bestämmelser för att verksamheten ska genomföras säkert, det vill säga med en tolerabel risk för personal och tredje man samt för att minimera skador på materiel, egendom och yttre miljö. Bestämmelser ska tillämpas vid utbildning och övningar samt under insats i fred, vid höjd beredskap och vid insats som inte innebär stridshandling. SäkR riktar sig till chefer för organisationsenheter (C OrgE), övningsledare, truppförande chefer samt övrig personal som deltar i Försvarsmaktens verksamhet.

Underlag till SäkR hämtas från *Systemsäkerhetsgodkännanden* (SSG), *Systemsäkerhetsmeddelande* (SSM) samt från erfarenheter av tekniska system under användning och underhåll.

7.5 Övriga reglementen och handböcker

Försvarsmakten ger för viss lagstiftning ut reglementen och kompletterande handböcker, exempelvis:

- Handbok Förvaring och transport av ammunition och övriga explosiva varor (H IFTEX)
- Handbok för åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor (H BVKF)
- Handbok Grundtillsyn av fordon (FAG F)

8 Designregler och tekniska handlingsregler

Syftet med detta kapitel är att beskriva avsikt och tillämpning av Designregler (tekniska krav) och tekniska handlingsregler (administrativa krav) hos olika aktörer.

8.1 Allmänt om designregler och tekniska handlingsregler

Designregler (DR) avser att styra utformning av tekniska system och produkter i syfte att uppfylla krav på egenskaper såsom prestanda, tillgänglighet, samfunktion mellan system, ekonomi samt informations- och systemsäkerhet.

Designregler (DR), ur ett systemsäkerhetsperspektiv, kan omfatta krav på viss konstruktion eller krav på principer för sådan konstruktion så att kända olycksrisker reduceras eller undviks. Syftet är att för beprövad teknik ange lämpligt sätt att förebygga eller reducera effekten av kända olycksrisker.

Tekniska handlingsregler (THR) syftar till att styra administrativa rutiner i samband med utformning av tekniska system och produkter samt för att underlätta användning, underhåll, förrådshållning (transport) och avveckling (återanvändning). *Tekniska handlingsregler* (THR) anger hur administration runt tekniska system och produkter ska genomföras och är inte direkt designpåverkande.

8.2 Försvarsmaktens designregler och tekniska handlingsregler

Militär verksamhet kan innebära att Försvarsmakten behöver strängare systemsäkerhetskrav på materielen än vad lagstiftningen föreskriver för att uppnå betryggande säkerhet. Försvarsmakten kan då fastställa dessa strängare systemsäkerhetskrav som till exempel *Designregler* (DR) så att viss konstruktion eller konstruktionsprincip tillämpas, eller att ett visst strängare gränsvärde innehålls.

För militär materiel som är särskilt konstruerad och tillverkad för visst militärt ändamål, eller för övrig militär verksamhet, medges ibland undantag från föreskrifters krav, till exempel avseende gränsvärden i Arbetsmiljöverkets olika föreskrifter. Om behov finns kan Försvarsmakten ta fram egna *Designregler* (DR) med riktlinjer och gränsvärden som Försvarsmakten definierar som tolerabla för svensk militär personal. Även andra typer av styrningar kan tas fram av Försvarsmakten. Dessa kan, men behöver inte, omsättas till *Designregler* (DR).

Att hantera olycksrisker genom att hålla sig inom fastställda gränsvärden förordas framför värdering av motsvarande olycksrisk mot en *Tolerabel risknivå* (TR) uttryckt i riskmatris. Gränsvärdet kopplas direkt till aktuella olycksrisker medan den tolerabla risknivån är generell. Ett uttalat krav på gränsvärde ger mindre utrymme för tolkningar och subjektiva bedömningar och kan dessutom användas för olika tekniska system och produkter. Om sådana gränsvärden inte har tagits fram, hanteras frågan istället som risk för viss skadeverkan och värderas mot aktuellt tekniskt systems tolerabla risknivå uttryckt i riskmatris.

Försvarsmaktens Tekniska direktör fastställer försvarsmaktsgemensamma *Designregler* (DR) och *Tekniska handlingsregler* (THR) och respektive Teknisk chef har fastställer *Designregler* (DR) och *Tekniska handlingsregler* (THR) inom eget verksamhetsområde. Utöver ovanstående kan Försvarsmaktens Tekniska direktör fastställa direktiv, anvisningar och instruktioner inom ramen för Försvarsmaktens designverksamhet. Försvarsmakten vidmakthåller en förteckning över fastställda gemensamma och domänspecifika *Designregler* (DR) och *Tekniska handlingsregler* (THR).

Tillämpliga *Designregler* (DR) och *Tekniska handlingsregler* (THR) för det tekniska systemet eller produkterna ska specificeras i *Systemmålsättning* (SMS 2).

Information kan även samlas in systematiskt från användning och underhåll. Informationen kan bestå av olycks- och tillbudsrapporter, felutfall, prestandabrister eller tekniska statusundersökningar. Vid uppföljning av inträffade olyckor, tillbud och avvikelser, uppstår normalt ny kunskap om tekniska systems olycksrisker. Det är angeläget att denna information inklusive vidtagna riskreducerande åtgärder kommer till FMV:s och tillverkarens (industrins) kännedom.

De av Försvarsmakten beslutade *Designreglerna* (DR) gäller, i förekommande fall, för de uppdrag och beställningar som FMV utför åt Försvarsmakten.

8.3 FMV:s designregler och tekniska handlingsregler

FMV vidmakthåller en förteckning över fastställda *Designregler* (DR), handböcker (designregelsamlingar) och *Tekniska handlingsregler* (THR) som ska tillämpas vid anskaffning och ändring (modifiering) av tekniska system och produkter.

Om Försvarsmakten identifierar en säkerhetsbrist under användning eller underhåll av tekniskt system tar FMV på beställning från Försvarsmakten fram konstruktionslösningar i syfte att eliminera olycksrisken eller att minska sannolikhet för upprepade olyckor och/eller minska dess konsekvenser om olyckan ändå inträffar. Den nya konstruktionslösningen som införs skulle kunna tillämpas vid en framtida användning av motsvarande teknik. Erfarenheter från sådana konstruktionsändringar kan omformas till generella konstruktionskrav till en *Designregel* (DR). Även kunskap som framkommit genom omvärldsanalys eller genom nya/reviderade standarder kan tas in i *Designregeln* (DR).

Handböcker (designregelsamlingar) tas antingen fram för att tekniska system inom ett visst område bedöms kunna ha högre risker eller att det sedan tidigare finns generell kunskap om systemområdets olycksrisker. I flera fall har nya *Designregler* (DR) för en hel systemgrupp dokumenterats och börjat tillämpats efter utredningar av faktiska olyckor som kunnat påvisa att brister i ett tekniskt system varit bidragande orsaker till olyckans inträffande.

FMV:s handböcker (designregelsamlingar) inom systemsäkerhetsområdet är:
- Handbok Vapen- och Ammunitionssäkerhet (H VAS)
- Handbok för Programvara i säkerhetskritiska tillämpningar (H ProgSäk)
- Handbok för Fordonssäkerhet (H FordonSäk)
- Handbok Säkra elektriska produkter och system (H SEPS)
- Handbok för Säkra fältmässiga arbetsplatser (H SFAPL)

Det finns även andra handböcker utgivna av FMV som ställer krav på tekniska system och produkter, t ex Handbok EMMA (Handbok Elektromagnetisk miljö användarhandbok)

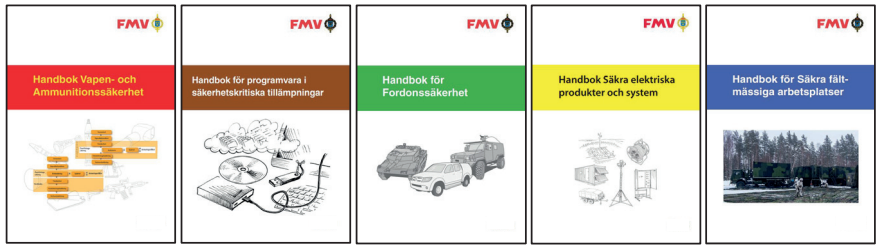


Bild 8.1 *FMV:s handböcker (designregelsamlingar) inom systemsäkerhetsområdet.*

I de fallen områdesspecifika handböcker (designregelsamlingar) finns så tillämpas dessa parallellt med Handbok Systemsäkerhet. Om det tekniska systemet inkluderar vapen och/eller ammunition ska FMV Handbok Vapen- och ammunitionssäkerhet (H VAS) användas tillsammans med denna handbok. Motsvarande gäller för övriga produktsäkerhetsområden där det tekniska systemet exempelvis inkluderar plattformar, programvara och elektriska produkter.

FMV:s områdesspecifika handböcker kan dels tillämpas frivilligt, dels göras tvingande genom direktiv inom en organisation eller genom kontrakt (eller motsvarande) till en annan aktör (myndighet) eller en tillverkare (industrin).

Tekniska handlingsregler (THR) kan finnas för att tekniska system ska uppfylla särskilda regler, genomföra viss provning eller genomgå oberoende granskning inför användning inom ett visst teknikområde. Vidare kan regler för exempelvis krav på förvaltningsdata finnas.

De enskilda krav som ska gälla för aktuellt tekniskt system eller produkt, ska hämtas ur *Designreglerna* (DR), handböckerna (designregelsamlingarna) och de *Tekniska handlingsreglerna* (THR). Dessa krav skrivs in i den tekniska specifikationen (TS) för det tekniska systemet respektive i verksamhetsåtagandespecifikationen (VÅS) om kravet är av verksamhetskaraktär.

Designregler (DR), handböcker (designregelsamlingar) och *Tekniska handlingsregler* (THR) har inte samma status som harmoniserad standard och ger således inte presumtion om överensstämmelse med ett EU-direktivs grundläggande krav.

Krav hämtade från *Designregler* (DR), handböcker (designregelsamlingar) och *Tekniska handlingsregler* (THR) för tekniska system och produkter ska specificeras i *Förfrågningsunderlaget* (RFP)

8.4 Tillverkarens konstruktionsregler

Tillverkarens konstruktionsregler syftar främst till att uppfylla EU-rätt, svensk lagstiftning samt tekniska standarder.

Tillverkaren finns ofta på en eller flera konkurrensutsatta marknader. För att bibehålla eller öka sina marknadsandelar krävs att de produkter som marknadsförs är tillräckligt säkra samt har konkurrenskraftig prestanda och god tillgänglighet. Vidare krävs att produkterna följer internationella standarder för att undvika tekniska handelshinder på den globala marknaden.

9 Språk

Syftet med detta kapitel är att redogöra för EU-rättens och Försvarsmaktens krav på språk för teknisk information. Det är angeläget att information kan förstås av användaren och särskilt viktigt att säkerhetsbestämmelser inte missförstås på grund av språkförbistringar. Försvarsmakten behöver därför ställa krav på språk för olika användargränssnitt och materieldokumentation.

9.1 Språk för olika användargränssnitt

Ett grafiskt användargränssnitt, är en form av informationsbärare som gör att användaren kan interagera genom grafiska symboler och alarm, istället för textbaserade användargränssnitt eller textnavigering. Användarinstruktioner kan, förutom att vara i form av en tryckt bruksanvisning, visas på tryckknappar, på tryckkänsliga skärmar eller som projicerad information i en *Head-up display* (HUD). Texter på tryckknappar och på tryckkänsliga skärmar omfattas normalt också av språkkravet i EU-direktiven. Samma språkkrav gäller även i de fallen produkten talar/läser upp instruktioner för handhavande.

9.2 Språk i teknisk information för försvarsmateriel

Rätten, skyldigheten och ansvaret att ge ut nödvändiga styrande och informativa dokument för tekniska system följer med det tekniska designansvaret.

Med teknisk information för försvarsmateriel avses materieldokumentation och tekniska data. Materieldokumentation är den dokumentation som erfordras för säker användning, underhåll, hantering, försörjning och modifiering. Med tekniska data avses sådant som ska redovisas i olika förvaltningssystem. Hit hör exempelvis säkerhetsdatablad (*Safety Data Sheets,* SDS) för kemiska produkter.

Materieldokumentation är ett samlingsbegrepp för både tryckta skrifter (inbundna eller lösblad) och elektroniska dokument som främst behandlar funktion, handhavande, drift och underhåll. Det kan även vara varselmärkningar såsom skyltar och dekaler fästa på tekniska system och produkter.

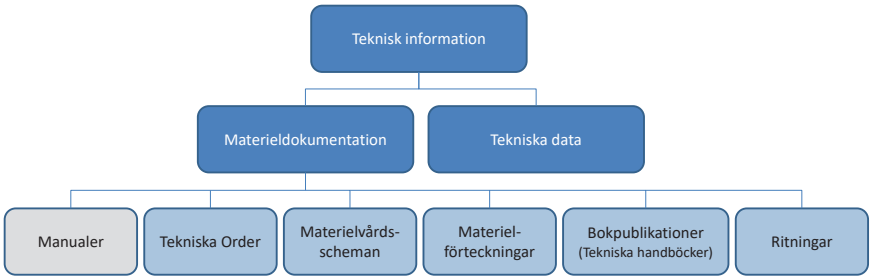


Bild 9.1 *Förenklad bild över teknisk information vid Försvarsmakten.*

För teknisk information för försvarsmateriel används en annan nomenklatur vid FMV.

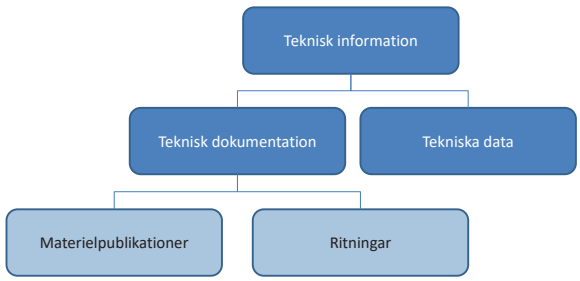


Bild 9.2 *Förenklad bild över teknisk information vid FMV.*

Språk för materieldokumentationen specificeras i *Systemmålsättningen* (SMS 2) Inom vissa områden finns det regelkrav (EU-rätt, svensk lagstiftning, Försvarsmaktens interna bestämmelser (FIB) eller designregler/tekniska handlingsregler) som anger att säkerhetsinstruktioner ska vara skrivna på svenska. Normalt sett bör all materieldokumentation avsedd för användaren finnas på svenska, medan övrig teknisk dokumentation och tekniska data kan vara på engelska.

Inom vissa områden, exempelvis flygområdet, är engelska huvudspråket och då är översättning till svenska inte aktuellt. Bedöms den tekniska personalen som ska underhålla materielen, exempelvis en helikopter eller en vägambulans, ha erforderliga kunskaper i teknisk engelska kan engelska väljas som språk för materieldokumentationen.

I de fallen tillverkarens bruksanvisningar och underhållsinstruktioner samt varselmärkning såsom skyltar och dekaler ska översättas till svenska är det tillverkaren av det tekniska systemet som ansvarar för denna översättning. I systemsäkerhetsbeslutet ska det finnas angivet att den tekniska informationen utgör en översättning och från vilket språk denna är gjord. Den utländska versionen av texten ska ingå i den produktdokumentation som levereras.

Om Försvarsmakten eller FMV tillhandahåller skyltar och dekaler för varselmärkning till tillverkaren är det Försvarsmaktens eller FMV:s ansvar att dessa uppfyller svensk lagstiftning och att eventuell text är korrekt.

9.3 Språk i teknisk information för CE-märkta produkter

Tillverkaren (den legala tillverkaren) som CE-märker en produkt ska uppfylla svensk lagstiftning inklusive EU-direktiv inom området. I samband med CE-märkningen ska tillverkaren upprätta teknisk dokumentation för produkten samt utfärda en Försäkran om överensstämmelse (DoC). Den tekniska dokumentationen (*Technical file*) sammanställs av tillverkaren och är enbart avsedd för marknadskontrollerande myndigheter och inte för användaren av produkten. Den tekniska dokumentationen (*Technical file*) är en delmängd av produktens totala konstruktions- och tillverkningsunderlag och ska finnas på ett EU-språk, exempelvis engelska.

Både EU-förordningar och EU-direktiv överförd till svensk lagstiftning, föreskriver att dokumentation avsedd för den dagliga användaren såsom säkerhetsinstruktioner och märkningar samt instruktioner för montering, installation och användarens dagliga underhåll ska upprättas på ett av de officiella språk (ej minoritetsspråk) i landet där produkten ska användas, det vill säga svenska. Underhållsinstruktioner (servicemanual) för teknisk personal är avsedd för de som ska underhålla, reparera eller kalibrera produkten. Teknisk personal kan finnas inom tillverkarens egen organisation eller hos annan aktör, exempelvis Försvarsmakten. Underhållsinstruktionerna ska finnas på ett EU-språk, exempelvis engelska, som den tekniska personalen oftast förväntas kunna.

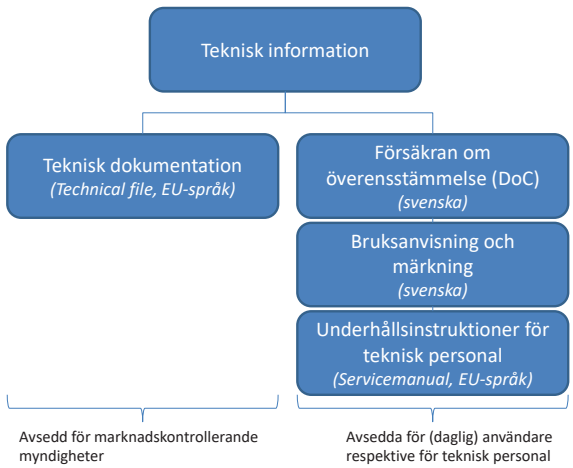


Bild 9.3 *Teknisk information i samband med CE-märkning.*

Vid en CE-liknande process för produkter som är undantagna ett EU-direktiv, och som istället är särskilt framtagna för visst militärt ändamål kan godkännanden och övriga redovisande dokument vara skrivna på det språk, företrädelsevis svenska eller engelska, som avtalats i kontrakt. Krav på accepterade språk för teknisk information specificeras i *Systemmålsättningen* (SMS 2).

9.4 Språk enligt EU-förordningen REACH

EU-förordningen REACH *(Registrering, utvärdering, godkännande och begränsning av kemikalier)* anger att säkerhetsdatablad för kemiska produkter ska tillhandahållas på ett officiellt språk i den medlemsstat där den farliga produkten släpps ut på marknaden. Därför ska säkerhetsdatablad vara skrivna på svenska för kemiska produkter som släpps ut på den svenska marknaden

9.5 Språk vid anskaffning av MOTS

Vid anskaffning av MOTS-produkter (*Military Off the Shelf*) och vid internationella samarbeten med organisationer eller annan stat, kan godkännanden och övriga redovisande dokument vara skrivna på det språk, företrädelsevis engelska, som avtalats i kontrakt. Krav på accepterade språk för teknisk information specificeras i *Systemmålsättningen* (SMS 2).

9.6 Språk i redovisande och beslutsdokument

Systemsäkerhetsbeslut såsom *Systemsäkerhetsdeklaration* (SSD), *Systemsäkerhetsgodkännande* (SSG) och *Systemsäkerhetsmeddelande* (SSM) ska vara skrivna på svenska.

Vid exportaffärer utfärdas systemsäkerhetsbeslut och övrig systemsäkerhetsdokumentation på det språk som avtalats i kontrakt med aktuell stat.

Tillverkaren ska i redovisande och beslutsdokument såsom *Systemsäkerhetsplan* (SSPP), *Systemsäkerhetsutlåtande* (SCA), *Systemsäkerhetsrapport* (SAR) samt i *Riskloggen* (RL) skriva dessa på svenska eller på det språk som avtalats i kontrakt. Övriga dokument ska vara på svenska eller engelska, eller på det språk som avtalats i kontraktet.

10 Anskaffning av tekniska system

Syftet med detta kapitel är att ge vägledning för hur systemsäkerhetsarbetet kan anpassas beroende på lagstiftning, kategorier av tekniska system eller produkter samt om dessa ska anskaffas, återanskaffas eller ändras (modifieras).

10.1 Allmänt om anskaffning av tekniska system och produkter

Utifrån EU-rätt, svensk lagstiftning och det tekniska systemets komplexitet, beskaffenhet och riskinnehåll behöver omfattningen på systemsäkerhetsarbetet anpassas.

All materiel som ska ingå i ett krigsförband eller som ska användas i Försvarsmaktens förbandsverksamhet, behöver genomgå ett väl avvägt systemsäkerhetsarbete.

Standardprodukter utan undantag för militär materiel, exempelvis CE-märkta, som anskaffas för övrig verksamhet och som används i enlighet med tillverkarens anvisningar kan tas i bruk utan att genomgå ett systemsäkerhetsarbete. Notera dock att all form av samfunktion i ett annat tekniskt system behöver analyseras ur ett systemsäkerhetsperspektiv.

Tekniska system och produkter som återanskaffas och som redan finns registrerade i Försvarsmaktens förvaltningssystem kräver inget förnyat systemsäkerhetsarbete så länge de används och underhålls enligt tidigare utfärdade systemsäkerhetsbeslut. Notera dock att om EU-direktiv eller harmoniserade standarder har ändrats krävs en ny Försäkran om överensstämmelse (DoC). Om serietillverkning återupptas kan en ny verifiering erfordras.

10.2 Gränsytor mellan tekniska system och anläggningar

Anläggningar är en av flera olika omgivningsmiljöer där det tekniska systemet ska kunna installeras, anslutas, förrådshållas eller brukas. Anläggningar i sig ska inte ingå i systemsäkerhetsbesluten.

Anläggningar kan, förutom skydd, även tillhandahålla vissa anläggningstekniska basresurser såsom el, kraft, värme, kyla, ventilation, vatten och avlopp för att upprätthålla såväl funktion som säkerhet hos materielen. Anläggningars gränsytor, alternativt med basresurserna inkluderat, mot tekniska system och produkter kan hanteras på olika sätt beroende på hur dessa definieras. Val av modell enligt nedan ska framgå av *Systemmålsättningen* (SMS 2):

- **Alternativ 1:**
  Det tekniska systemets krav på de *anläggningstekniska basresursernas gränsytor* samt dess prestanda och kvalitet ska ingå i systemsäkerhetsbesluten.
- **Alternativ 2:**
  Det tekniska systemet ska tillsammans med de *anläggningstekniska basresurserna* ingå i systemsäkerhetsbesluten.

Benämningen *anläggningar* tillämpas ibland på materiel, exempelvis en vapenkassun, som i denna handbok benämns som tekniska system eller produkter.

10.3 Uppbyggnad av tekniska system och produkter

I arkitekturen för systemlösningen identifieras hur ett system-av-system lämpligast byggs upp av olika systemelement (tekniska system, delsystem, produkter och integrationsprodukter).

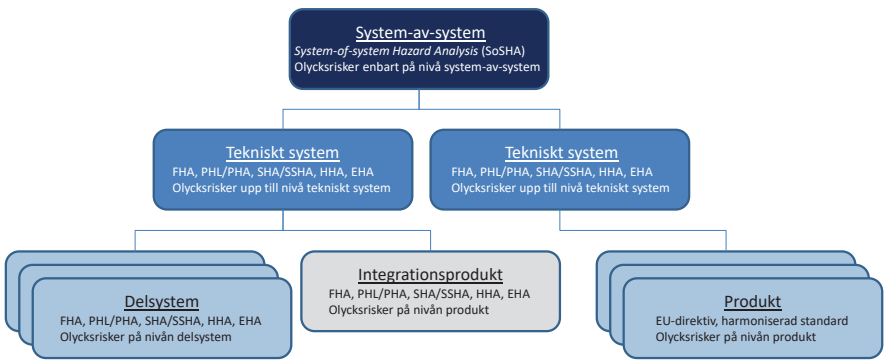


Bild 10.1 *System-av-system kan bestå av valfria kombinationer av tekniska system, delsystem, produkter och integrationsprodukter.*

I arkitekturen för systemlösningen kan det även ingå särskilda systemelement (delsystem, produkter eller integrationsprodukter) som ur systemsäkerhetsperspektiv kan hanteras på olika sätt.

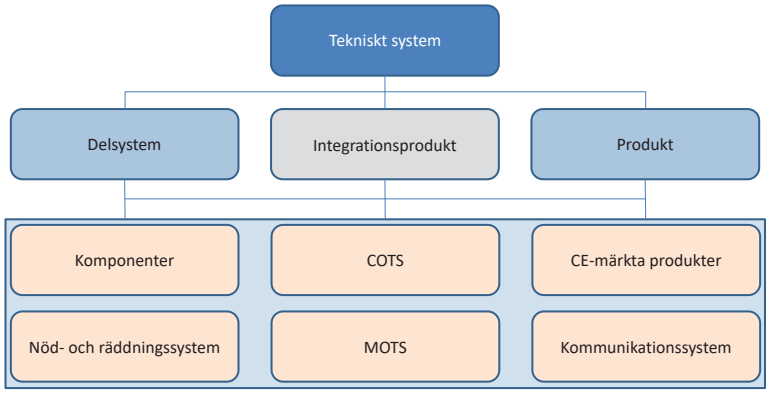


Bild 10.2 Exempel på systemelement som kan hanteras i särskild ordning.

10.4 Olika kategorier av systemelement

Nedan presenteras olika kategorier av systemelement för uppbyggnad av system-av-system, tekniska system och produkter. För var och en av dessa kategorier ges inriktning för systemsäkerhetsarbetet och hur man kan resonera kring dessa.

10.4.1 Standardprodukter för övrig verksamhet

Standardprodukter som anskaffas för *övrig verksamhet* såsom kontor, skol- och matsalar samt andra typer av personalutrymmen och som där används i enlighet med tillverkarens bruksanvisning kan tas i bruk utan genomförande av systemsäkerhetsarbete eller systemsäkerhetsbeslut. Motsvarande gäller för produkter utan undantag för militär materiel, som används vid exempelvis verkstäder och hangarer.

Notera dock att all form av samfunktion i annat tekniskt system som ligger utanför tillverkarens bruksanvisning behöver analyseras ur ett systemsäkerhetsperspektiv.

10.4.2 Reservmateriel

Produkter (reservmateriel, utbytesenheter) som återanskaffas kräver normalt inget förnyat systemsäkerhetsarbete såvida produkten inte är modifierad eller att andra krav på omgivningsmiljö anges.

10.4.3 Komponenter

Till denna kategori hör komponenter av civilt eller militärt ursprung. Dessa komponenter har ingen egen funktion och får anpassas för att kunna monteras. Komponenterna är tänkta att kopplas samman på en bestämd plats, ofta i en plattform för att uppfylla ett speciellt ändamål, men utan avsikt att driftsättas som en enda funktionell enhet. Komponenterna (var för sig eller i grupp) kan således inte användas eller fungera fristående och dessa kräver inget systemsäkerhetsarbete eller systemsäkerhetsbeslut.

Exempel på komponenter kan vara rack för radioapparater, kabelrännor och hållare för lös utrustning, men inkluderar även ”metervara” som anpassas, exempelvis vajer, rör och elkabel.

10.4.4 Produkter med eller utan en primär riskkälla

Till denna kategori av materiel hör enkla produkter (triviala) som inte kan hänföras till de tidigare presenterade kategorierna. Produkterna kan ha en enda primär riskkälla som därmed är enkla att förstå med avseende på systemsäkerhet, alternativt är det produkter som saknar specifika riskkällor.

Det är tillverkarens (eller importörens) ansvar att tillse att produkten uppfyller svensk lagstiftning och får släppas ut på marknaden. Produkterna är tänkta att användas fristående eller tillsammans med andra produkter utifrån tillverkarens bruksanvisning. Den avsedda användningen inom Försvarsmakten ska inte skilja sig nämnvärt mot civil användning.

Om tekniska standarder för konstruktion och verifiering saknas så behöver ett mindre omfattande, men väl avvägt systemsäkerhetsarbete genomföras. I vissa fall kan *beställaren* redan i *Förfrågningsunderlaget* (RFP) ange vilka olycksrisker som tillverkaren ska analysera och för dessa redovisa vilka riskreducerande åtgärder som vidtagits.

För kemiska produkter räcker det med ett säkerhetsdatablad.

Exempel på materiel med eller utan en primär riskkälla är persedlar till soldatsystemet, termos och målarfärg.

10.4.5 COTS-produkter

Till COTS-produkter *(Commercial off the shelf)* hör produkter som redan finns på marknaden och som kan vara godkända av ackrediterat organ mot internationella standarder.

Det är tillverkarens (eller importörens) ansvar att tillse att COTS-produkten uppfyller svensk lagstiftning och därmed får släppas ut på marknaden. I denna kategori återfinns produkter som åsatts olika märkningar, exempelvis rattmärkning av marina utrustningar. En mycket stor del utgörs dock av CE-märkta produkter, vilka behandlas i egna avsnitt.

Produkten är tänkt att användas fristående eller tillsammans med andra produkter utifrån tillverkarens anvisningar. Om den avsedda användningen inom Försvarsmakten avviker från tillverkarens anvisningar behöver användningen genomgå ett särskilt systemsäkerhetsarbete.

Produkten får inte ändras (modifieras). Om produkten ändras (modifieras) så att den inte längre uppfyller de grundläggande kraven, upphör tillverkarens produktsäkerhets- och produktansvar och intyget/märkningen (om tillämplig) från ackrediterat/Anmält organ är därmed inte längre giltig.

Om produkten stämmer in på ovan nämnda beskrivning kan systemsäkerhetsarbetet reduceras till att kontrollera att det ackrediterade organet, om sådant har deltagit i bedömning av överensstämmelse, är behörigt för godkännande (certifiering) av aktuell produkt samt att den tänkta användningen inom Försvarsmakten ryms inom godkännandet, tillverkarens anvisningar och eventuell märkning.

Exempel på COTS-produkter är rattmärkta produkter, helbilsgodkännande av vägfordon och CIP-märkt ammunition (jakt och sportskytte).

10.4.6 Nöd- eller räddningssystem

Till denna kategori hör säkerhetsprodukter och säkerhetssystem som används i nöd- eller räddningssituationer. Dessa kan vara ständigt aktiva (övervakning sker med sensorer och aktiveras automatiskt) eller passiva (aktiveras av användaren).

Ett nöd- eller räddningssystem kan innehålla eller generera stora energier och kan därmed vara relativt farlig för användaren om de inte används eller hanteras

på ett korrekt sätt. Systemsäkerhetsarbetet behöver visa att ett nöd- eller räddningssystems nytta alltid är större än de konsekvenser som kan uppstå vid användning, felfunktion eller vid vådautlösning. För nöd- eller räddningssystem kan under vissa förutsättningar, såsom tillgänglighet och prestanda, en mildare tolerabel risknivå accepteras än för den aktuella plattformen.

Säkerhetsprodukters utformning och prestanda styrs ofta av regelverk. Exempelvis får ett säkerhetsbälte eller en krockkudde orsaka viss skada (hörselskada, slag mm) när de aktiveras eftersom dess nytta med att rädda liv eller undvika allvarliga personskador väger tyngre än hörselnedsättning och blåmärken.

En flytväst ska ha vissa egenskaper oavsett i vilket tekniskt system den ingår. Antalet flytvästar ombord på ett fartyg eller i en luftfarkost styrs av internationella regelverk och påverkar därför inte plattformens säkerhetsarkitektur. Att tillföra dubbelt så många flytvästar gör inte att en sämre sjövärdighet hos fartyget kan accepteras. Att installera ett effektivt brandsläckningssystem gör heller inte att man kan tillåta fler bränder.

Exempel på nöd- eller räddningssystem är handbrandsläckare, brandsläckningssystem, flytväst, livbåt, krockkudde, bältessträckare och bältesskärare.

10.4.7 CE-märkta produkter

Till CE-märkta produkter hör tekniska system och produkter som dels redan är släppta på marknaden, dels ännu inte är släppta på marknaden och där Försvarsmakten blir den förste brukaren. Den CE-märkta produkten används oftast fristående, vilket innebär att tillverkarens bruksanvisning följs avseende fastsättning, installation, kraftförsörjning och inkoppling till olika teknik- och informationssystem.

10.4.7.1 Produkten är släppt på marknaden redo att tas i bruk

Om produkten är släppt på marknaden och redo att tas i bruk är det tillverkarens (eller importörens) ansvar att tillse att den CE-märkta produkten uppfyller gällande lagstiftning och är korrekt CE-märkt för att tas i bruk i Sverige.

Den tänkta användningen inom Försvarsmakten får inte skilja sig från tillverkarens angivna (avsedda) användningssätt. Produkten får heller inte ändras (modifieras). Om produkten ändras (modifieras) så att den inte längre uppfyller de grundläggande kraven eller om dess bruksanvisning ändras, upphör den

legala tillverkarens produktsäkerhets- och produktansvar och CE-märkningen är därmed inte längre giltig.

Om produkten är CE-märkt enligt ovan kan systemsäkerhetsarbetet reduceras till att kontrollera att Försäkran om överensstämmelse *(Declaration of Conformity, DoC)* är komplett samt att EU-direktiv och harmoniserade standarder finns angiva och är tillämpliga för produkten. *Beställaren* kan behöva efterfråga vilka kravnivåer som har använts i standarderna och granska att dessa är tillräckliga för anskaffad produkt, exempelvis avseende EMC-krav.

Vidare kontrolleras att svensk bruksanvisning inklusive CE-märkning och eventuell annan märkning finns samt att den tänkta användningen inom Försvarsmakten ryms inom CE-märkningen.

Om det för den CE-märkta produkten krävs en registrering eller certifikat (även andra begrepp kan förekomma) från ett tredjepartsorgan, exempelvis ett Anmält organ, granskas att den som utfärdat certifikatet är behörig för aktuell produktkategori och använda testmetoder för verifiering samt att den CE-märkta produkten omfattas av certifikatet. Vidare bör granskning ske av vilka harmoniserade standarder som tillverkaren respektive tredjepartsorganet har tillämpat vid verifieringen och om dessa bedöms vara tillämpliga för ändamålet.

I de fallen andra standarder, enbart delar av harmoniserade standarder eller upphävda harmoniserade standarder har tillämpats (ty presumtion inte längre finns), bör granskningen omfatta hur tillverkaren har uppfyllt motsvarande grundläggande säkerhetskrav i EU-direktiven. I vissa fall kan det vara önskvärt att även ta del av utförd riskanalys som ligger till grund för CE-märkningen.

Utöver svensk bruksanvisning och Försäkran om överensstämmelse *(Declaration of Conformity, DoC*), ska det genom en beständig märkning (skylt, gravering, ingjutning) på produkten gå att identifiera tillverkare, importör, adress, typbeteckning samt vid behov individmärkning.

Tillverkarens Försäkran om överensstämmelse *(DoC)* med referenser till EU-direktiv, standarder och om möjligt delar av teknisk dokumentation *(Technical file)*, ska biläggas systemsäkerhetsbesluten.

Exempel på redan CE-märkta produkter är arbetsmaskiner, elverk, tryckkärl, bakgavellyft, lyftdon, gummibåtar, snöskoter och telekom-utrustning.

10.4.7.2 Produkten är ännu inte släppt på marknaden

Om produkten ännu inte är släppt på marknaden och Försvarsmakten blir den förste brukaren kan kontraktskrav ställas på insyn i tillverkarens systemsäkerhetsarbete och hur det ska genomföras. Det är dock tillverkarens (eller importörens) ansvar att tillse att den CE-märkta produkten uppfyller gällande lagstiftning och är korrekt CE-märkt för att tas i bruk i Sverige.

Systemsäkerhetsarbetet, inklusive CE-märkningen, ska utgå ifrån Försvarsmaktens ställda krav på användningsmiljö och operationsbetingelser (inklusive tekniska prestanda). De militära standarderna och de viktigaste harmoniserade standarderna som ska tillämpas anges i *Förfrågningsunderlaget* (RFP).

Produkten ska CE-märkas enligt alla tillämpliga EU-direktiv och det görs innan leverans till Försvarsmakten eller FMV. Om Försvarsmakten har krav utöver EU-direktivens minimikrav vad gäller grundläggande hälsa och säkerhet, ska dessa framgå av *Förfrågningsunderlaget* (RFP) och ingå i CE-märkningen. *Beställaren* kan begära att dessa krav dessutom ska verifieras separat och redovisas i en provrapport eller i en *Systemsäkerhetsrapport* (SAR). *Beställaren* kontrollerar att ställda krav är uppfyllda.

EU-direktiv kan kräva att produkten och/eller tillverkarens kvalitetssystem behöver ett godkännande/certifikat från ett Anmält organ.

I de fallen EU-direktiven medger frihet att anlita ett tredjepartsorgan eller laboratorium behöver eventuella krav på detta framgå av *Förfrågningsunderlaget* (RFP). Ett sådant organ ska vara ackrediterat för aktuell produktkategori och för testmetoder för verifiering.

Produkten ska uppfylla harmoniserade standarder som ger presumtion med krav i EU-direktiven. I de fallen delar av harmoniserade standarder, eller exempelvis militära standarder används, ska tillverkaren särskilt redovisa hur EU-direktivens krav omhändertagits. I de fallen tillämpliga standarder saknas kan man vara tvungen att kombinera krav från olika standarder.

Beställaren kan ange att vissa militära standarder ska följas. Dessa standarder har ofta högre eller mycket högre krav på säkerhet och skydd jämfört med motsvarande harmoniserade standarder. *Konstruktören* behöver jämföra kraven, och eventuella skillnader i kravnivå, mellan standarderna och bedöma om kraven

i de harmoniserade standarderna är uppfyllda eller om kompletterande provning och verifiering erfordras. Att kraven i de harmoniserade standarderna därigenom anses vara uppfyllda ska redovisas som en del av den tekniska dokumentationen (*Technical file*).

Utöver svensk bruksanvisning och Försäkran om överensstämmelse *(Declaration of Conformity, DoC)*, ska det genom en beständig märkning (skylt, gravering, ingjutning) på produkten gå att identifiera tillverkare, importör, adress, typbeteckning samt vid behov individmärkning.

Tillverkarens Försäkran om överensstämmelse *(DoC)* med referenser till EU-direktiv, standarder och teknisk dokumentation *(Technical file)* ska biläggas systemsäkerhetsbesluten.

Exempel på produkter som blivit CE-märkta med Försvarsmakten som förste brukare är funktionscontainrar.

10.4.8 Produkter som genomgår en CE-liknande process

De fåtal tekniska system och produkter som är undantagna CE-märkning från ett visst EU-direktiv kan istället för detta EU-direktiv genomgå en *CE-liknande process.* Notera dock att vissa EU-direktiv inte medger några undantag från CE-märkning.

Produkter som exempelvis har anskaffats från en annan stat och som faller under säkerhetsskyddsklassificerade uppgifter (försvarssekretess) kan medföra att CE-märkning inte kan eller får genomföras, exempelvis för en signalskyddsenhet. Ofta uppfyller dock sådana produkter redan strängare krav utifrån militära standarder.

Maskiner som är *särskilt konstruerade och tillverkade för militärt ändamål* är undantagna från CE-märkning och ska (får) inte CE-märkas enligt aktuellt EU-direktiv för maskiner. Andra EU-direktiv kan dock vara tillämpliga parallellt och ändå kräva CE-märkning, exempelvis EMC-direktivet. Ett fåtal ytterligare undantag kan finnas i andra EU-direktiv, men de är definierade på andra sätt. Notera dock om produkten (eller en liknande produkt) kan ha dubbla användningsområden (dual use), det vill säga kan användas både civilt respektive militärt, så kan militärt undantag inte åberopas utan produkten ska CE-märkas.

Den *CE-liknande processen* innebär att samma process och krav gäller som vid CE-märkning av produkter enligt ett visst EU-direktiv. Skillnaden är att den produkt som följer den *CE-liknande processen* inte ska (får) CE-märkas för just detta EU-direktiv. För särskilt riskfyllda produkter finns heller inte något certifikat utfärdat av Anmält organ. Produkten kan däremot behöva CE-märkas enligt andra EU-direktiv.

Beställaren bör i *Förfrågningsunderlaget* (RFP) ställa krav på att vissa metoder och standarder, inklusive harmoniserade standarder, ska följas. Eventuella krav på användning av tredjepartsorgan (ackrediterat certifieringsorgan eller laboratorium, dock inte Anmält organ) ska särskilt anges. *Beställaren* kan även ange att vissa militära standarder ska följas.

Exempel på produkter där CE-liknande process kan tillämpas är på MOTS, radioutrustning som uteslutande används av Försvarsmakten och för vissa påbyggnader på vägfordon.

Tillverkaren äger inte rätt att modifiera en produkt enbart för att undvika CE-märkning.

10.4.9 Integrationsprodukter

Till denna kategori av materiel hör civila och militära produkter. Dessa produkter kan integreras i andra tekniska system, ofta plattformar, eller kan användas fristående. För integrationsprodukter genomförs ett systemsäkerhetsarbete och systemsäkerhetsbeslut utfärdas.

Ammunition är alltid att betrakta som ett fristående tekniskt system samtidigt som den ofta utgör integrationsprodukt i ett eller flera tekniska system. För ammunition ska alltid systemsäkerhetsbeslut utfärdas.

Exempel på integrationsprodukter kan vara ammunition, vapenstationer, BT-46, justerbart schaktblad till arbetsmaskin och CE-märkta spänningsaggregat.

10.4.10 Delvist nyutvecklade tekniska system

Ett delvist nyutvecklat tekniskt system kan kännetecknas av att befintliga kända delsystem och produkter sätts samman till ett nytt tekniskt system. Alternativt kan en känd grundkonstruktion vidareutvecklas med annan alternativt med

ytterligare funktionalitet eller ändrad prestanda. Således finns kunskap och erfarenhet av delsystem och grundkonstruktion.

Tidigare systemsäkerhetsarbete och erfarenheter från användning och underhåll kan åberopas, men behöver omprövas utifrån det nya användningssättet och de nu ställda kraven på systemsäkerhet. Drifterfarenheter kan visa på svagheter i konstruktion och eventuella säkerhetsbrister som behöver omhändertas i det nya tekniska systemet.

Om äldre delsystem eller grundkonstruktion används kan dokumentation och tidigare systemsäkerhetsarbete saknas eller vara ofullständigt för det nya användningssättet. I dessa fall räcker det inte med att enbart analysera integrationen med andra delsystem. Systemsäkerhetsarbete kan behöva genomföras separat för de äldre delsystemen eller grundkonstruktionen innan integrationen till det nya tekniska systemet analyseras.

För det delvist nyutvecklade tekniska systemet ska lagstiftningen uppfyllas, men undantag för militär materiel kan tillämpas. För delsystem och grundkonstruktion finns normalt standarder och *Designregler* (DR) att följa. Systemsäkerhetsarbetet ska dels omfatta integrationen mellan de olika delsystemen, dels den nya funktionaliteten och ändrade prestandan. Därför kan ett mer omfattande, men ändå ett väl avvägt systemsäkerhetsarbete behöva genomföras på det nya kompletta tekniska systemet.

Exempel på delvist nyutvecklat tekniskt system är Granatkastarpansarbandvagn 90 (GRKPBV90).

10.4.11 Nyutvecklade tekniska system

Ett helt nyutvecklat tekniskt system föregås ofta av både Forskning och teknikutveckling (FoT) och konceptarbete då nya tekniska lösningar till tekniska system eller delsystem behöver utvecklas.

Lagstiftningen ska uppfyllas, men undantag för militär materiel får tillämpas. Tekniska standarder och *Designregler* (DR) kan saknas eller inte fullt ut vara tillämpbara. Därför kan ett mer omfattande systemsäkerhetsarbete behöva genomföras.

Exempel på nyutvecklat tekniskt system är ubåt (typ Blekinge).

10.4.12 System-av-system

Med system-av-system avses tekniska system och produkter som var för sig redan har egna systemsäkerhetsbeslut utfärdade, men som i gemensamt uppträdande skapar nya förmågor och funktioner. Med detta förstås att inget av de tekniska systemen integreras i det andra systemet, utan att de enbart samverkar.

I ett system-av-system uppnås funktion exempelvis genom att tillgänglig information delas eller överförs från ett system till ett annat. Dessa gemensamma informationstillgångar har påverkan på systemsäkerheten för det samverkande systemet-av-system då de påverkar det system som innehåller riskkällorna. Informationens integritet och korrekthet medför att kravställning måste hantera krav på viss kritikalitetsnivå i de ingående delsystemen. Om de systemsäkerhetskritiska informationstillgångarna inte kan hållas separerade från övrig funktionalitet medför detta krav på en gemensam kravställning avseende kritikalitetsnivå på alla ingående delsystem i det nya systemet-av-system.

I systemsäkerhetsarbetet för system-av-system måste de kritiska informationstillgångarna identifieras så att fel i dessa inte leder till en vådahändelse i det delsystem som utgör den verkställande delen.

Systemsäkerhetsbesluten för system-av-system ska omfatta de nya olycksriskerna som uppkommer i det gemensamma uppträdandet. De ingående systemen kan behöva konstrueras om för att hantera olycksrisker som uppstår då systemen samverkar.

Exempel på system-av-system kan vara att en helikopter ska kunna landa på ett fartyg eller att en plattform kan agera eldledningsplats och lämna information till ett skjutande förband.

Ett annat exempel är ledningssystem som ska förmedla elduppdrag till olika pjäsgrupperingar över ett stort grupperingsområde där både position för skyddsobjekt och mål samt tid för gemensam insats blir systemsäkerhetskritiska informationstillgångar.

10.4.13 Kommunikationssystem

Till denna kategori hör system där sammanlänkade produkter endast överför information i form av talade eller skriftliga meddelanden mellan människor, utan att informationen i sin tur överförs eller används i ett annat tekniskt system, exempelvis för att styra farliga energier såsom vapen eller autonoma system.

Kommunikationssystem som används för att styra eller påverka säkerhetskritiska tekniska system tillhör kategorin system-av-system.

Det sammansatta systemet består systemsäkerhetsmässigt av relativt enkla produkter. Produkterna kan vara godkända av annan stat (MOTS), part (ackrediterat organ mot internationella standarder) eller CE-märkta av tillverkaren. Det kan även ingå produkter (COTS) som ur funktionell synvinkel saknar specifik riskkälla, exempelvis kablage, kontaktdon och hållare.

Kommunikationssystem kan ur ett informationssäkerhetsperspektiv vara ett komplext integrerat system och utgöras av en mängd olika produkter, exempelvis datorer, bildskärmar, högtalare och skrivare. Samma system kan ur ett systemsäkerhetsperspektiv anses vara trivialt där produkterna är utan inbördes systemsäkerhetspåverkan. Det sammanlänkade systemet kan ur ett systemsäkerhetsperspektiv betraktas som ofarligt, men kan samtidig ur ett informationssäkerhetsperspektiv (security) behöva hanteras som ett kritiskt system.

För kommunikationssystem som används för att varna andra, exempelvis ombord på ett fartyg, så kommer dess tillförlitlighet att vara säkerhetskritisk då utebliven funktion i förlängningen kan leda till allvarliga konsekvenser, exempelvis om personal inte utrymmer vissa platser vid brand. Sådana olycksrisker hanteras i kategorin system-av-system.

Olycksrisker som finns i de fristående MOTS, COTS och CE-märkta produkterna för kommunikation omhändertas på produktnivå enligt någon av kategorierna ovan. Dessa olycksrisker ska således inte eskaleras till kategorin kommunikationssystem.

Exempel på kommunikationssystem är radio eller ledningsbundet system för tal eller textmeddelanden.

10.4.14 MOTS-produkter

Till MOTS-produkter *(Military off the shelf)* hör tekniska system, produkter och reservmateriel framtagna för särskilt militärt ändamål. Dessa är tagna i bruk hos minst en stat och kan därmed finnas tillgängliga för försvarsmyndigheter.

För MOTS-produkter där kontrakt tecknas mellan stater, exempelvis *Foreign Military Sales* (FMS), eller mellan försvarsmyndighet och annan organisation, exempelvis *NATO Support and Procurement Agency* (NSPA), gäller särskilda villkor. Försvarsmakten eller FMV i rollen som *beställare* ska säkerställa att MOTS-produkten uppfyller svensk lagstiftning och därmed kan släppas ut på marknaden för att tas i bruk vid Försvarsmakten.

För MOTS-produkter där kontrakt tecknats mellan stater får den avsedda användningen av MOTS-produkten inom Försvarsmakten inte skilja sig mot den utländska försvarsmyndighetens anvisningar. MOTS-produkten får heller inte ändras (modifieras). Om MOTS-produkten ändras (modifieras) eller används på annat sätt än enligt den utländska försvarsmyndighetens eller tidigare köpares anvisningar, kan deras godkännande upphöra att gälla.

För MOTS-produkter där kontrakt tecknats mellan stater kan systemsäkerhetsarbetet reduceras till att kontrollera att svensk lagstiftning är uppfylld samt att avsedd användning ryms inom godkännandet och är i enlighet med den utländska försvarsmyndighetens anvisningar. Vidare bör kontakt tas med stater som använder MOTS-produkten. Dessa stater har redan granskat och godkänt MOTS-produkten samt har drifterfarenheter. Spårbara och trovärdiga drifterfarenheter kan utvärderas och åberopas i systemsäkerhetsbesluten.

Exempel på MOTS-produkter är Terrängbil 16 (kontrakt med tillverkare), Helikopter 16 (FMS) och maskeringsnät (NSPA).

Den som anskaffar en MOTS-produkt måste fullt ut analysera innebörden och omfattningen av de godkännanden som erhålls från annan stat.

10.4.15 Utbildningssystem och utbildningsmateriel

De flesta tekniska system och produkter används vid både utbildning, övning och insats. Dock kan farliga komponenter bytas mot mindre farliga i de skarpa systemen under utbildning och övning för att minska konsekvenserna om en olycka ändå skulle inträffa. Exempelvis kan lös eller blind ammunition användas i ett vapen.

Utbildningssystem och utbildningsmateriel som anskaffas för att enbart användas vid utbildning och övning ska normalt uppfylla lagstiftningen utan undantag för militär materiel. Detta eftersom denna materiel inte är avsedd för visst militärt ändamål och därmed inte har någon förstörelsebringande effekt. Utbildningssystem och utbildningsmateriel kan hänföras till flera av kategorierna ovan såsom CE-märkt produkt eller MOTS.

Utbildningssystem och utbildningsmateriel kan dock behöva utvärderas individuellt från fall till fall om eventuella undantag för militär materiel behöver användas.

Utbildningssystem och utbildningsmateriel ska normalt uppfylla lagstiftningen utan undantag för militär materiel.

Om syftet med utbildningen är att lära ut ett korrekt handhavande behöver utbildningssystemet eller utbildningsmaterielen och det skarpa systemet till fullo överensstämma. I systemsäkerhetsarbetet behöver olycksrisker som uppstår vid användning av det skarpa systemet till följd av att utbildningssystemet avviker från det skarpa systemet i något sammanhang hanteras. Dessa olycksrisker kan uppstå då användaren, som genomfört sin utbildning med utbildningssystemet, handhar det skarpa systemet på samma invanda och potentiellt felaktiga sätt, vilket kan leda till olyckor. Skillnader mellan utbildningssystem och utbildningsmateriel och det skarpa systemet betraktas som potentiella bidragande orsaker till olyckor. Detta måste alltid utredas av *beställaren* av utbildningsmaterielen.

Om syftet med utbildningen är att lära ut taktiskt uppträdande eller data, konstruktion och funktion så behöver inte utbildningsmaterielen ur ett systemsäkerhetsperspektiv spegla det verkliga tekniska systemet rent handhavandemässigt. Det ska för användaren som genomför utbildningen dock

inte råda några tvivel om att utbildningsmaterielen rent handhavandemässigt inte fullt ut speglar det skarpa systemet. Sådan utbildningsmateriel bedöms inte medföra några olycksrisker i det skarpa systemet till följd av felinlärt handhavande.

Om syftet innefattar någon form av övning i handhavande kan utbildningssystem och utbildningsmateriel delas in i olika kategorier. För var och en av kategorierna föreslås omfattningen av systemsäkerhetsverksamhet som erfordras för systemet:

Typ av utbildningssystem eller utbildningsmateriel	Erforderligt systemsäkerhetsarbete	Exempel på utbildningsmateriel
Utbildningsmaterielen består av det skarpa systemet och används i samma användningsmiljö som det skarpa, men användningen är anpassad för utbildning.	Systemsäkerhetsanalys genomförs enligt Försvarsmaktens ställda krav. Olycksrisker förknippade med inlärningsfel till följd av eventuella avvikelser från ett skarpt system ska identifieras och bedömas i systemsäkerhetsarbetet.	Vapen med blind, lös eller övningsammunition. CBRN-materiel med alternativa eller utspädda verksamma ämnen (agenser).
Utbildningsmateriel används i annan användningsmiljö men innehåller samma funktioner och omfattas av eller kontrollerar samma energier som den skarpa motsvarigheten.	Uppfyllande av lagstiftning genom CE-märkning. Utöver lagstiftningen krävs en inledande bedömning och dokumentation avseende eventuella olycksrisker förknippade med inlärningsfel till följd av avvikelser från det skarpa systemets operatörsmiljö. Om sådana olycksrisker identifieras ska dessa hanteras i enlighet med systemsäkerhetsmetodiken.	Dykkammare Elektrisk broläggare

Typ av utbildningssystem eller utbildningsmateriel	Erforderligt systemsäkerhetsarbete	Exempel på utbildningsmateriel
Utbildningsmaterielen används i annan användningsmiljö och innehåller endast simulerade funktioner motsvarande de som finns i det skarpa systemet. Skillnad från det skarpa systemet är att energin inte genereras av funktionen. Systemet kan dock generera viss energi för att efterlikna det skarpa systemet.	Uppfyllande av lagstiftning genom CE-märkning. Utöver lagstiftningen krävs en inledande bedömning och dokumentation avseende eventuella olycksrisker förknippade med inlärningsfel till följd av avvikelser från det skarpa systemets operatörsmiljö. Om sådana olycksrisker identifieras ska dessa hanteras i enlighet med systemsäkerhetsmetodiken.	Körutbildningssimulator G-kraftscentrifug Simulatorer av operatörssystem Docka för hjärt-lungräddning Ammunitionseffekter som simulerar skarpa explosioner Målbogseringsutrustning
Specialfall, utbildningsmaterielen stämmer inte in på någon av ovanstående beskrivningar eller är en kombination av dessa.	Uppfyllande av lagstiftning. Systemsäkerhetsanalys genomförs enligt Försvarsmakten ställda krav. Olycksrisker förknippade med inlärningsfel till följd av avvikelser från skarpt system ska bedömas i systemsäkerhetsarbetet.	Strid i bebyggelse Inomhusträningsanläggning för CBRN

Tabell 1.1 Exempel på indelning av utbildningssystem och utbildningsmateriel.

De eventuella skillnaderna mellan utbildningssystem och utbildningsmateriel och det skarpa systemet behöver beaktas i systemsäkerhetsarbetet.

10.5 Tillhandahållen materiel till utvecklande industri

Med tillhandahållen materiel (*Government Furnished Equipment*, *GFE*) avses produkter som redan finns i Försvarsmaktens förvaltningssystem eller på annat sätt tillhandahålls av Försvarsmakten eller FMV. Det kan vara mängdmateriel såsom spadar, yxor och spett, men även specifika delsystem, exempelvis apparater och andra anordningar för montering och integration.

Konstruktören ansvarar för integration och funktionen mellan tillhandahållen materiel och det tekniska systemet. *Konstruktören* bör även ansvara för att det tekniska systemet tillsammans med den tillhandahållna materielen är säker att använda. Notera att i de fallen *konstruktören* inte ansvarar för helheten (tekniskt system inklusive tillhandahållen materiel) blir *beställaren* integrationsansvarig ur ett systemsäkerhetsperspektiv.

Beställare som lånar ut materiel, skarp eller attrapper, till *konstruktören* ansvarar även för att överlämna erforderlig systemsäkerhetsdokumentation för materielen.

11 Vägvalsmodellen

Syftet med detta kapitel är att förklara Vägvalsmodellen (VVM) samt att beskriva hur krav på betryggande säkerhet och acceptanskriterier kan ställas med stöd av denna.

11.1 Beskrivning av Vägvalsmodellen

Vägvalsmodellen (VVM) är en iterativ metod som både kan användas vid anskaffning och vid ändring (modifiering) av tekniska system och produkter. Den används vid kravställning för att tillåta, inrikta och begränsa olika vägval. Under konstruktions- och integrationsarbete prövas de tillåtna vägvalen avseende möjligheterna att uppfylla acceptanskriterier för dessa. Under systemsäkerhetsvärderingen verifieras argument och belägg för att bekräfta att ställda systemsäkerhetskrav är uppfyllda.

Första tillfället när *Vägvalsmodellen* (VVM) används är när Försvarsmakten påbörjar arbetet med *Systemmålsättning* (SMS). *Vägvalsmodellen* (VVM) tillämpas av respektive aktör under de olika livscykelskedena.

Vägvalsmodellen (VVM) tillämpas för all materiel med eller utan undantag för militär materiel. Den visar även hur man för militär materiel kan gå tillväga för att tillgodoräkna sig uppfyllande av lagstiftning, standarder och *Designregler* (DR) samt godkännanden av annan part eller stat.

Vägvalsmodellen (VVM) tillämpas på såväl tekniska system, delsystem och produkter som för enskilda olycksrisker. Detta kan exempelvis ske genom ett helbilsgodkännande (CoC) för en lastbil (tekniskt system) eller genom en Försäkran om överensstämmelse (DoC) för ett CE-märkt tryckkärl (komponent) integrerat i ett tekniskt system. Vidare kan enskilda olycksrisker hanteras såsom eldrörssprängning (brister i tekniken) eller felriktning av vapen (mänskligt felhandlande).

Det tekniska systemet behöver brytas ned till en ändamålsenlig systemstruktur med en tillräcklig detaljeringsgrad för att kunna tillämpa de olika vägvalen.

Vägvalsmodellen (VVM) tillämpas på såväl tekniska system och komponenter som för enskilda olycksrisker.

Vägvalsmodellen (VVM) omfattar följande vägval (VV):

- Vägval 1 – Författningsenliga krav
- Vägval 2 – Godkänd av annan stat
- Vägval 3 – Godkänd av annan part
- Vägval 4 – Övriga standarder
- Vägval 5 – Designregler
- Vägval 6 – Beprövat system
- Vägval 7 – Riskmatriser

Vägvalen prövas normalt i nummerordning, dvs VV1 före VV2, före VV3. Ibland kan en kombination av vägval bli nödvändig, exempelvis VV1, VV4 och VV5 för att tillsammans kunna visa på betryggande säkerhet. För olycksrisker som inte har kunnat hanteras i tidigare vägval tillämpas vägval (VV7).

Om undantag för militär materiel nyttjas, kan fler vägval i *Vägvalsmodellen* (VVM) behövas för att kunna påvisa betryggande säkerhet.

Vägval (VV1) tillämpas alltid eftersom de författningsenliga kraven alltid ska uppfyllas. I vägval (VV1) ingår exempelvis CE-märkning. Om vägval (VV1) inte är tillräckligt för att uppnå betryggande säkerhet för det tekniska systemet eller produkten går man vidare till vägval (VV2 – VV6). Om det finns olycksrisker som inte har kunnat omhändertas i dessa vägval går man vidare till vägval (VV7) med bedömning mot riskmatriser.

Systemsäkerhetsvärderingen utgör det samlade resultatet och består av argument och belägg från de olika vägvalen och som tillsammans med ett ställningstagande redovisas i aktuellt systemsäkerhetsbeslut.

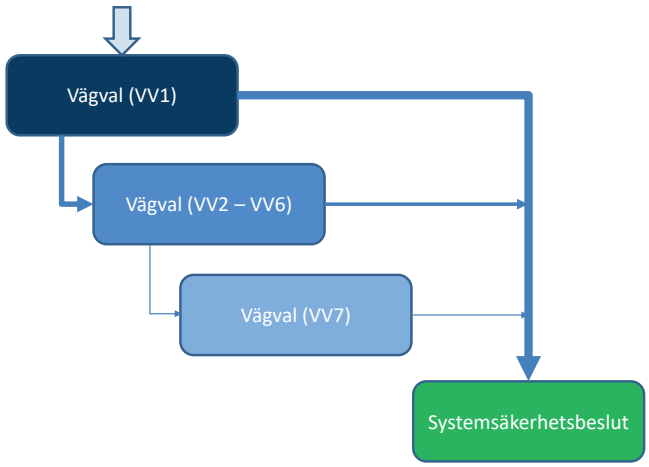


Bild 11.1 Principiell tillämpning av Vägvalsmodellen (VVM).

11.2 Beskrivning av de olika Vägvalen

Syftet med avsnittet är att utifrån de olika vägvalen beskriva hur dessa kan tillämpas vid kravställning i *Systemmålsättning* (SMS) och *Förfrågningsunderlag* (RFP).

I *Systemmålsättningen* (SMS) anges inriktning och acceptanskriterier för tillåtna vägval. I *Förfrågningsunderlaget* (RFP) preciseras krav och acceptanskriterier för de olika vägvalen.

11.2.1 Vägval 1 – Författningsenliga krav

Syftet med Vägval (VV1) är att säkerställa att tekniska system och produkter kan uppfylla de författningsenliga kraven.

Med författningsenliga krav avses EU-rätt och svensk lagstiftning med sina förordningar och föreskrifter. Hit räknas även de harmoniserade standarderna som, när deras mer detaljerade krav uppfylls, presumeras uppfylla författningarnas motsvarande krav.

Att konstruera en produkt direkt mot de grundläggande kraven i ett EU-direktiv är mycket krävande och går i praktiken inte att genomföra då kraven är för generella. Ur systemsäkerhetsperspektiv räknas EU-direktivens harmoniserade standarder därför som viktiga och i princip helt nödvändiga att följa. I de fallen harmoniserade standarder saknas kan andra etablerade internationella standarder användas, dock (nota bene) utan att presumtionsprincipen kan tillämpas.

I vissa författningar finns *Allmänna råd* (AR) hur något kan eller bör utföras. Dessa är dock inte tvingande men anger lämpligt arbetssätt eller tolkning.

Vägval (VV1) handlar om att öppna för, alternativt bestämma, om det tekniska systemet eller produkten ska vara:

- Militär materiel (MOTS)
- Materiel med civil eller militär bakgrund utan undantag för viss militär materiel
- Materiel med civil eller militär bakgrund med undantag för viss militär materiel

Det tänkta tekniska systemet eller produkten måste falla inom ramen för aktuell lagstiftning. Detta gäller även för militär materiel.

För viss materiel, såsom vägfordon särskilt konstruerade och tillverkade för visst militärt ändamål, har Försvarsmakten föreskriftsrätt inom det utrymme lagen ger. För andra tekniska system och produkter, exempelvis för maskiner, har Försvarsmakten tolkningsföreträde huruvida dessa kan betraktas som *militär materiel* eller *militär materiel som är särskilt konstruerade och tillverkade för visst militärt ändamål*. Om Försvarsmakten inte använder sitt tolkningsföreträde så anskaffas i första hand materiel utan militära undantag.

Försvarsmakten har tolkningsföreträde avseende möjligheten att nyttja undantag i lagstiftningen för militär materiel respektive för materiel som är särskilt konstruerad och tillverkad för visst militärt ändamål. *Beställaren* har alltid bättre rätt än *konstruktören* att tolka lagstiftningen

För många tekniska system och produkter kan de civila författningskraven på säkerhet och skydd anses tillräckliga om avsedd användning ryms inom till-

verkarens bruksanvisningar och underhållsföreskrifter. Detta kan även gälla för delsystem och komponenter som senare sätts samman till militär materiel. Exempelvis kan hela, eller delar av, det tekniska systemet omfattas av krav på CE-märkning, såsom EU-direktiven för elektromagnetisk kompatibilitet (EMCD) och maskindirektivet (MD) eller Rattmärkning.

Att uppfylla lagstiftningens tekniska krav för tekniska system och produkter ska eftersträvas, exempelvis genom CE- eller rattmärkning. För materiel som kan ha ett undantag från exempelvis CE-märkningen kan betryggande säkerhet uppnås på alternativa sätt. Detta kan exempelvis ske genom att uppfylla regelverkets tekniska krav inklusive riskanalys och harmoniserade standarder, så långt som möjligt, även om formell märkning av produkten inte genomförs. I denna handbok kallas detta för en *CE-liknande process.*

För vissa typer av tekniska system och produkter kan särskilda beslut eller intyg från myndigheter utanför Försvarsmakten krävas för att få ta systemen i bruk. Exempelvis kan godkännande krävas från:

- Myndigheten för samhällsskydd och beredskap (MSB) avseende klassning av explosivämnen
- Strålsäkerhetsmyndigheten (SSM) för användning av strålkällor
- Naturvårdsverket (NV) för användning av utarmat uran
- Livsmedelsverket (LMV) avseende veterinärintyg för hantering av livsmedel
- Delegationen för folkrättslig granskning av vapenprojekt

I *Systemmålsättning* (SMS 2) bör det finnas en lista över vilka godkännanden som behövs för att det tekniska systemet eller produkten ska kunna tas i bruk. I *Förfrågningsunderlaget* (RFP) ska krav ställas på vilka godkännanden som *konstruktören* ansvarar för.

För kvarstående olycksrisker som inte omhändertagits genom de författningsenliga kraven i vägval (VV1), ska i första hand vägval (VV2) prövas.

11.2.2 Vägval 2 – Godkänd av annan stat

Syftet med vägval (VV2) är att säkerställa att tekniska system och produkter som redan är godkända av annan stat även kan uppfylla Försvarsmaktens krav på betryggande säkerhet för avsedd användning.

Med godkännande utgivet av annan stat avses främst en utländsk försvarsmyndighet. Om en annan stat har godkänt (eller likvärdig benämning) det tekniska systemet så bör det även infordras en systemsäkerhetsrapport eller annan motsvarande systemsäkerhetsdokumentation.

Notera dock att det normalt endast är en försvarsmyndighet, exempelvis Försvarsmakten eller FMV, som kan anskaffa tekniska system av en utländsk försvarsmyndighet.

Systemsäkerhetsarbetet från annan stat bör ha följt en etablerad systemsäkerhetsstandard såsom MIL-STD-882 eller DEF STAN 00-056. Den som anskaffar tekniska system eller produkter från en annan stat, måste fullt ut analysera innebörden och omfattningen av de godkännanden som systemsäkerhetsvärderingen avser att stödja sig på. Granskningen innebär även att säkerställa att godkännandet är korrekt och rymmer Försvarsmaktens avsedda användning.

I *Systemmålsättning* (SMS 2) bör det finnas en lista över vilka stater vars godkännanden kan accepteras. Från den stat från vilken anskaffning sker bör man begära tillgång till den systemsäkerhetsdokumentation som godkännandet grundar sig på.

För kvarstående olycksrisker som inte omhändertagits genom de författningsenliga kraven i vägval (VV1) och genom godkännanden av annan stat i vägval (VV2), ska i första hand vägval (VV3) prövas.

11.2.3 Vägval 3 – Godkänd av annan part

Syftet med vägval (VV3) är att säkerställa att tekniska system och produkter som är godkända av annan part även kan uppfylla Försvarsmaktens krav på betryggande säkerhet för avsedd användning.

Med annan part avses civila myndigheter, klassningssällskap, certifierings- och kontrollorgan samt andra organ för validering och verifiering.

Civila myndigheter kan godkänna vissa typer av tekniska system, exempelvis luftfartsmyndigheter (FAA i USA och EASA i Europa) för flygplan. Dessa myndigheter certifierar flygplan och utfärdar luftvärdighetsbevis.

Ett klassningssällskap eller klassificeringssällskap är en organisation som handhar klassifikation av bland annat fartyg. Klassningssällskap tar fram regler för fartygs och andra marina installationers egenskaper ur ett systemsäkerhetsperspektiv och kan sedan göra inspektioner för att säkerställa att installationen uppfyller ställda krav. Inspektionerna kan avse tekniskt utförande men också underhållsrutiner och kvalitetsnivån på utförda varvsarbeten. Klassningssällskapen är medlemmar i den internationella branschorganisationen *International Association of Classification Societies* (IACS).

Ackreditering av laboratorier, certifierings- och kontrollorgan innebär att den verksamhet de bedriver för bedömning av överensstämmelse mot olika standarder, har granskats och godkänts. Ackrediteringen innebär kontroller av att verksamheten utförs objektivt, korrekt och grundas på internationellt erkända standarder.

Ett organ kan vara ackrediterat för en eller flera typer av besiktningar, ett certifieringsorgan för vissa standarder eller vissa produkter och ett laboratorium för ett antal specifika metoder. Det är därför viktigt att kontrollera vad ackrediteringen gäller för. Varje ackrediteringsmärke är unikt och innehåller beteckningen för den standard som ackrediteringen gäller för, tillsammans med organets ackrediteringsnummer. I Sverige är det bara organ som är ackrediterade av Swedac som får använda ackrediteringsmärket.

Bild 11.2 *Ackrediteringsmärke för organ som är ackrediterade av Swedac.*

Inom vissa områden är ackreditering obligatoriskt. Ett företag som bedriver fordonsbesiktning måste vara ackrediterat. Inom andra områden, till exempel för medicinska laboratorier är ackreditering frivillig och fungerar som en kvalitetsstämpel. Det är därför viktigt att kontrollera om ackreditering inom aktuellt område är obligatorisk eller frivillig.

I *Systemmålsättning* (SMS 2) bör det finnas en lista över vilka godkännanden från annan part som kan accepteras. I *Förfrågningsunderlaget* (RFP) ska krav ställas på tillgång till de standarder som godkännandet grundar sig på.

För kvarstående olycksrisker som inte omhändertagits genom de författningsenliga kraven i vägval (VV1), genom godkännanden av annan stat i vägval (VV2) och/eller genom annan part i vägval (VV3), ska i första hand vägval (VV4) prövas.

11.2.4 Vägval 4 – Övriga standarder

Syftet med vägval (VV4) är att säkerställa att tekniska system och produkter, som följer branschstandarder eller standarder knutna till internationella organisationer, uppfyller Försvarsmaktens krav på betryggande säkerhet för avsedd användning.

Med branschstandarder menas etablerade och internationellt tillämpade standarder samt *Allmänna råd* (AR) inom tillämpningsområdet. Med standarder knutna till internationella organisationer avses främst sådana som syftar till att möjliggöra interoperabilitet, exempelvis NATO, genom att ange gemensamma krav på systemsäkerhet eller områden som påverkar systemsäkerhet.

Vid utveckling kan krav ställas i *Systemmålsättning* (SMS 2) på att följa specifika civila och/eller militära standarder för att kunna uppfylla vissa grundläggande krav på exempelvis interoperabilitet, tekniksamordning, driftsäkerhet eller kompatibilitet med generella logistiksystem. Dessa standarder är normalt inte systemsäkerhetsrelaterade, men kan dock ge argument och belägg för systemsäkerhetsarbetet.

Det finns specifika systemsäkerhetsrelaterade standarder som anger både administrativa aspekter och konstruktionsmetodik för att kunna uppnå en viss systemsäkerhetsnivå. Användning av etablerade systemsäkerhetsrelaterade branschstandarder, som inte ligger till grund för exempelvis CE-märkning eller rattmärkning, kan ge förutsättningar för att kunna värdera åtgärder och bedöma dessa ur systemsäkerhetssynpunkt eftersom dessa kan anses vara beprövade och allmänt accepterade. Verifieringskriterier i använd standard ska alltid vara uppfyllda för att senare kunna åberopas vid systemsäkerhetsvärderingen.

I *Systemmålsättning* (SMS 2) bör det finnas en lista över vilka övriga standarder som kan accepteras. I *Förfrågningsunderlaget* (RFP) ska krav ställas på tillgång till

de standarder som godkännandet grundar sig på. Motsvarande gäller även för standarder knutna till internationella organisationer syftande till interoperabilitet.

Med etablerade systemsäkerhetstandarder för systemsäkerhetsverksamhet avses exempelvis MIL-STD-882, DEF STAN 00-056, GEIA-STD-0010 och ISO 12100.

Med etablerade tekniska standarder avses exempelvis SS-EN 61508, SS-EN ISO 13849 och DO 178C.

För kvarstående olycksrisker som inte omhändertagits genom de författningsenliga kraven i vägval (VV1), genom godkännanden av annan stat i vägval (VV2), genom annan part i vägval (VV3) och/eller genom övriga standarder i vägval (VV4), ska i första hand vägval (VV5) prövas.

11.2.5 Vägval 5 – Designregler

Syftet med vägval (VV5) är att säkerställa att tekniska system och produkter som följer *Designregler* (DR) uppfyller Försvarsmaktens krav på betryggande säkerhet för avsedd användning.

Designregler (DR) kan avse Försvarsmaktens interna bestämmelser (FIB), Försvarsmaktens *Designregler* (DR) samt FMV:s *Designregler* (DR) och handböcker (designregelsamlingar).

Designregler (DR) finns där lagstiftning och standarder är otillräckliga eller där erfarenheter av säkra konstruktioner finns av liknande tekniska system. *Designregler* (DR) handlar om hur tidigare kända olycksrisker kan undvikas eller reduceras genom viss konstruktion eller krav på principer för sådan konstruktion. Syftet är att för beprövad teknik ange lämpligt sätt att genom konstruktion eller krav på konstruktionens egenskaper, förebygga eller reducera effekten av kända olycksrisker.

I *Systemmålsättning* (SMS 2) kan det finnas en, för det tekniska systemet eller produkten, utvald lista över Försvarsmaktens FIB/DR och/eller FMV:s *Designregler* (DR) och handböcker (designregelsamlingar). I *Förfrågningsunderlaget* (RFP) kan krav ställas utifrån Försvarsmaktens FIB/DR och/eller FMV:s *Designregler* (DR) och handböcker (designregelsamlingar).

För ammunition ska alltid Vägval (VV5) tillämpas. Detta innebär att kraven i Handbok Vapen- och ammunitionssäkerhet tillämpas respektive att råd inhämtas från FMV:s Rådgivningsgrupper. Vid behov tillämpas även Vägval (VV7).

För kvarstående olycksrisker som inte omhändertagits genom de författningsenliga kraven i vägval (VV1), genom godkännanden av annan stat i vägval (VV2), genom annan part i vägval (VV3), genom övriga standarder i vägval (VV4) och/eller *Designregler* (DR) i vägval (VV5), ska i första hand vägval (VV6) prövas.

11.2.6 Vägval 6 – Beprövat system

Syftet med vägval (VV6) är att beskriva kriterier för att kunna åberopa trovärdiga och spårbara drifterfarenheter för ett beprövat system.

Med drifterfarenheter från ett beprövat system avses användning och underhåll i Försvarsmakten. Den tidigare användningen ska vara relevant för den i framtiden avsedda användningen i motsvarande användningsmiljöer. Det innebär flerårigt regelbundet brukande som genererat många drifttimmar så att trovärdiga och spårbara drifterfarenheter (Proven-In-Use) finns.

Vidare ingår analys av olycks- och tillbudsrapporter samt drift- och feluppföljning. Även brukarerfarenheter om säkerheten vid användning och underhåll kan ge värdefull information om eventuella säkerhetsbrister i det tekniska systemet eller produkten. Aspekter som förändrat användningssätt (normglidning) vid användning, ändrade underhållsintervall eller att förebyggande och avhjälpande underhåll inte har genomförts enligt anvisningar, behöver beaktas.

För att kunna åberopa drifterfarenheter för ett beprövat system så behövs om möjligt den ursprungliga dokumentationen tas fram som en gång i tiden godkände materielen för att tas i bruk. Med denna dokumentation som grund och drifterfarenheter kan det tekniska systemet, visst delsystem eller produkten hanteras som ett beprövat system.

I *Förfrågningsunderlaget* (RFP) kan kriterier för trovärdiga och spårbara drifterfarenheter finnas samt att krav ställs på tillgång till den dokumentation som använts i analysarbetet.

För kvarstående olycksrisker som inte omhändertagits genom de författningsenliga kraven i vägval (VV1), genom godkännanden av annan stat i vägval (VV2), genom annan part i vägval (VV3), genom övriga standarder i vägval (VV4), genom *Designregler* (DR) i vägval (VV5) och utifrån drifterfarenheter i vägval (VV6), ska i första hand en ny konstruktionslösning prövas. Om den nya konstruktionslösningen systemsäkerhetsmässigt inte heller kan visas uppnå betryggande säkerhet genom tillämpning av vägval (VV1 – 6), ska vägval (VV7) tillämpas.

11.2.6.1 Erfarenhetsmässiga bedömningar

Kriterier för riskvärderingen avseende vägval (VV6) Beprövat system, grundar sig på drifterfarenheter (Proven-In-Use) med ursprung i exempelvis inträffade olyckor och tillbud för samma tekniska system och produkter. Det krävs att dessa erfarenhetsdata är trovärdiga och spårbara över en längre tidsperiod. Erfarenhetsdata kan användas från samma tekniska system i bruk eller från avvecklade system. Även annan stats erfarenhetsdata kan användas om motsvarande användningsmiljöer och operationsbetingelser kan påvisas. Erfarenhetsmässiga uppskattningar betraktas därför som en kvalitativ metod.

En enkel metod för att identifiera olycksrisker för nya tekniska system är att ta tillvara på lärdomar från liknande tekniska system och produkter, dock är det är ofta vanskligt att kunna hävda liknande driftsbetingelser. Transformering och anpassning av sådana data för riskvärderingar är i princip omöjligt att göra sanna och trovärdiga.

Den som vill göra en riskvärdering grundad på drifterfarenheter (Proven-in-use) måste noggrant motivera varför jämförelsen kan göras.

11.2.7 Vägval 7 – Riskmatriser

Syftet med vägval (VV7) är att beskriva kriterier för att genom systemsäkerhetanalys bedöma om de kvarstående enskilda olycksriskerna ryms inom *Tolerabel risknivå* (TR) uttryckt i riskmatris. Riskmatriser kan vara såväl kvalitativa som kvantitativa.

Användning av riskmatriser är det sista steget i *Vägvalsmodellen* (VVM). När andra vägval (VV1 – 6), eller kombinationer av dessa, inte bedöms vara tillräckliga eller tillämpliga för att kunna påvisa betryggande säkerhet, kan vägval (VV7) tillämpas.

En kvantitativ riskmatris kan användas för olycksrisker med överskådliga orsakssamband och tillförlitliga numeriska data (inhämtade eller skattade). I övriga fall tillämpas en kvalitativ riskmatris.

Nedanstående riskvärderingsmetoder kan användas enskilt eller i kombination. Oavsett metod ska fakta och gjorda skattningar motiveras och dokumenteras för att kunna åberopas vid riskvärdering.

> Alla riskvärderingar är förutsägelser om framtiden. De utgör inte sanningar och bedömningar som uttrycks med siffror är fortfarande bara förutsägelser. En modell är alltid ett försök till avbildning av det verkliga tekniska systemet ur valda aspekter.

11.2.7.1 Expertbedömningar

Expertbedömningar används i samband med kvalitativ riskmatris för att styrka att olycksrisker anses tolerabla. Riskvärderingar för vägval (VV7) som grundar sig på expertbedömningar, är en metod som innebär att en eller helst flera personer med ingående kunskap om det tekniska systemets egenskaper och dess användning gör en kvalitativ riskvärdering. Expertbedömningar kan användas som argument för att värdera olycksrisker som har enkla samband och händelseförlopp för att en olycka ska kunna inträffa. Exempel på tekniker och metoder som är lämpliga för kvalitativa bedömningar är det tekniska systemets beteende vid enkelfel.

Expertbedömningar tenderar att bli relativt personberoende och får anses giltiga i en viss tidsperiod och kontext. Om det finns brister i dokumentationen bedöms

de därför bli svåra att få spårbara för att i framtiden kunna upprepa den gjorda riskvärderingen. En annan negativ aspekt kan vara att riskvärderingen kopieras från andra liknande tekniska system, utan att det först kritiskt har granskats om dessa bedömningar är relevanta för det nya tekniska systemet.

Som stöd för expertbedömningar kan kvalitativa felträdsmodeller och/eller händelseträdsmodeller användas.

11.2.7.2 Modelleringar

Modelleringar används i samband med kvantitativ riskmatris för att styrka att olycksrisker anses tolerabla. Riskvärderingar för vägval (VV7) som grundar sig på sannolikhetsberäkningar kan exempelvis innebära att aktuellt tekniskt system åskådliggörs i en felträdsmodell där bashändelserna åsätts siffervärden. Dessa siffervärden kan dels hämtas från tillverkarens produktinformation, dels vara erfarenhetsvärden, dels vara skattade värden. Beräkningar betraktas därför som en kvantitativ metod.

Modelleringen kan bli komplex och svåröverskådlig för större system och kräver kännedom om ingående komponenters och delsystems interna relationer och interaktioner. Osäkerheten kan dessutom öka i kombination med en osäker driftprofil. Trots detta ges ibland värdena ändå alltför hög tilltro.

Alla modeller är per definition ofullständiga eftersom de endast fokuserar på de identifierade beroendena. Modeller kan endast användas som stöd för beläggen för att göra argumenten starkare vid riskvärderingen.

11.3 Ställningstagande, argument och belägg

Under konstruktions- eller integrationsarbetet prövas möjligheterna att uppfylla acceptanskriterierna för de tillåtna vägvalen (VV1 – VV6) för det tänkta tekniska systemet, eller för dess ingående komponenter. Möjliga argument och belägg identifieras, för att succesivt under konstruktions- eller integrationsarbetet kunna visa att hela eller delar av det tekniska systemet uppfyller ställda systemsäkerhetskrav. Om det för vissa enskilda olycksrisker inte går att visa på kravuppfyllnad genom vägvalen (VV1 – VV6) tillämpas vägval (VV7).

I systemsäkerhetsbeslutet ska ställningstagandet visa att betryggande säkerhet för det tekniska systemet har uppnåtts. I arbetet med systemsäkerhetsvärderingen ska argument presenteras som redogör för varför det är säkert utifrån givna förutsättningar.

Argument är ett, men ofta flera, påstående som anförs för att det tekniska systemet ska anses uppfylla lagstiftning respektive ställda systemsäkerhetskrav. Argumenten ska så långt som möjligt styrkas med belägg.

Belägg kan dels vara bevis, dels bestå av andra uppgifter av starkare eller svagare karaktär som helt eller till del styrker olika argument. Flera olika belägg kan föras samman för att styrka ett visst argument.

Argumenten bedöms dels utifrån om beläggen som argumenten bygger på är hållbara, dels om beläggen är relevanta. Om beläggen är hållbara och relevanta är argumentet giltigt. Granskning av argument går ut på att hitta ogiltiga eller svaga argument och ta bort dessa så enbart giltiga argument blir kvar i systemsäkerhetsvärderingen.

I engelskspråkiga sammanhang benämns ett resonemang med ställningstagande, argument och belägg ofta som *Safety Case*.

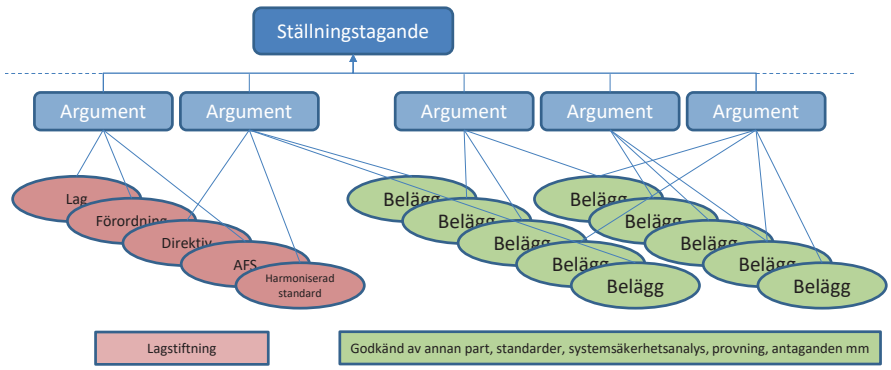


Bild 11.3 Ställningstagandet i systemsäkerhetsbeslutet byggs upp av argument och belägg.

12 Val av systemsäkerhetsaktiviteter

Syftet med detta kapitel är att beskriva hur val av systemsäkerhetsaktiviteter kan ske utifrån aktuellt tekniskt system, lagstiftning, övriga regelverk, erfarenheter samt med hänsyn tagen till de olika aktörerna och deras roller.

12.1 Grunder inför anpassning av systemsäkerhetsverksamheten

Systemsäkerhetsverksamhet genomförs under ett tekniskt systems alla livscykelskeden. För vissa tekniska system och produkter finns utförlig lagstiftning till skydd mot ohälsa och olycksfall. För andra tekniska system kan det finnas behov av ett särskilt systemsäkerhetsarbete om lagstiftning och övriga regelverk saknar detaljerade och verifierbara krav.

För produkter som granskas och verifieras/godkänns via ett annat förfarande, exempelvis CE-märkning eller rattmärkning, kan detta omhänderta delar av systemsäkerhetsarbetet.

Systemsäkerhetsarbetet består dels av obligatoriska aktiviteter, dels av aktiviteter för selektivt urval utifrån aktuellt tekniskt system. Behovet av aktiviteter utöver de obligatoriska kan vara svårt att förutse innan den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) överenskoms och konstruktionsarbetet påbörjas. Aktiviteter för selektivt urval kan under konstruktionsarbetet både läggas till eller väljas bort. Alla aktiviteter får vid behov anpassas utifrån aktuellt tekniskt system eller utifrån ändringens (modifieringens) dignitet.

De obligatoriska aktiviteterna genomförs alltid för samtliga tekniska system och produkter. Aktiviteter för selektivt urval kan exempelvis erfordras för att visa hur betryggande säkerhet har uppnåtts. Aktiviteter för selektivt urval kan ersättas med andra motsvarande aktiviteter eller, efter medvetet beslut, väljas bort.

12.2 Motiv för att anpassa av systemsäkerhets-arbetet

För att kunna anpassa det systemsäkerhetsarbete som fordras av en aktör i en viss roll behöver det aktuella tekniska systemet avgränsas och riskinnehåll identifieras. Anpassningen av systemsäkerhetsarbetet genom val av aktiviteter sker efter en sammanvägning av flera olika faktorer enligt nedan.

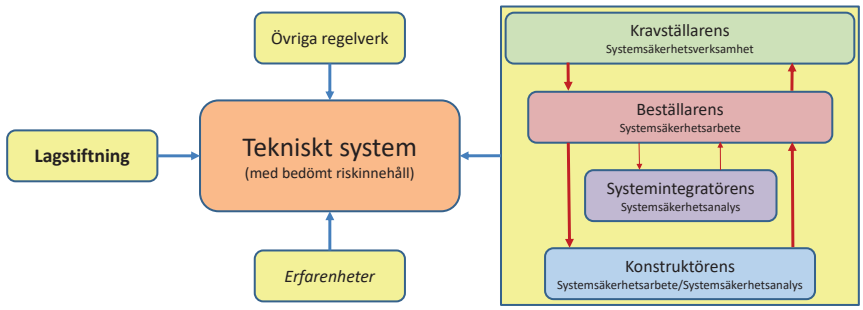


Bild 12.1 *Systemsäkerhetsarbetets omfattning behöver anpassas utifrån olika faktorer och aktörens roll.*

12.2.1 Tekniska systemets inramning och bestämmande av kategori

För att kunna anpassa systemsäkerhetsarbetet behöver det aktuella tekniska systemet ramas in och dess gränsytor definieras. Det krävs även en inriktning i *Systemmålsättningen* (SMS 2) om det tekniska systemet bör vara utan eller får vara med undantag för militär materiel. Därefter bestäms till vilken eller vilka kategorier det tekniska systemet med dess ingående produkter hör. Se kapitel 10 *Anskaffning av tekniska system.*

12.2.2 Lagstiftning, övriga regelverk och erfarenheter

Uppfyllande av EU-rätt, svensk lagstiftning, tillämpning av övriga regelverk och förhållningssätt till erfarenheter för att kunna uppnå betryggande säkerhet framgår av kapitel 11 *Vägvalsmodellen*.

12.2.3 Aktörer och roller

Systemsäkerhetsarbetets omfattning och djup varierar för de olika rollerna. Notera att en aktivitet som är obligatorisk för en roll kan vara föremål för selektivt urval för en annan roll.

Kravställaren leder systemsäkerhetsverksamheten för det tekniska systemet under alla dess livscykelskeden. *Kravställaren* ställer krav på och inriktar det systemsäkerhetsarbete som *beställaren* ska genomföra. *Beställaren* i sin tur ställer krav på och inriktar *konstruktörens* respektive *systemintegratörens* systemsäkerhetsarbete och systemsäkerhetsanalyser samt ställer krav på systemsäkerhetsdokumentationen. *Konstruktören* och *systemintegratören* får lägga till fler aktiviteter än de som *beställaren* har kravställt.

Systemintegratören har ett konstruktionsansvar som liknar *konstruktörens*, men ansvaret är begränsat så länge det handlar om att skapa nya förmågor och funktionaliteter genom samfunktion utan att de ingående systemen sammanbyggs eller att omkonstruktioner genomförs. *Systemintegratören* säkerställer dels att de fysiska gränsytorna passar ihop, dels att programvaror kan utbyta information, dels att de tekniska systemen inte påverkar varandra, exempelvis avseende elektromagnetisk strålning (EMC). Om de ingående systemen sammanbyggs (integreras) kan denna aktör komma att betraktas som tillverkare enligt EU-direktiven. Eventuella omkonstruktioner genomförs därför alltid av en *konstruktör*.

12.3 Karta över systemsäkerhetsaktiviteter

Systemsäkerhetsaktiviteterna som till största delen är baserade på standarden MIL-STD-882E, är indelade i fem olika sektioner. För varje sektion finns dels obligatoriska aktiviteter som ska genomföras, dels aktiviteter för selektivt urval. Aktiviteter för selektivt urval kan ibland ersättas av aktiviteter i andra standarder eller genom motsvarande aktörsinterna aktiviteter.

Aktiviteterna är indelade i följande sektioner:

- SEKTION 100 Planering/Styrning
- SEKTION 200 Analyser
- SEKTION 300 Utvärdering
- SEKTION 400 Verifiering
- SEKTION 500 Beslut

Nedan visas hur aktiviteterna i de olika sektionerna i stort samverkar. Flera av aktiviteterna samverkar med ytterligare aktiviteter, vilket framgår under respektive aktivitetsbeskrivning i bilaga 3. Endast de mest väsentliga kopplingarna har tagits med i bilden nedan.

Exempelvis kan *Systemsäkerhetsledningsplanen* (SSMP) reglera fler aktiviteter i sektionerna 100, 300 och 500. *Systemsäkerhetsplanen* (SSPP) kan reglera flertalet av aktiviteterna i sektionerna 200, 300, 400 samt vissa av aktiviteter i sektion 100 och 500.

Bilden nedan åskådliggör även i någon mån tidsaspekten. Den första aktiviteten *Systemsäkerhetsprogram* (SSP) finns längst upp till vänster och den sista aktiviteten *Systemsäkerhetsgodkännande* (SSG) finns längst ner till höger. Se bilaga 3.

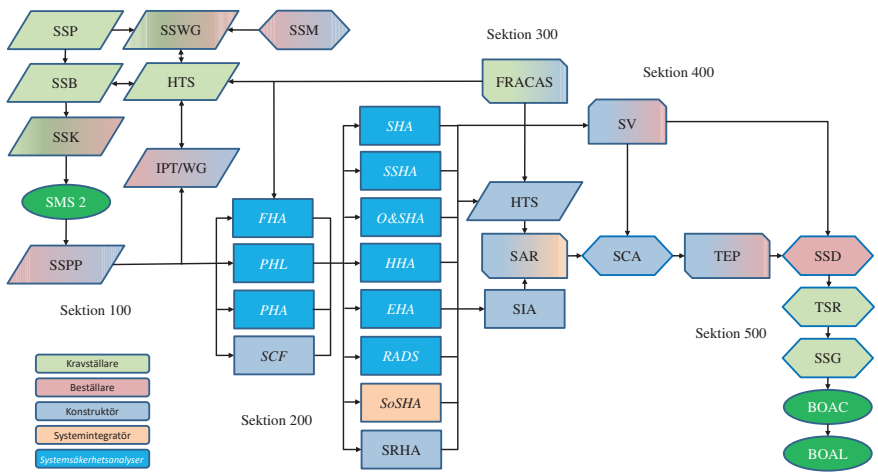


Bild 12.2 *Väsentligaste kopplingarna mellan olika systemsäkerhetsaktiviteter ur kravställarens perspektiv.*

12.4 Anpassning av systemsäkerhetsarbetet

Flera av systemsäkerhetsaktiviteterna kan genomföras av olika aktörer i deras roller som *kravställare, beställare, systemintegratör* respektive *konstruktör.* Aktiviteterna kan därför återkomma flera gånger under livscykeln och genomföras med olika omfattning och djup. Gemensamt för aktörerna är att anpassning av systemsäkerhetsarbetet behöver genomföras utifrån aktuellt tekniskt system eller ändringens (modifieringens) dignitet. Vidare kan de olika aktiviteterna behöva anpassas utifrån möjliga vägval i *Vägvalsmodellen* (VVM).

För vissa kategorier av tekniska system och produkter krävs att många olika aktiviteter genomförs. För andra tekniska system kan de selektivt valda aktiviteterna slås ihop eller, efter medvetet beslut, väljas bort. Vid anpassning av aktiviteter kan exempelvis andra metoder tillämpas eller annat format för rapportering användas än de som anges i aktivitetsbeskrivningarna. Vissa rapporter kan slås samman eller informationen kan infogas i andra rapporter.

Aktiviteter för systemsäkerhetsanalyser kan ibland slås samman till ett färre antal aktiviteter. Resultatet av systemsäkerhetsanalyserna ska dock spegla alla aspekter som de olika separata aktiviteterna avser att omhänderta. Exempelvis kan den hälsoinriktade aktiviteten (HHA) och den miljöinriktade (EHA) samordnas. De aktiviteter som väljs ska dokumenteras i *Systemsäkerhetsplanen* (SSPP). Om aktiviteterna anpassas (förenklas) gentemot aktivitetsbeskrivningarna behöver även detta beskrivas i *Systemsäkerhetsplanen* (SSPP).

12.5 Aktörernas obligatoriska systemsäkerhetsaktiviteter

Försvarsmakten i rollen som *kravställare* genomför ett antal obligatoriska systemsäkerhetsaktiviteter som i sin tur styr eller inriktar *beställarens*, *konstruktörens* och/eller *systemintegratörens* systemsäkerhetsarbete och systemsäkerhetsanalyser.

Beställaren, konstruktören och/eller *systemintegratören* genomför ett antal obligatoriska systemsäkerhetsaktiviteter. Utöver de obligatoriska kan selektivt valda aktiviteter genomföras som underlag till systemsäkerhetsvärderingen.

Nedan presenteras de systemsäkerhetsaktiviteter som normalt är obligatoriska vid anskaffning av tekniska system eller vid ändring (modifiering).

12.5.1 Kravställarens obligatoriska systemsäkerhetsaktiviteter

Försvarsmakten i rollen som *kravställare* genomför följande obligatoriska systemsäkerhetsaktiviteter under ett tekniskt systems olika livscykelskeden.

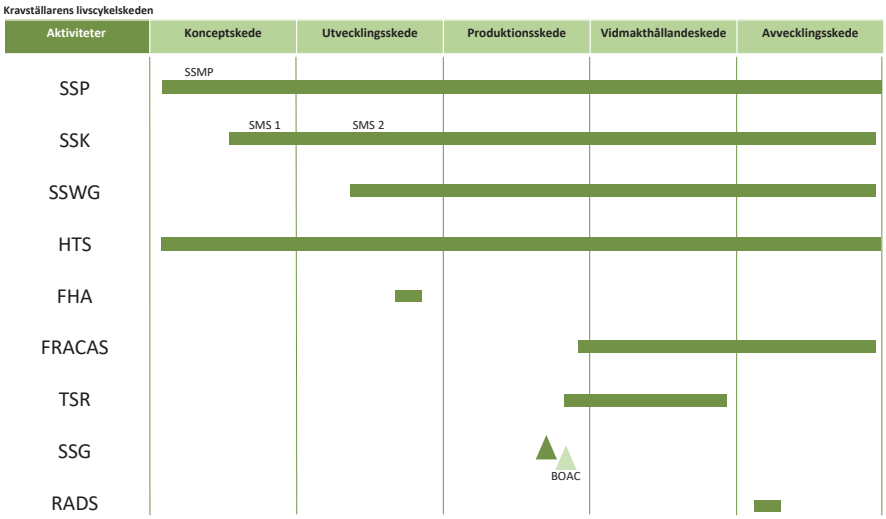


Bild 12.3 Kravställarens obligatoriska systemsäkerhetsaktiviteter.

12.5.2 Beställarens obligatoriska systemsäkerhetsaktiviteter

Beställaren genomför följande obligatoriska systemsäkerhetsaktiviteter under Försvarsmaktens *produktionsskede. Beställaren* kan biträda *kravställaren* i arbetet redan under Försvarsmaktens *utvecklingsskede.* Utöver systemsäkerhetsaktiviteterna i bilden nedan kan någon selektivt vald systemsäkerhetsaktivitet tillkomma.

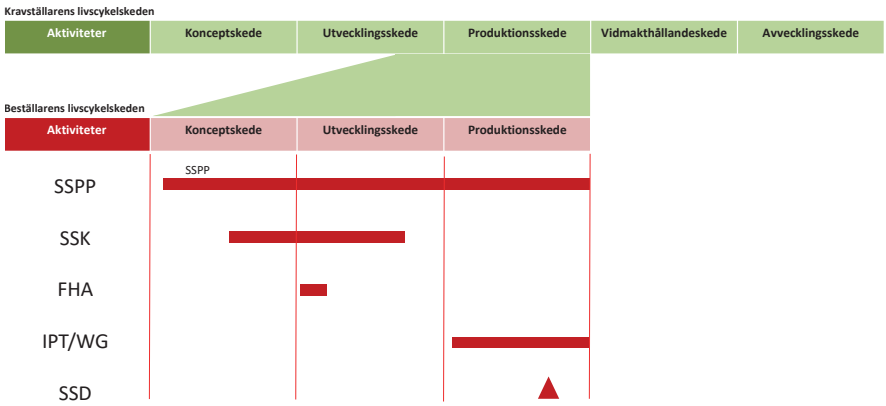


Bild 12.4 Beställarens obligatoriska systemsäkerhetsaktiviteter.

12.5.3 Konstruktörens obligatoriska systemsäkerhetsaktiviteter

Konstruktören tillämpar oftast en etablerad utvecklingsmodell för nya tekniska system. De granskningar som ska genomföras regleras normalt i en *Systems Engineering Management Plan* (SEMP).

Redovisning av resultat från de olika systemsäkerhetsaktiviteterna kopplas lämpligen till olika konstruktions-/tekniska genomgångar *(Technical Reviews)*. Fördelen med att koppla systemsäkerhetsarbetet till konstruktions-/tekniska genomgångar är att dessa integreras med *Systems Engineering*-verksamheten. På detta sätt erhåller man en strikt koppling till det tekniska systemets utveckling.

Vid eller inför dessa konstruktions-/tekniska genomgångar sker lämpligen även tekniska granskningar av det tekniska systemet för att säkerställa att EU-rätt, svensk lagstiftning, kundkrav och relaterade standarder/handböcker uppfylls. Detta sker lämpligen vid preliminär konstruktionsgranskning *(Preliminary Design Review,* PDR*)* och kritisk konstruktionsgranskning *(Critical Design Review,* CDR*)*.

Preliminär konstruktionsgranskning (PDR) – En formell granskning som bekräftar att den preliminära designen uppfyller kraven. Det resulterar normalt i godkännande för att påbörja en detaljerad konstruktion.

Kritisk konstruktionsgranskning (CDR) – En formell granskning för att utvärdera konstruktionens fullständighet och dess gränssnitt.

Beroende på det tekniska systemets komplexitet, riskinnehåll och möjliga vägval i *Vägvalsmodellen* (VVM) kan *konstruktören* genomföra följande systemsäkerhetsaktiviteter under *beställarens produktionsskede*, som hos *konstruktören* utgörs av *koncept-, utvecklings-* respektive *produktionsskede*. Utöver systemsäkerhetsaktiviteterna i bilden nedan kan ytterligare selektivt valda systemsäkerhetsaktiviteter tillkomma.

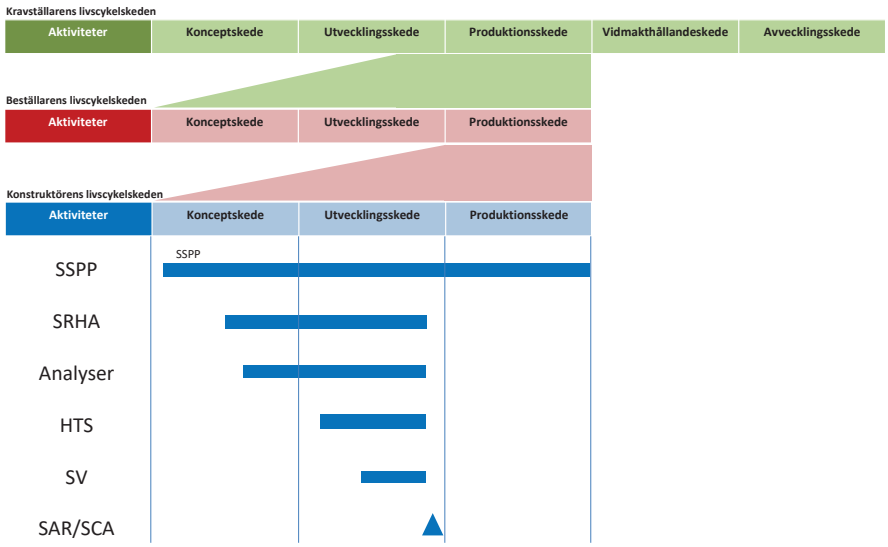


Bild 12.5 *Konstruktörens obligatoriska systemsäkerhetsaktiviteter.*

Till Analyser i bilden ovan kan ett flertal systemsäkerhetsaktiviteter från SEKTION 200 inordnas.

12.5.4 Systemintegratörens obligatoriska systemsäkerhets-aktiviteter

Beroende på det tekniska systemets/system-av-systems komplexitet, riskinnehåll och möjliga vägval i *Vägvalsmodellen* (VVM) kan *systemintegratören* genomföra följande systemsäkerhetsaktiviteter under *beställarens Produktionsskede*. Utöver systemsäkerhetsaktiviteterna i bilden nedan kan ytterligare selektivt valda systemsäkerhetsaktiviteter tillkomma.

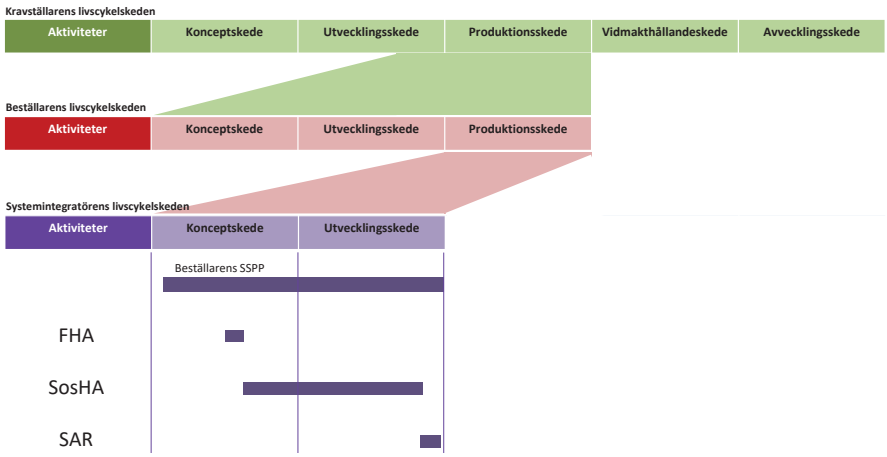


Bild 12.6 Systemintegratörens obligatoriska systemsäkerhetsaktiviteter.

12.6 Metodik inför selektiva val av systemsäkerhetsaktiviteter

Generellt kan systemsäkerhetsaktiviteterna delas upp i obligatoriska aktiviteter respektive aktiviteter för selektivt urval. Vissa systemsäkerhetsaktiviteter är normalt alltid tillämpliga, exempelvis systemsäkerhetsbesluten (SEKTION 500) som utfärdas av olika aktörer. Normalt väljs en eller flera aktiviteter från respektive sektion. Se bilaga 3 *Beskrivning av systemsäkerhetsaktiviteter.*

Vid selektivt val av systemsäkerhetsaktiviteter behöver en inledande systemsäkerhetsanalys genomföras för att klarlägga huruvida det finns olycksrisker förknippade med det tekniska systemet, dess användning och/eller hantering. Detta kan ske genom en *Funktionell riskanalys* (FHA) och/eller genom *Risk-*

källelista (PHL). Denna inledande systemsäkerhetsanalys behöver dock inte vara formell eller följa någon särskild standard.

För vissa produkter behövs endast de obligatoriska systemsäkerhetsaktiviteterna tillämpas. För andra tekniska system krävs att selektivt valda systemsäkerhetsaktiviteter läggs till.

För att bedöma behovet av ytterligare systemsäkerhetsaktiviteter utöver de obligatoriska behöver följande överväganden göras:

- Omfattar det tekniska systemet många identifierade olycksrisker vars konsekvenser kan betraktas som allvarliga?
- Kan det antas att det tekniska systemet innehåller olycksrisker vars orsakssamband är svåra att förutse och därför kräver ett systematiskt arbetssätt för att redas ut?
- Har det tekniska systemet komplexa gränsytor och interaktioner till andra system där samspelet mellan dessa kräver ett systematiskt arbetssätt för att redas ut?
- Finns tekniska nyheter för vilka begränsad erfarenhet finns eller saknas?
- Används tidigare känd teknik i en annan kontext eller på ett nytt sätt än som gjorts tidigare?
- Kan det antas att det tekniska systemet innehåller eller kan generera farliga ämnen av olika slag? Då kan *hälso-* (HHA) och *miljöinriktade* (EHA) systemsäkerhetsanalyser tillämpas.
- Kan det antas att det tekniska systemet kommer att kräva särskild hantering? Då kan *Riskanalys för användning och underhåll* (O&SHA) tillämpas.
- Bedöms det att producentansvar för det tekniska systemet kommer att saknas? Då kan *Riskanalys inför avveckling av system* (RADS) tillämpas. Notera att aktiviteten RADS även kan användas som ett konstruktionshjälpmedel under utvecklingsarbetet.
- Kan det antas att lagstiftning och standarder är nya eller är signifikant ändrade i samband med ändring (modifiering) sedan det tekniska systemet togs i bruk? Då kan aktiviteten *Systemsäkerhetskravanalys* (SRHA) tillämpas.

12.7 Aktörernas selektiva urval av systemsäkerhetsaktiviteter

Tabellen nedan anger vilken roll *(kravställare, beställare, systemintegratör, konstruktör)* som normalt genomför de olika systemsäkerhetsaktiviteterna vid utveckling av ett nytt tekniskt system eller vid ändring (modifiering). Detta gäller inte för produkter som kommer att granskas och verifieras/godkännas via ett annat förfarande, exempelvis genom CE-märkning eller rattmärkning.

I tabellen nedan används följande kodning:

- Röda aktiviteter genomförs alltid (obligatoriska)
- Gula aktiviteter genomförs normalt, men kan väljas bort (selektivt urval)

Aktivitet		Kravställare	Beställare	Systemintegratör	Konstruktör
SEKTION 100	SSP	SSMP			
	SSB	SSB			
	SSK	SMS	RFP		
	SSPP		SSPP		SSPP
	SSWG	SSWG	SSWG		
	IPT/WG		IPT/WG	IPT/WG	IPT/WG
	HTS	HTS	HTS		HTS
SEKTION 200	FHA	FHA	FHA	FHA	FHA
	PHL	PHL	PHL	PHL	PHL
	PHA				PHA
	SCF				SCF
	SRHA			SRHA	SRHA
	SSHA				SSHA
	SHA				SHA
	O&SHA				O&SHA
	SoSHA			SoSHA	SoSHA
	HHA				HHA
	EHA				EHA
	SIA			SIA	SIA
	RADS	RADS			RADS

Aktivitet		Kravställare	Beställare	System-integratör	Konstruktör
SEKTION 300	SAR	SAR	SAR	SAR	SAR
	TEP		TEP	TEP	TEP
	FRACAS	FRACAS	FRACAS		FRACAS
	SR				SR
SEKTION 400	SV		SV	SV	SV
SEKTION 500	SCA				SCA
	SSD		SSD		
	TSR	TSR			
	SSG	SSG			
	SSM		SSM		SSM

Bild 12.7 Roller som vanligtvis genomför vissa systemsäkerhetsaktiviteter.

13 Olycksriskmodellen

Syftet med detta kapitel är att beskriva sambandet mellan vådahändelse, olycka, tillbud, olycksrisk och skadeutfall samt att redogöra för Försvarsmaktens Olycksriskmodell (ORM) som ger möjlighet att på ett systematiskt sätt arbeta med riskreducerande åtgärder.

13.1 Samband mellan vådahändelse, olycka, tillbud och olycksrisk

Försvarsmakten ställer krav på att tekniska system och produkter erbjuder betryggande säkerhet. För enskilda olycksrisker, som behöver hanteras genom systemsäkerhetsanalys och riskvärdering i vägval (VV7), ställs krav på riskbedömning mot en *Tolerabel risknivå* (TR) uttryckt i en riskmatris. Inför leverans eller överlämning av tekniska system eller produkter till Försvarsmakten sker en redovisning av dels hur betryggande säkerhet har uppnåtts, dels hur enskilda olycksrisker kan anses underskrida *Tolerabel risknivå* (TR). Genom systemsäkerhetsvärderingen fås den samlade bilden av det tekniska systemets eller produktens säkerhet och ställningstagandet redovisas med argument och belägg.

Olycksriskens storlek och omfattning uttrycks i sannolikhet för olycka med vissa skadeutfall. Ju allvarligare skadeutfall och ju högre sannolikheten är för denna skada, desto större anses olycksrisken vara. Därför behöver nivån för *Tolerabel risknivå* (TR) sättas i relation till dels skadeutfallets allvarlighet, dels sannolikheten för att den relaterade olyckan inträffar.

En olycka inträffar om en vådahändelse inträffar och något skyddsvärt skadas. Med tillbud menas att en vådahändelse inträffar som inte leder till något skadeutfall.

13.2 Beskrivning av Olycksriskmodellen (ORM)

Varje olycka eller tillbud är unik utifrån att olika förutsättningar och betingelser gäller just då händelsen inträffar. Olyckor har ofta komplexa händelseförlopp sett till de orsaker och indirekta förhållanden som föranlett dem. En *Olycksriskmodell* (ORM) kan därför aldrig till fullo beskriva alla olika förutsättningar och

betingelser som kan finnas, utan endast visa en förenklad bild över faktorer som behöver tas hänsyn till i systemsäkerhetsarbetet.

Olycksriskmodellen (ORM) är främst beskriven för att användas i dialogen mellan *beställare* och *konstruktör* i samband med konstruktionsgranskning och gäller främst för olycksrisker som hanteras genom Vägval (VV7).

Olycksriskmodellen (ORM) kan tillämpas för både fysiska och funktionella riskkällor. *Olycksriskmodellen* (ORM) kan därmed ge stöd för argument och belägg vid genomförande av systemsäkerhetsvärderingen.

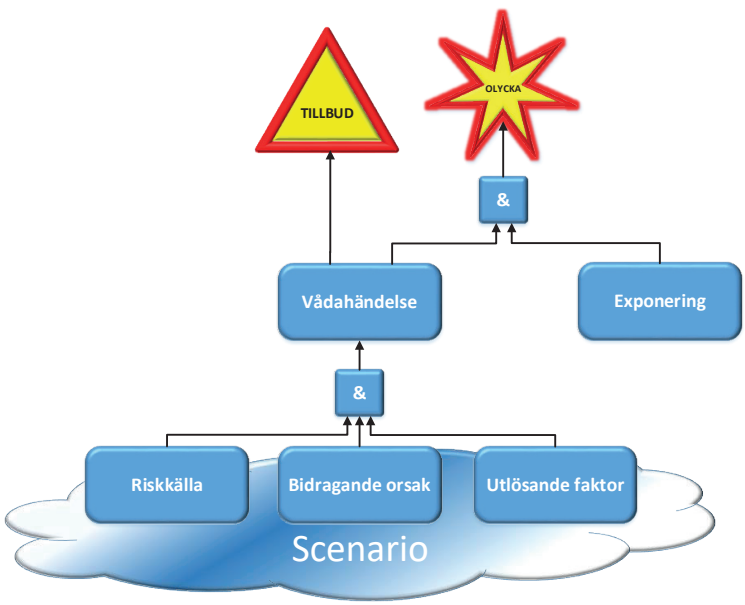


Bild 13.1 Olycksriskmodellen (ORM).

Nedan finns beskrivningar av begrepp anpassade för *Olycksriskmodellen* (ORM). Det är således inga strikta definitioner av termer.

13.2.1 Riskkälla

Olycksriskmodellen (ORM) utgår från att varje olycka har sitt ursprung i en riskkälla. En riskkälla kan vara en funktionell eller fysikalisk egenskap. Det kan

vara en farlig funktion, komponent, substans eller annan omständighet som kan orsaka skada på person, egendom eller yttre miljö. Riskkällorna är oftast, men inte nödvändigtvis, någon form av information, energi eller emission.

En komponent eller substans kan ha en eller flera olika typer av farliga fysikaliska egenskaper (riskkällor). Ett vägfordon i rörelse har riskkällan kinetisk rörelseenergi som kan skada personer i och utanför vägfordonet vid en kollision. Ett explosivt ämne är en riskkälla vars farliga egenskap ligger i den energi som kan utvecklas vid en detonation. Riskkällan kan utgöras av något som har potentiell (lagrad) energi som farlig egenskap, exempelvis en spänd stålfjäder, fritt hängande last eller om en person befinner sig på en hög höjd. Riskkällan kan även utgöras av elektricitet eller strålning. En komponent redovisas alltid tillsammans med sina farliga egenskaper (riskkällor).

En komponent kan generera en eller flera funktionella riskkällor genom fel i de olika funktionerna som den representerar, såsom felaktig information. Exempelvis kan en funktionell riskkälla ange fel måldata, grupperingsdata eller tid, där sådana fel kan leda till en vådahändelse hos det tekniska systemet. Fel måldata från ett ledningssystem kan ge till resultat att vapenverkan inte sker mot avsett mål.

Riskkällor kan även vara naturfenomen såsom åsknedslag, statisk elektricitet och isbildning. De farliga egenskaper som inte är förknippade med en energi- eller emissionsform, kan vara ett farligt ämne eller en syrefattig atmosfär i ett slutet utrymme.

Olika standarder kan ha skilda definitioner av begreppet riskkälla. O*lycksrisk-modellens* (ORM) uppdelning av komponent/substans, riskkälla, bidragande orsak och farligt tillstånd kan alla benämnas som riskkällor i andra standarder.

En *riskkälla* är en farlig egenskap som kan leda till skada på person, egendom eller yttre miljö. En *riskkälla* kan även vara ett naturfenomen.

För att sammanställa en lista över komponenter/substanser med dess riskkällor kan aktiviteten *Riskkällelist*a (PHL) tillämpas.

Komponent	Riskkälla
Lucka	Lägesenergi som övergår i rörelseenergi

Tabell 13.1 Exempel på komponent med sin riskkälla.

Att riskkällan finns närvarande betyder inte att det behöver vara någon omedelbar eller direkt fara för en olycka eller tillbud. I vissa fall kan det finnas ett mervärde att dokumentera i vilka situationer som riskkällan är aktiv respektive latent.

Komponent	Riskkälla	Farligt tillstånd	”Ofarligt” tillstånd
Lucka	Lägesenergi som övergår i rörelseenergi	Luckan öppen	Luckan stängd

Tabell 13.2 Exempel på situation med aktiv eller latent riskkälla.

13.2.2 Scenario

Ett scenario beskriver de olika förutsättningar och betingelser som gäller innan en händelsekedja inleds som kan leda till en olycka eller ett tillbud. En beskrivning av ett scenario kan innehålla:

- Den verksamhet som utövas/pågår, antingen genom att:
  - Definiera specifika situationer
  - Använda standardscenarion såsom användning, förflyttning, strid, vård, underhåll och förrådshållning (transport)
  - Beakta nödsituationer såsom nödutrymning och räddningsoperationer
- Antal personer närvarande, deras ansvar, uppgifter och eventuell anspänningsnivå
- Användningsmiljö
- Ljusförhållanden
- Ljudbild
- Väderbetingelser/-förhållanden
- Övriga aspekter som kan vara av intresse
  - Närvaro av personlig skyddsutrustning (PPE)
  - Gränsytor till anläggningars basresurser
  - Tredje person eller dennes egendom inblandat

Ett *scenario* beskriver användningsmiljön.

13.2.3 Vådahändelse

En vådahändelse är en icke önskvärd händelse som inträffar oavsiktligt. Dels kan det vara ett tekniskt fel, dels kan det vara ett mänskligt felhandlande som sker av våda eller genom misstag (okoncentration). En vådahändelse kan resultera i en olycka om något skyddsvärt exponeras, annars sker ett tillbud.

En riskkälla orsakar inte vådahändelser enbart genom sin närvaro, utan det krävs att komponenten/substansen av någon anledning hamnar i ett oönskat tillstånd så att dess farliga egenskaper är fria eller aktiverade.

En vådahändelse inträffar oavsiktligt och utan uppsåt och kan resultera i olycka eller tillbud.

Komponent	Riskkälla	Farligt tillstånd	Vådahändelse
Lucka	Lägesenergi som övergår i rörelseenergi	Luckan öppen	Luckan faller igen

Tabell 13.3 Exempel på vådahändelse.

13.2.4 Bidragande orsaker

Bidragande orsaker är förhållanden som tillsammans med en riskkälla ger förutsättningar för en vådahändelse. Om en pågående bidragande orsak kan upptäckas i tid och hindras innan en vådahändelse inträffar återgår det tekniska systemet eller produkten till ett säkert (säkrare) tillstånd.

De bidragande orsakerna kan delas upp i tillåtna orsaker, direkta orsaker och säkerhetskulturella orsaker.

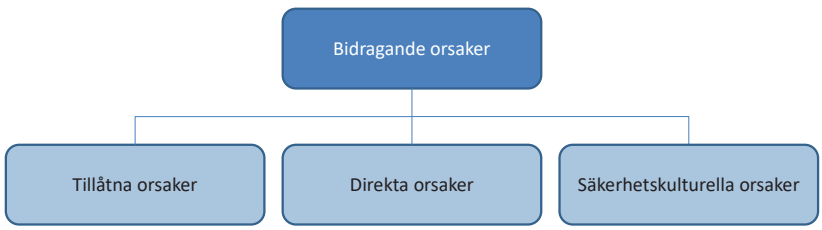


Bild 13.2 Bidragande orsaker kan vara tillåtna, direkta eller säkerhetskulturella orsaker.

Med tillåtna orsaker menas att det tekniska systemet eller produkten är i ett visst tillåtet systemtillstånd såsom att ett vapen är osäkrat, viss data tas emot av ett datorsystem, en strömbrytare är på eller av, eller att ett lock eller lucka är öppen eller stängd. Tillstånden är således både ämnade och rimliga vid avsedd användning. Ansvaret för dessa vilar främst på *konstruktören*.

Med direkta orsaker menas de förhållanden som existerar under en tid före och fram till att vådahändelsen inträffar. Dessa kan delas upp i *bristfälliga förhållanden* respektive *bristfälliga handlingar* eller *felaktig praxis*.

Bristfälliga förhållanden kan till exempel vara otillräckliga varningssystem, otillräcklig eller felaktig skydds-/säkerhetsutrustning eller farliga miljöer. Ansvaret för att åtgärda dessa vilar främst på *konstruktören*.

Bristfälliga handlingar eller felaktig praxis kan till exempel vara att säkerhetsutrustning sätts ur funktion, felaktig användning av maskiner och utrustning eller underlåtenhet att använda personlig skyddsutrustning (PPE). Ansvaret för att åtgärda dessa vilar främst på den som har arbetsgivar- och delegerad arbetsmiljöuppgift.

De säkerhetskulturella orsakerna är detsamma som de verkliga anledningarna som ligger till grund för att *bristfälliga handlingar* eller *praxis* uppstår eller får fortgå. De säkerhetskulturella orsakerna kan delas upp i *organisatoriska* och *personliga faktorer.*

Organisatoriska faktorer kan vara brister i utformning av arbetsplatsen, undermåligt underhåll, brister i utrustning, materiel och verktyg, undermåliga instruktioner för uppgiftens utförande eller bristfälligt ledarskap. Ansvaret för dessa vilar främst på den som har arbetsgivar- och delegerad arbetsmiljöuppgift.

Personliga faktorer kan vara otillräckliga kunskaper, otillräcklig kapacitet, trötthet, stress eller bristande motivation. Ansvaret vilar främst på den som har arbetsgivar- och delegerad arbetsmiljöuppgift.

Bidragande orsaker är förhållanden som tillsammans med en riskkälla ger förutsättningar för en vådahändelse.

Komponent	Riskkälla	Bidragande orsaker	Vådahändelse
Lucka	Lägesenergi som övergår i rörelseenergi	Luckan är inte spärrad i uppfällt läge	Luckan faller igen

Tabell 13.4 Exempel på bidragande orsak.

13.2.5 Utlösande faktor

Med utlösande faktor menas att en viss omständighet inträffar som utlöser en vådahändelse, förutsatt att både riskkällan och de bidragande orsakerna existerar samtidigt.

En riskkälla och en utlösande faktor kan ibland vara svåra att skilja på i ett visst scenario. En utlösande faktor i ett scenario, kan vara en riskkälla i ett annat scenario eller omvänt. Utlösande faktorer kan således vara brister i det tekniska systemet eller produkten, alternativt komponenter som används på ett korrekt sätt och där systemtillståndet medvetet ändras, exempelvis via en strömbrytare.

Utlösande faktorer kan även vara yttre påverkan såsom brand, regn, åsknedslag, statisk elektricitet, värme, kyla, fukt eller skadedjur. Även ett fientligt angrepp kan vara en utlösande faktor men detta hanteras utanför systemsäkerhetsområdet.

En *utlösande faktor* är en mekanism som tillsammans med en riskkälla och bidragande orsaker åstadkommer en vådahändelse.

Komponent	Bidragande orsaker	Utlösande faktor	Vådahändelse
Lucka	Luckan är inte spärrad i uppfällt läge	Vind eller stormby	Luckan faller igen

Tabell 13.5 Exempel på utlösande faktor.

13.2.6 Olycka

Med olycka menas att en vådahändelse inträffar samtidigt som något skyddsvärt såsom person, egendom och/eller yttre miljö skadas. En olycka är alltid oplanerad och oavsiktlig. Olyckan är inte ett resultat av exempelvis en fientlig handling.

En olycka kan ge både omedelbara skador såsom dödsfall, förlorad syn eller benbrott alternativt initiera skador som kan vålla ohälsa under lång tid framöver såsom hörselnedsättning eller en whiplash-skada. Psykisk ohälsa i form av krisreaktion med anledning av olyckan hanteras utanför systemsäkerhetsområdet.

En *olycka* inträffar då person, egendom och/eller yttre miljö skadas av riskkällan som följd av att vådahändelsen inträffar.

För att enklare identifiera olycksrisker, och inte kvalitetsmässiga brister, bör dessa alltid formuleras enligt nedan. Gradera heller inte allvarlighetsgraden i formuleringen.

- Personskada vid… orsakad av/på grund av/vållad av…
- Egendomsskada vid… orsakad av/på grund av/vållad av…
- Miljöskada vid… orsakad av/på grund av/vållad av…

Komponent	Vådahändelse	Skyddsvärt	Olycksrisker
Lucka	Luckan faller igen	Person	Personskada (klämskada) orsakad av fallande lucka

Tabell 13.6 Exempel på olycksrisk.

13.2.7 Tillbud

Med tillbud menas att en vådahändelse inträffar men där inte något skyddsvärt såsom person, egendom eller yttre miljö skadas.

Det förekommer många fler tillbud än det inträffar olyckor. Från båda händelsetyperna, olycka och tillbud, kan värdefull information erhållas för att förbättra systemsäkerheten genom att identifiera de bidragande orsakerna och utlösande faktorerna. Genom detta är det möjligt att identifiera riskreducerande åtgärder för att minska sannolikheten för vådahändelsen inträffar eller att begränsa konsekvenserna om den ändå inträffar.

Med *tillbud* menas att en vådahändelse inträffar men den orsakar ingen skada.

13.3 Tillämpning av Olycksriskmodellen (ORM)

*Olycksriskmodellen (*ORM) ger möjligheter till ett systematiskt systemsäkerhetsarbete för att identifiera en eller flera olika åtgärder för riskreducering. Modellen kan under utvecklingsarbetet komplettera *Riskkällelista* (PHL) och/eller en *Riskkälleanalys (*PHA). Vid konstruktionsgranskning kan modellen ge argument och belägg till systemsäkerhetsvärderingen.

Genom att metodiskt gå igenom samtliga delar i *Olycksriskmodellen* (ORM) kan ett antal olika riskeliminerande/riskreducerande åtgärder identifieras för varje identifierad olycksrisk. Vissa åtgärder kan påverka skadeutfallet, andra åtgärder kan påverka sannolikhet/frekvens för inträffandet.

Genom att tillämpa nedanstående tabell kan förslag till riskreducerande åtgärder identifieras för respektive kolumn. Vissa åtgärder kan påverka flera olika faktorer i tabellen.

Komponent	Riskkälla	Scenario	Bidragande orsaker	Utlösande faktor	Vådahändelse	Exponering	Olycka
Lucka	Rörelseenergi	Frekvent använd materiel förvaras under luckan	Luckan saknar spärr i uppfällt läge	Luckan stöts ofrivilligt till, vind eller stormby	Luckan faller igen	Person	Personskada orsakad av fallande lucka
Förslag	*Förslag*	*Förslag*	*Förslag*	*Förslag*		*Förslag*	
Lucka i lättare material	Tillföra mjukstängande broms	Flytta materiel, vilket ger färre antal öppningar/stängningar av luckan	Tillföra mekanisk spärr som hindrar luckan från att falla	Luckan läggs ner från uppfällt läge för att undvika vindfång		Instruktion om att en person ska hålla i luckan i uppfällt läge	

Tabell 13.7 Exempel på tabell vid tillämpning av Olycksriskmodellen (ORM).

14 Riskmatris och tolerabel risknivå

Syftet med detta kapitel är att beskriva hur riskbedömning för olycksrisker kan ske mot en Tolerabel risknivå (TR) uttryckt i riskmatris utifrån grundmatriser för person, egendom och yttre miljö, samt framtagning av belägg för riskreduceringen efter åtgärd.

14.1 Grundmatris

Riskmatriser används för att redovisa olycksrisker som inte har kunnat omhändertas i de tidigare vägvalen (VV1–VV6) i *Vägvalsmodellen* (VVM).

Försvarsmakten ställer krav på att olycksrisker hanterade genom vägval (VV7) ska bedömas mot en *Tolerabel risknivå* (TR) uttryckt i riskmatris. Denna kan vara definierad för ett produktområde eller visst tekniskt system och infogas i *Systemsäkerhetsledningsplanen* (SSMP). Försvarsmaktens generella riskmatriser enligt avsnitten 14.3–14.5 tillämpas normalt, om inte särskilda skäl föreligger.

Systemmålsättning (SMS 2) ska referera till produktområdets *Systemsäkerhetsledningsplan* (SSMP) och behöver därför inte innehålla riskmatriser om inte anpassning varit nödvändig för aktuellt tekniskt system.

Nedanstående beskriver uppbyggnaden av en kvalitativ grundmatris.

Sannolikhet		Skadeklass			
		I	II	III	IV
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	ET	T	T
D	Ej trolig	ET	BT	T	T
E	Osannolik	BT	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 14.1 Kvalitativ grundmatris med Tolerabel risknivå (TR).

I riskmatrisen har färgerna följande betydelse:

- Röd Ej tolerabel (ET)
- Gul Begränsat tolerabel (BT)
- Grön Tolerabel (T)
- Blå Undanröjd

Riskmatriserna använder fyra definierade skadeklasser (I–IV) för konsekvens, där I är den allvarligaste skadeklassen. För definition av respektive skadeklass för person, egendom och miljö se avsnitten 14.3–14.5.

För sannolikhet används sex olika klasser (A–F), där A är den högsta sannolikheten. Nivå F (blått område) *Undanröjd* används enbart för att redovisa olycksrisker där skadeklassen inte är aktuell.

Sannolikhet klass	Benämning	Kvalitativ definition av sannolikhet för olycka under livslängden
A	Frekvent	Olyckan kan inträffa frekvent
B	Trolig	Olyckan kan inträffa flera gånger
C	Möjlig	Olyckan kan inträffa någon gång
D	Ej trolig	Olyckan kan inträffa enstaka gång
E	Osannolik	Olyckan kan inte antas inträffa någon gång
F	Undanröjd	Olyckan kan inte förekomma

Bild 14.2 Kvalitativa sannolikhetsklasser för ett exemplar av det tekniska systemet under livslängden.

Den markerade linjen mellan *Ej tolerabel* (ET) (rött område) och *Begränsat tolerabel* (BT) (gult område) definieras som *Tolerabel risknivå* (TR). Denna linje anger den övre gränsen för den risknivå som Försvarsmakten kan acceptera, utan att undantag från kravställningen i *Systemmålsättning* (SMS 2) behöver beviljas. Strävan är dock att alla hanterade olycksrisker efter det att riskreducerande åtgärder har införts ska ligga i *Tolerabelt* (T) (grönt område) eller i *Undanröjd* (blått område).

Försvarsmakten tillämpar en anpassad utformning av riskmatriser som ligger nära den som finns beskriven i standarden MIL-STD-882E. Riskmatriserna ska tillämpas för ett (1) exemplar av det tekniska systemet eller produkten.

14.2 Sannolikhets- respektive frekvensintervall

Vid kvantitativ bedömning av olycksrisk mot *Tolerabel risknivå* (TR) för vägval (VV7) kan nedanstående sannolikhetsintervall tillämpas om inte annat har angivits i produktområdets *Systemsäkerhetsledningsplan* (SSMP) eller i *Systemmålsättningen* (SMS 2) för aktuellt tekniskt system.

Sannolikhets-intervall	Benämning	Kvantitativ definition av sannolikhet (p) för olycka
A	Frekvent	$p \geq 10^{-1}$
B	Trolig	$10^{-2} \leq p < 10^{-1}$
C	Möjlig	$10^{-3} \leq p < 10^{-2}$
D	Ej trolig	$10^{-6} \leq p < 10^{-3}$
E	Osannolik	$p < 10^{-6}$
F	Undanröjd	Olyckan kan inte förekomma

Bild 14.3 Kvantitativa sannolikhetsintervall för ett exemplar av det tekniska systemet.

Sannolikhetsintervallen A–F överensstämmer med standarden MIL-STD-882E. Notera att intervallet D ($10^{-6} \leq p < 10^{-3}$) omfattar tre tiopotenser. För att omklassificera en olycksrisk förbi detta intervall krävs en riskreduceringsfaktor på mer än 10^{-3} för att underskrida *Tolerabel risknivå* (TR) enligt riskmatrisen för personskada.

De kvantitativa sannolikhetsintervallen avser sannolikheten för olycka per definierad aktivitet, exempelvis sannolikhet för olycka/skott eller olycka/laddning. Aktivitet ska väljas utifrån vad som tydligast kan koppla riskkällan till möjlig vådahändelse och olycka för aktuellt tekniskt system.

Detta medför att sannolikheten för vådahändelse är lika med sannolikheten för olycka vid exponeringen = 1, se Bild 13.1 *Olycksriskmodellen* (ORM). Om en modellering av sannolikhet för vådahändelse kan göras måste detta ske med trovärdiga och spårbara erfarenhetsdata. Ingår datorsystem och programvara i modelleringen måste dessa följa krav enligt fastställd kritikalitetsnivå. Se metodiken i Handbok för Programvara i säkerhetskritiska tillämpningar (H ProgSäk).

Om sannolikhetsintervallen ska räknas om mot ett frekvensintervall behöver de kvantitativa sannolikhetsintervallen enligt Bild 14.3 definieras mot maximalt

förväntade/accepterade antal olyckor under en angiven exponering, där exponeringen kan baseras på exempelvis antal avfyrningar, drifttimmar, antal körda kilometrar beroende på vad som är mest relevant för de identifierade olycksriskerna utifrån driftprofilen.

Om ett annat sannolikhetsintervall ska användas, eller omräknas till ett frekvensintervall, ska detta också framgå av *Systemmålsättning* (SMS 2) för aktuellt tekniskt system.

14.3 Riskmatris och skadeklasser för personskada

Försvarsmaktens riskmatris för personskada ska tillämpas för alla tekniska system och produkter om inte annat har överenskommits inom produktområdet eller för visst tekniskt system.

Sannolikhet		Skadeklass			
		I	II	III	IV
		Dödsfall	Allvarlig personskada	Mindre allvarlig personskada	Försumbar personskada
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	ET	T	T
D	Ej trolig	ET	BT	T	T
E	Osannolik	BT	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 14.4 Riskmatris för personskada.

Konsekvenser/skadeutfall för person avser oavsiktliga skador på:

- Försvarsmaktens egen personal
- Tredje person

Skadeklass	Personskada	Konsekvens
I	Dödsfall	En olycka som resulterar i enstaka eller flera dödsfall
II	Allvarlig personskada	En olycka som resulterar i en eller flera allvarliga personskador, där förlust av kroppsfunktion befaras
III	Mindre allvarlig personskada	En olycka som resulterar i en eller flera mindre allvarliga personskador, där de som utsätts förväntas bli återställda efter vård och rehabilitering
IV	Försumbar personskada	En olycka som resulterar i en eller flera lättare personskador, där de som utsätts blir helt återställda utan vård eller rehabilitering.

Bild 14.5 Definition av skadeklasser för personskada.

14.4 Riskmatris och skadeklasser för egendomsskada

Försvarsmaktens riskmatris för egendomsskada ska tillämpas för alla tekniska system och produkter om inte annat har överenskommits inom produktområdet eller för visst tekniskt system.

Sannolikhet		Skadeklass			
		I	II	III	IV
		Katastrofal egendomsskada	Kritisk egendomsskada	Allvarlig egendomsskada	Försumbar egendomsskada
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	BT	T	T
D	Ej trolig	BT	T	T	T
E	Osannolik	T	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 14.6 Riskmatris för egendomsskada.

Konsekvenser/skadeutfall för egendom avser oavsiktliga skador på:

- Försvarsmaktens tekniska system, produkter eller annan egendom, exempelvis anläggningar
- Tredje persons egendom (ej yttre miljö)

Beloppsintervallen för egendomsskada ska anpassas mot kostnaden för återanskaffning av aktuellt tekniskt system eller annan skada till ett belopp som motsvarar respektive skadeklass (inklusive system-av-system). Om återanskaffningskostnaden överstiger 100 mnkr så är detta beloppet för skadeklass I. Övriga beloppsintervall kan ansättas till 1/10 för varje skadeklass.

Skadeklass	Egendomsskada	Konsekvens beloppsintervall	Konsekvens
I	Katastrofal egendomsskada	≥ 100 mnkr	En olycka som resulterar i skada i paritet med total systemförlust (kassation) eller skada som gör det aktuella systemet obrukbart under en längre tid. Omfattande reparation eller utbyte krävs.
II	Kritisk egendomsskada	< 100 mnkr	En olycka som resulterar i skada som gör väsentliga delar av systemet obrukbart, men viss funktionalitet kan upprätthållas. Stora reparationsinsatser krävs.
III	Allvarlig egendomsskada	< 10 mnkr	En olycka som resulterar i skada som degraderar vissa funktioner, men systemets huvudfunktion bibehålls. Mindre reparationsinsatser krävs.
IV	Försumbar egendomsskada	< 1 mnkr	En olycka som resulterar i mindre skada som påverkar vissa funktioner, men systemet i stort kan fortfarande användas i väntan på reparation.

Bild 14.7 Definition av skadeklasser för egendomsskada inklusive tredje persons egendom.

14.5 Riskmatris och skadeklasser för miljöskada

Försvarsmaktens riskmatris för miljöskada ska tillämpas för alla tekniska system och produkter om inte annat har överenskommits inom produktområdet eller för visst tekniskt system.

Sannolikhet		Skadeklass			
		I	II	III	IV
		Katastrofal miljöskada	Kritisk miljöskada	Allvarlig miljöskada	Försumbar miljöskada
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	ET	T	T
D	Ej trolig	ET	BT	T	T
E	Osannolik	BT	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 14.8 Riskmatris för miljöskada.

Konsekvenser/skadeutfall för egendom avser oavsiktliga skador på:

– Yttre miljö som kan åtgärdas och repareras genom exempelvis sanering

Irreversibla (förödande) miljöskador undviks genom reglering av tillståndspliktig verksamhet och hanteras inom ramen för Försvarsmaktens hållbarhetsarbete. Tillåten arbetsmiljö- och miljöpåverkan såsom buller, utsläpp av föroreningar (emissioner) och energiförbrukning hanteras utanför systemsäkerhetsarbetet.

Beloppsintervallen för miljöskada anpassas mot bedömd kostnad för skadeklass I. Om den bedömda kostnaden för att genomföra sanering av miljön är 100 mnkr så är detta beloppet för skadeklass I. Övriga beloppsintervall kan ansättas till 1/10 för varje skadeklass.

Skadeklass	Egendomsskada	Konsekvens beloppsintervall	Konsekvens
I	Katastrofal Miljöskada	≥ 10 mnkr	En olycka som resulterar i en reversibel skada på miljön men med betydande miljöpåverkan. Mycket omfattande sanering erfordras
II	Kritisk Miljöskada	< 10 mnkr	En olycka som resulterar i en reversibel skada på miljön med stor miljöpåverkan. Omfattande sanering erfordras
III	Allvarlig Miljöskada	< 1 mnkr	En olycka som resulterar i en reversibel skada på miljön med mindre miljöpåverkan. Mindre sanering erfordras
IV	Försumbar Miljöskada	< 0,1 mnkr	En olycka som resulterar i en reversibel skada på miljön med obetydlig miljöpåverkan. Sanering oftast inte nödvändig

Bild 14.9 Definition av skadeklasser för miljöskada.

14.6 Riskmatris, kriterier för belägg av riskreducering

För en olycksrisk, vilken före åtgärd bedöms hamna i *Ej tolerabelt* (ET) rött område eller i *Begränsat tolerabelt* (BT) gult område i riskmatrisen, ska de riskreducerande åtgärderna redovisas som belägg för att kunna flytta dessa i riskmatrisen efter åtgärd. Åtgärder kan bestå av konstruktionsåtgärder som minskar sannolikheten för vådahändelse och därmed i motsvarande grad olycksrisken.

Om konstruktionsåtgärder kan eliminera eller kapsla in riskkällan, undanröjs olycksrisken helt. Konstruktionsåtgärder kan även ha inverkan på de bidragande orsakerna eller hindra de utlösande faktorerna.

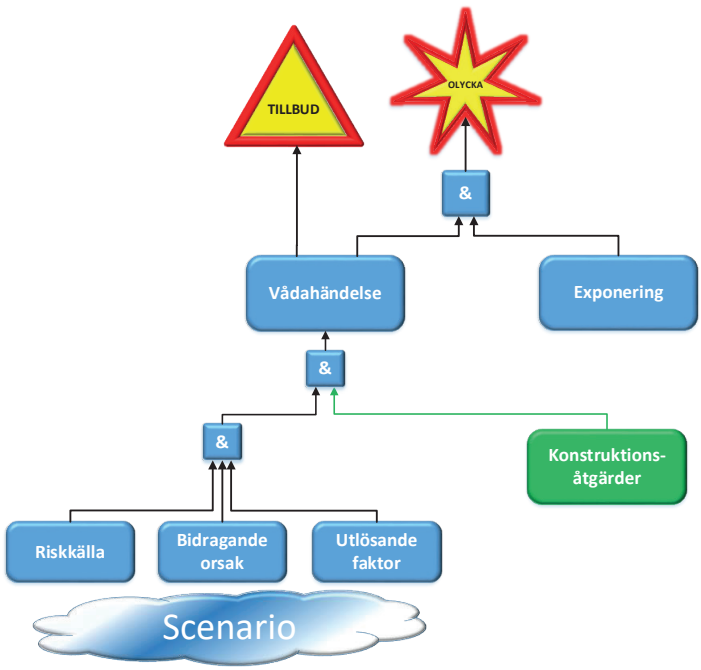


Bild 14.10 *Riskreducering med konstruktionsåtgärd.*

Om konstruktionsåtgärderna inte bedöms tillräckliga kan även varningsanordningar, personlig skyddsutrustning (PPE) eller begränsningar i användning

införas som då minskar exponeringen och därmed kan ses som ytterligare ett villkor som reducerar olycksrisken.

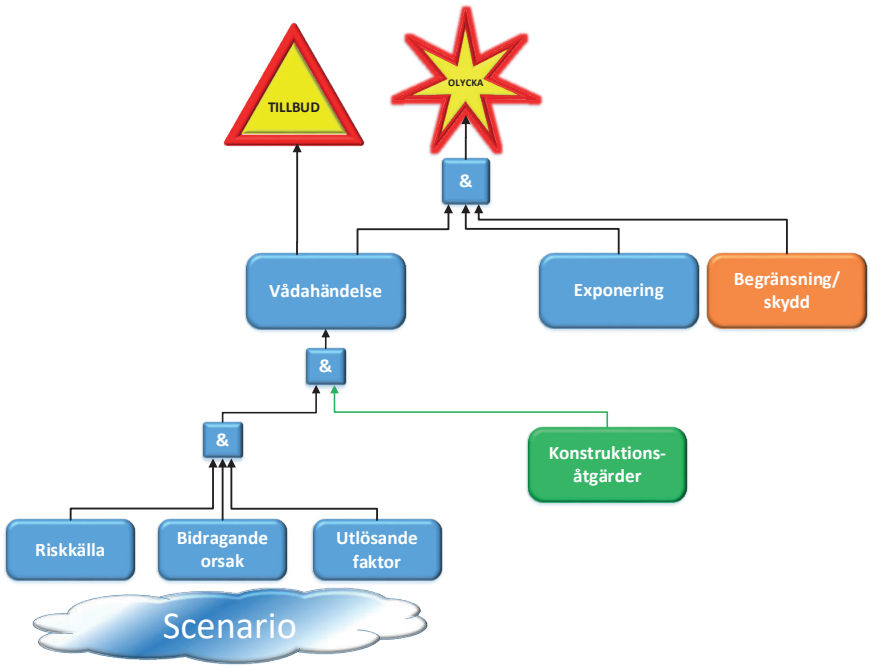


Bild 14.11 Riskreducering med konstruktionsåtgärder och begränsning/skydd.

14.6.1 Redovisning av konstruktionsåtgärder

För varje hanterad olycksrisk i riskmatrisens röda (ej tolerabelt) eller gula (begränsat tolerabelt) område ska konstruktionsåtgärder redovisas som kan påvisa att det krävs ytterligare minst ett &-villkor för att vådahändelse ska kunna inträffa för exempelvis IIC till IIE. Dessa åtgärder medför en förflyttning vertikalt i riskmatrisen. Konstruktionsåtgärder som ger ökad säkerhetsmarginal kan även betraktas som ett &-villkor.

Sannolikhet		Skadeklass			
		I	II	III	IV
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	ET	T	T
D	Ej trolig	ET	BT	T	T
E	Osannolik	BT	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 14.12 Riskreducering i riskmatris.

I bild 14.13 nedan har konstruktionsåtgärder redovisats som är oberoende &-villkor vid samtidiga fel för att en vådahändelse ska inträffa. Konstruktionsåtgärder kan ha påverkan på riskkällan, bidragande orsaker eller utlösande faktorer, men redovisas i bilden nedan förenklat som tillkommande &-villkor för att vådahändelsen ska kunna inträffa.

Vid en kvantitativ systemsäkerhetsanalys ska redovisning också omfatta en redovisning som visar att införda konstruktionsåtgärder också medför risk-reducering som motsvarar sannolikhetsintervallet i riskmatrisen efter åtgärd. Det vill säga för ändringen från IIC till IIE medför krav att kunna redovisa en riskreduceringsfaktor på mer än 10^{-3} jämfört med ändringen från IIIA till IIIC som medför ett krav på riskreduceringsfaktor på mer än 10^{-2}.

För att erhålla en erforderlig riskreducering kan således flera konstruktionsåtgärder bli nödvändiga. Varje konstruktionsåtgärd ska kunna visas vara oberoende för att modellen nedan ska vara giltig. Finns trovärdiga erfarenhetsdata kan dessa användas för att beräkna en felsannolikhet, annars får en uppskattning göras (konservativ ansättning) på vad konstruktionsåtgärden kan bedömas tillföra. Om ett antagande görs för en riskreducering för en konstruktionsändring så bör den inte ansättas ett värde som medför en riskreduceringsfaktor på mer 10^{-1}. Om en större riskreducering krävs måste denna kunna styrkas.

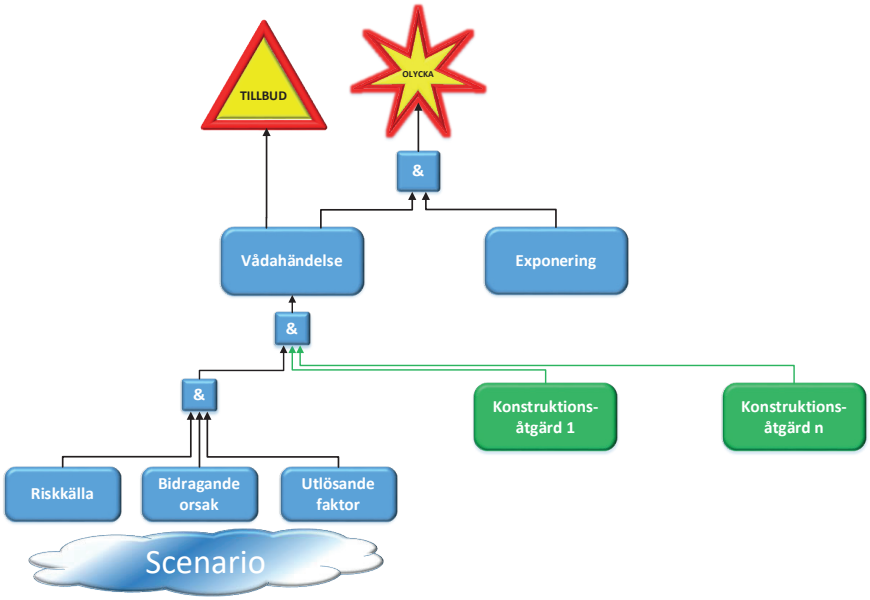


Bild 14.13 Riskreducering med konstruktionsåtgärder.

14.6.2 Redovisning av reducerad exponering

Om införda konstruktionsåtgärder inte bedöms medföra tillräcklig riskreducering kan faktorer som påverkar exponeringen vid vådahändelse införas.

Denna typ av åtgärder kan exempelvis vara skydd, förändrad arbetssätt eller begränsning i användning. Dessa åtgärder reducerar främst skadeklassen (konsekvensen), det vill säga medför en förflyttning horisontellt efter åtgärd i riskmatris.

Sannolikhet		Skadeklass			
		I	II	III	IV
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	ET	T	T
D	Ej trolig	ET	BT	T	T
E	Osannolik	BT	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 14.14 Riskreducering med konstruktionsåtgärder och reducerad exponering.

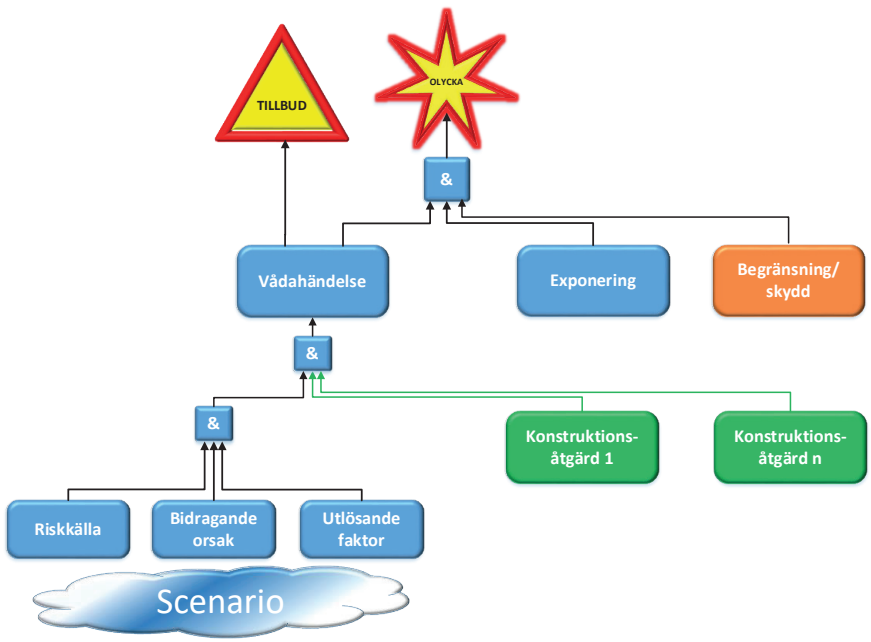


Bild 14.15 Riskreducering med konstruktionsåtgärder och reducerad exponering.

15 Olycksriskvärdering och klassificering

Syftet med detta kapitel är att beskriva hur riskvärdering och klassificering av olycksrisker kan genomföras samt hur stängning av systemsäkerhetsarbetet för enskilda olycksrisker kan utföras.

15.1 Grundprinciper för ALARP över kvarstående olycksrisker

Inför det att Försvarsmakten ska ta nya eller ändrade (modifierade) tekniska system i bruk behöver noggranna överväganden ske för kvarstående olycksrisker. Det innebär att alla identifierade olycksrisker till sin art ska vara kända och dokumenterade, vid behov reducerade och att acceptansbeslut för var och en av dem ska vara fattat.

Försvarsmakten ställer krav på att riskbedömning ska ske för kvarstående olycksrisker som inte har omhändertagits i vägval (VV1–VV6) mot en *Tolerabel risknivå* (TR) uttryckt i riskmatris. Samtidigt eftersträvas att alla riskreducerande åtgärder som bedöms vara effektiva för riskreducering vidtas, oavsett var olycksrisken är klassificerad i riskmatrisen.

Principen att varje kvarstående olycksrisk ska vara så låg som möjligt kallas allmänt för ALARP (*As Low as Reasonably Practicable*). Begreppet rimligen praktiskt genomförbart innebär att man väger en olycksrisk mot de problem, den tid och de pengar som behövs för att reducera den. Det finns dock olika sätt att definiera så låg som möjligt och begreppet behöver därför oftast ställas i relation till något annat. Med så låg som möjligt kan en olycksrisk anses vara reducerad till en tillräckligt låg risknivå om god praxis har följts. Med det menas bland annat att etablerade standarder och *Designregler* (DR) har följts utifrån dagens teknriknivå.

För att kunna bedöma om ytterligare riskreducerande åtgärder rimligen och praktiskt är genomförbara kan följande beaktas och avdömas:

- Påvisbart riskreducerande om de genomförs
- Prestandadegradering är avvägd och acceptabel i relation till säkerhetshöjningen
- Ekonomiskt försvarbara i jämförelse med den statistiskt beräknade olyckskostnaden
- Enkelt realiserbara och att leveransförseningar kan undvikas

Oftast är det en kombination av ovanstående punkter som avgör om det är en tillräcklig argumentation för ALARP. Normalt tillämpas ALARP för olycksrisker som klassificerats inom *Begränsat tolerabel* (BT) (gult område).

15.2 Klassificering av olycksrisk före riskreducering

Under konstruktionsarbetet av ett tekniskt system eller produkt identifierar *konstruktören* ett antal olycksrisker. Olycksriskerna värderas initialt utifrån vilka konsekvenser som kan inträffa. Genom en iterativ process inleds *konstruktörens* arbete med strävan att eliminera olycksriskerna.

Vissa olycksrisker kan konstrueras bort och andra kan reduceras. Vissa olycksrisker kan anses vara omhändertagna genom att de helt eller delvis hanterats genom vägval (VV1–VV6). Övriga olycksrisker och de som delvis hanterats genom vägval (VV1–VV6) ska riskbedömas utifrån konsekvens/skadeutfall och sannolikhet/frekvens. De ska därefter klassificeras i kravställda riskmatriser för person, egendoms och yttre miljö genom vägval (VV7) och redovisas för *beställaren*.

När *konstruktören* anser att det tekniska systemet eller produkten är klar för *beställarens* första konstruktionsgranskning presenteras även samtliga kvarstående olycksrisker före riskreducering på överenskommet sätt. *Beställaren* kan under konstruktionsgranskningen anföra synpunkter på både konstruktionen och klassificeringen av olycksriskerna.

Olika systemsäkerhetsstandarder anger skilda principer för vad som kan presenteras avseende kvarstående olycksrisk. Det kan vara *värsta tänkbara* konsekvens, *värsta troliga* konsekvens eller *oftast befarad* konsekvens. Oavsett redovisningsmetod ovan anger detta bara en delmängd av de befarade konsekvenserna om en olycka inträffar. Försvarsmakten rekommenderar en metod där samtliga skadeklasser i riskmatrisen presenteras för varje enskild olycksrisk. Förslag på metod finns i avsnitt 15.8.1.

15.3 Val av riskreducerande åtgärder

Efter klassificering av de kvarstående olycksriskerna kan vissa olycksrisker vara nödvändiga att åtgärda, medan andra olycksrisker kan reduceras ytterligare i enlighet med grundprinciperna för ALARP. För var och en av de kvarstående olycksriskerna för person-, egendoms- och miljöskada ska förslag på riskreducerande åtgärder, inklusive skattad effekt, tas fram och dokumenteras.

Om en olycksrisk klassificeras som *Ej tolerabel* (ET) (rött område) ska riskeliminering/-reducering ske för att underskrida krav på *Tolerabel risknivå* (TR). För olycksrisker som klassificeras som *Begränsat tolerabel* (BT) (gult område) eller *Tolerabel* (T) (grönt område) bör åtgärder vidtas om dessa bedöms stå i proportion till skattad effekt för riskreducering i enlighet med grundprinciperna för ALARP.

I vissa fall kan verksamhetsregler hantera olycksrisker då det inte är önskvärt att begränsa funktionalitet som motverkar säkerheten i det tekniska systemet.

Varje förslag till riskreducerande åtgärd för en enskild olycksrisk behöver värderas med hänsyn till om det är konsekvens/skadeutfall och/eller sannolikhet/frekvens som berörs. Det är eftersträvansvärt att hitta riskreducerande åtgärder så att olycksrisken helt elimineras.

Det är dock få riskreducerande åtgärder som har positiv påverkan på både konsekvens/skadeutfall och sannolikhet/frekvens. Om det bedömda antalet olyckor som befaras att inträffa är konstant så påverkas skadeklasserna inbördes. Om en skadeklass elimineras så måste övriga skadeklasser värderas om. Detta

gäller även om sannolikheten för en skadeklass minskar så kan sannolikhet/frekvens för en eller flera av de övriga skadeklasserna öka.

När en riskreducerande åtgärd införs på det tekniska systemet ska olycksrisken på nytt värderas ur systemsäkerhetssynpunkt. Riskreduceringen ska styrkas och systemsäkerhetsanalysen ska även säkerställa att vald åtgärd för riskreducering inte medför någon höjning av risknivå på annan tidigare identifierad olycksrisk eller att dess riskkällor innebär nya olycksrisker.

Olika systemsäkerhetsstandarder har varierande prioriteringar för riskreducerande åtgärder. Gemensamt för dessa är dock preferensordningen; konstruera (olycksrisker ska så långt som möjligt undanröjas eller reduceras), skydda (nödvändiga skyddsåtgärder ska vidtas för sådana olycksrisker som inte kan undanröjas) och varna (information ska ges till användarna om kvarstående olycksrisker).

Följande prioriteringsordning kan vara lämplig vid val av en eller flera åtgärder:

- Eliminera eller byta till mindre farliga riskkällor
- Genomföra omkonstruktion
- Införa skyddsanordningar
- Införa varningsanordningar
- Tillföra personlig skyddsutrustning (PPE)
- Ta fram instruktioner, skyltar, dekaler
- Genomföra utbildning

Införande av en eller flera riskreducerande åtgärder innebär inte med automatik att olycksrisken erhåller en lägre klassificering. Alla förflyttningar i riskmatrisen efter införande av riskreducerande åtgärder ska kunna härledas med argument och belägg.

Vid ändring (modifiering) av tekniska system och produkter som tidigare har använts inom Försvarsmakten, ska nya olycksrisker som identifierats i samband med ändringen, underskrida *Tolerabel risknivå* (TR) samt att modifieringen inte bedöms medföra någon påtaglig höjning av risknivå på annan tidigare hanterad olycksrisk.

Om nya olycksrisker klassificerats som *Begränsat tolerabel* (BT) (gult område) eller *Tolerabel* (T) (grönt område) bör riskreducerande åtgärder vidtas om dessa bedöms stå i proportion till skattad effekt för riskreducering i enlighet med grundprinciperna för ALARP.

En tumregel är att nya olycksrisker som klassificerats som *Begränsat tolerabel* (BT) eller som *Tolerabel* (T) åtgärdas om dessa olycksrisker bedöms som allvarligare än för andra motsvarande kvarstående olycksrisker i det ursprungliga tekniska systemet.

15.3.1 Konstruktionsinriktade åtgärder

- Eliminera eller byta till mindre farliga riskkällor
- Genomföra omkonstruktion

Konstruktionsinriktade åtgärder kan minska både konsekvens och sannolikhet.

En riskkälla är något som kan orsaka skada på person, egendom eller yttre miljö genom dess farliga egenskaper. En komponent kan ha en eller flera olika riskkällor, exempelvis energi eller emissioner. Nära anslutet till riskkälla finns begreppen *funktionell riskkälla* samt *farligt tillstånd*, vilka oftast kan ses som bidragande orsaker till att en olycka inträffar. I vissa fall kan avvikelser i konstruktionsarbetet betraktas som ett *farligt tillstånd*, exempelvis ett fel i en programvara.

I första hand ska en konstruktionslösning som innehåller en särskilt farlig riskkälla elimineras och ersättas av annan konstruktion med en mindre farlig riskkälla. I andra hand kan den valda riskkällan minskas eller delas upp, exempelvis genom reduktion av volym eller mängd, minskad höjd eller storlek, utan att göra oacceptabla inskränkningar på det tekniska systemets funktioner och prestanda.

Riskkällan utgör ofta det tekniska systemets primära funktion, exempelvis strålning från en antenn, det explosiva ämnet i ammunition eller rörelseenergin i en funktion, och kan därför vara svår att reducera eller byta ut utan att det tekniska systemet förlorar sin prestanda.

Om riskkällan inte går att eliminera kvarstår identifierade olycksrisker, men andra åtgärder kan införas för att reducera dem. Dessa åtgärder kan vara tekniska,

administrativa eller organisatoriska och dessa åtgärder kan i sin tur reducera olycksrisken genom att vara förebyggande, det vill säga reducera sannolikheten för en olycka eller begränsa konsekvensen/skadeutfallet, om olyckan ändå skulle inträffa.

Med omkonstruktion menas en konstruktionsinriktad åtgärd för minskad exponering genom att permanent (helt eller delvis) avskilja eller kapsla in riskkällan på ett sätt som minskar sannolikheten att dess farliga egenskaper inte oavsiktligt exponeras för person, egendom eller yttre miljö.

Omkonstruktion kan även omfatta konstruktionsåtgärder som medför minskad sannolikhet för att vådahändelsen inträffar. Vidare kan det tekniska systemet behöva skyddas från påverkan av naturkrafter såsom blixtnedslag och statisk elektricitet. I begreppet omkonstruktion ingår även automation i syfte att ta bort farliga arbetsmoment samt att införa olika typer av säkerhetsfunktioner.

15.3.2 Skyddsinriktade åtgärder

- Införa skyddsanordningar
- Tillföra personlig skyddsutrustning (PPE)

Skyddsinriktade åtgärder kan minska både konsekvens och sannolikhet.

Med skyddsanordning menas en konstruktionsdetalj vars enda funktion är att skydda användaren direkt eller indirekt från riskkällan.

Med personlig skyddsutrustning (PPE) menas sådana skydd som inte tillhör det tekniska systemet eller produkten och som den enskilde användaren själv tillför för att skydda sig. Exempel på personlig skyddsutrustning är hörselskydd, skyddsmask, hjälm, skyddsglasögon, kläder, handskar och skor. Även om dessa skydd må vara effektiva för att undvika olyckor eller ohälsa kan skyddsutrustning ha en negativ påverkan på andra områden såsom funktion och prestanda. Skyddsinriktade åtgärder vidtas först efter det att möjligheter till konstruktionsinriktade åtgärder, inte längre är möjliga eller tillräckliga.

15.3.3 Varnings- och informationsinriktade åtgärder

- Införa varningsanordning
- Ta fram instruktioner, skyltar, dekaler
- Genomföra utbildning

Varnings- och informationsinriktade åtgärder minskar främst konsekvensen.

Med varningsanordning menas ett övervakande system som aktivt larmar om en farlig situation är på väg att inträffa eller just har inträffat. Varningsanordningar kan vara optiska, akustiska eller som genom vibrationer i manöverdon syftar till att påkalla användarens uppmärksamhet.

Med instruktioner, skyltar och dekaler menas information som passivt upplyser användaren om att det finns riskkällor och att farliga tillstånd kan inträffa. Till denna kategori hör även instruktioner eller annan begränsning i användandet såsom definierade riskområden för ammunition eller radarstrålning som påverkar exponeringen.

Med utbildning avses att ge förkunskaper och träning för säker användning och underhåll av det tekniska systemet eller produkten.

Varnings- och informationsinriktade åtgärder kan vara effektiva för att undvika olyckor eller ohälsa men först efter det att konstruktions- och skyddsinriktade åtgärder inte längre är möjliga eller tillräckliga.

För skadeklass I (katastrofala) och skadeklass II (kritiska) där konstruktionen inte följt god praxis är riskreducering med enbart personlig skyddsutrustning (PPE), instruktioner, skyltar, dekaler, utbildning, eller en kombination av dessa, inte tillräcklig

Provning är i sig inte någon riskreducerande åtgärd, men kan till del verifiera en funktion eller en sekvens för säker funktion om en vådahändelse inträffar.

15.4 Klassificering av olycksrisk efter riskreducering

När *beställaren* har anfört synpunkter på både konstruktionen och klassificeringen av olycksriskerna vid en första konstruktionsgranskning vidtar *konstruktören* riskreducerande åtgärder. *Konstruktören* gör en ny klassificering av kvarstående olycksrisker efter riskreducering på överenskommet sätt. *Beställaren* kan under kommande konstruktionsgranskningar anföra nya synpunkter. Förslag på metod finns i avsnitt 15.8.2.

15.5 Exponerings- och styrbarhetsfaktorer

När *beställaren* och *konstruktören* gemensamt anser att de möjliga konstruktions- och skyddsinriktade åtgärderna är vidtagna kan exponerings- och styrbarhetsfaktorer tillämpas som argument och belägg för att visa att sannolikheten för olycka rimligtvis är lägre.

Exponerings- och styrbarhetsfaktorer används endast för personskador och inte för egendoms- och miljöskador. Med exponeringsfaktor menas att användaren inte alltid finns närvarande när en vådahändelse inträffar. Med styrbarhetsfaktorer menas att användaren själv kan påverka ett farligt tillstånd genom att stoppa händelsekedjan eller ta visst skydd innan vådahändelsen inträffar.

Om användaren är helt eller delvis skyddad när en vådahändelse inträffar kan sannolikhet/frekvens för inträffad olycka minskas. Detta gäller även om användaren i tid kan upptäcka eller uppmärksammas på att en olycka är nära förestående och därmed hinner stoppa händelsekedjan eller ta visst skydd. Användaren kan då erhålla en lägre exponeringsfaktor än = 1 när vådahändelsen inträffar. Vid användning av exponeringsfaktor vid riskvärdering ska detta särskilt anges.

Exponeringsfaktorer får endast användas som komponent för att tillgodoräkna sig en minskad sannolikhet/frekvens för att personer skadas vid en olycka.

Vid riskvärdering före åtgärd ska exponeringsfaktorn vara = 1, vilket innebär att denna faktor endast kan tillgodoräknas som ett andra steg efter införande av riskreducerande åtgärder.

15.6 Ny klassificering av olycksrisk efter exponeringsfaktorer

Som ytterligare ett steg, om valda riskreducerande åtgärder ändå inte anses vara tillräckliga, kan uppskattade exponerings- och styrbarhetsdata för person tillgodoräknas vid beräkningar eller bedömningar kring olycksrisker.

Om riskkällan är vald kan övriga förutsättningar påverkas i konstruktionsarbetet och senare även i den avsedda användningen:

- Reducering av bidragande orsaker och utlösande faktorer till vådahändelsen
- Reducering av sannolikhet för exponering av personer
- Ökning av möjligheten för att upptäcka och kontrollera progressen innan vådahändelsen inträffar. I standarder benämnt som styrbarhet eller kontrollerbarhet
- Reducering av konsekvenser om olyckan ändå skulle inträffa

Genom att tillämpa *Olycksriskmodellen* (ORM) kan olika givna omständigheter påverkas vid konstruktionen av det tekniska systemet eller produkten.

15.7 Stängning av systemsäkerhetsarbetet för en olycksrisk

Systemsäkerhetsarbetet för en enskild olycksrisk som har klassificerats i en riskmatris kallas för öppen intill dess att de införda riskreducerande åtgärderna bedöms vara tillräckliga. Olycksrisken redovisas både skadeklassvis och med högsta skadeklass. Olycksriskens högsta skadeklass blir därmed styrande för den fortsatta hanteringen.

- För en olycksrisk som har minst en av de aktuella skadeklasserna inom *Ej tolerabel* (ET) (rött område) bedöms hela olycksrisken som *Ej tolerabel* (ET).
- För en olycksrisk som inte finns i rött område *Ej tolerabel* (ET), men som har minst en av de aktuella skadeklasserna inom *Begränsat tolerabel* (BT) (gult område) bedöms hela olycksrisken som *Begränsat tolerabel* (BT).
- För en olycksrisk som har alla de aktuella skadeklasserna inom *Tolerabel* (T) (grönt område) bedöms hela olycksrisken som *Tolerabel* (T).

Eftersom den högsta skadeklassen i exemplet nedan är röd innebär det att hela olycksrisken är *Ej tolerabel* (ET) och att ytterligare riskreducerande åtgärder behöver vidtas.

Klassificering (skadeklass/sannolikhet)	Skadeklassvis	Högsta skadeklass
ID		
IID		
IIIC		
IVB		

Bild 15.1 Exempel på redovisning skadeklassvis för en viss olycksrisk.

Om den högsta skadeklassen efter införda riskreducerande åtgärder är:

- Röd, ska *beställaren* skicka en hemställan med begäran om avsteg från *Tolerabel risknivå* (TR) till *kravställaren*. *Kravställaren* kan godkänna eller avvisa hemställan.
- Gul, ska *beställaren* förvissa sig om att den högsta skadeklassen av olycksrisken bedöms rymmas inom *Tolerabel risknivå* (TR) genom att granska att argument och belägg samt att de särskilt ställda kraven på ALARP avseende gula cellerna är uppfyllda. *Beställaren* kan bifalla, eller begära förtydliganden av *konstruktören*
- Grön, ska *beställaren* förvissa sig om att den högsta skadeklassen av olycksrisken bedöms rymmas inom *Tolerabel risknivå* (TR) genom att granska argument och belägg. *Beställaren* kan bifalla, eller begära förtydliganden av *konstruktören*.

Systemsäkerhetsarbetet för en enskild olycksrisk kan stängas när man har förvissat sig om att alla skadeklasser av olycksrisken bedöms rymmas inom *Tolerabel risknivå* (TR) eller att *kravställaren* har godkänt avsteg från kravställningen. Detta sker i samförstånd mellan *beställare* och *konstruktör* när argument och belägg för den enskilda olycksrisken är dokumenterad i *Systemsäkerhetsrapporten* (SAR) och *Riskloggen* (RL).

Olycksrisker som bedöms rymmas inom *Tolerabel risknivå* (TR) eller att *kravställaren* har godkänt avsteg från kravställningen benämns hanterade.

Olycksrisker där de riskreducerande åtgärderna ännu inte är införda och som därmed följs av restriktioner benämns kvarstående.

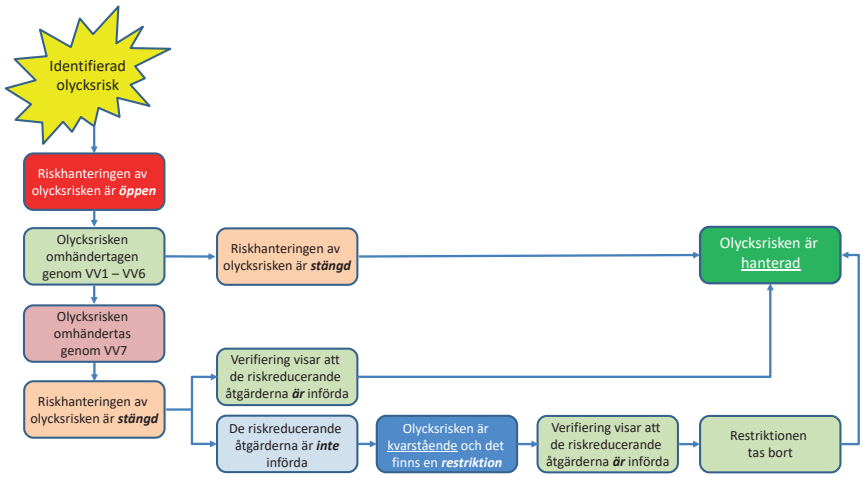


Bild 15.2 *Hanterad respektive kvarstående olycksrisk.*

15.8 Metod för klassificering av olycksrisk

Nedan beskrivs en metodik och arbetsgång för att klassificera och presentera det bedömda utfallet av hela olycksrisken.

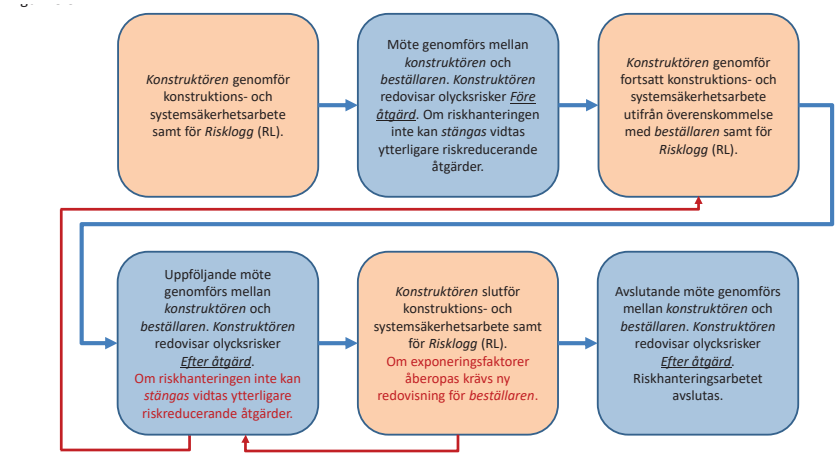


Bild 15.3 Arbetsgång vid riskreducering av olycksrisk.

15.8.1 Klassificering av olycka före riskreducering

När det tekniska systemet eller produkten är klar för en första konstruktionsgranskning ska samtliga kvarstående olycksrisker före riskreducering redovisas. Detta avser olycksrisker vilka hanteras med vägval (VV7) och kan genomföras enligt nedan angivna metod.

Klassificera en olycksrisk genomförs ett antal steg där använda data, gjorda antaganden och bedömda resultat dokumenteras.

1. Formulera olycksrisken för person, egendom respektive yttre miljö.
   Tillämpa råden i avsnittet Olycka under Olycksriskmodellen (ORM).
   – *Personskada vid… orsakad av/på grund av/vållad av…*
   – Egendomsskada vid… orsakad av/på grund av/vållad av…
   – *Miljöskada vid… orsakad av/på grund av/vållad av…*

2. Beskriv olycksriskens tänkta scenario och händelseförlopp.
   Tillämpa råden i avsnittet Scenario under Olycksriskmodellens (ORM).

3. Uppskatta hur ofta/många gånger olyckan kan inträffa utifrån driftprofil och livslängd.
   För detta kan Expertbedömningar eller Modelleringar användas.

4. Skriv ner alla tänkbara konsekvenser (skador på person, egendom respektive yttre miljö) som kan inträffa.
5. Tänk att olyckan inträffar 100 gånger (eller 1000) och uppskatta hur ofta de olika konsekvenserna kan tänkas inträffa och gör en procentuell fördelning mellan skadeklasserna.

Detta görs för person, egendom och yttre miljö, men exemplifieras enbart med bilden för personskada nedan. För skadeklasser som inte bedöms kunna inträffa sätts värdet till ”0%” och redovisas som ”Undanröjd” i riskmatrisen.

Skadeklass	Personskada	Fördelning i %
I	Dödsfall	*a*
II	Allvarlig personskada	*b*
III	Mindre allvarlig personskada	*c*
IV	Försumbar personskada	*d*
Summa:		*= 100 %*

Bild 15.4 *En procentuell fördelning av konsekvens/skadeutfall redovisas för en viss enskild olycksrisk för personskada före riskreducering*

6. För in resultatet i riskmatriserna för person, egendom respektive yttre miljö. *Detta görs för person, egendom och yttre miljö, men exemplifieras enbart med riskmatrisen för personskada nedan.*

Sannolikhet		Skadeklass			
		I	II	III	IV
		Dödsfall	Allvarlig personskada	Mindre allvarlig personskada	Försumbar personskada
A	Frekvent	ET	ET	ET	BT
B	Trolig	ET	ET	BT	T
C	Möjlig	ET	ET	T	T
D	Ej trolig	ET	BT	T	T
E	Osannolik	BT	T	T	T
F	Undanröjd	*Undanröjd*	*Undanröjd*	*Undanröjd*	*Undanröjd*

Bild 15.5 *Sannolikhet och konsekvens/skadeutfall redovisas för samtliga skadeklasser för en viss enskild olycksrisk för personskada före riskreducering.*

7. Dokumentera använda data, gjorda antaganden och bedömda resultat i *Systemsäkerhetsrapporten* (SAR) och i *Riskloggen* (RL).

15.8.2 Klassificering av olycka efter riskreducering

Riskvärdering och klassificering efter riskreducerande åtgärder, sker på samma sätt som riskvärdering och klassificering före åtgärd. Riskvärdering efter åtgärd genomförs ytterligare en gång efter att de riskreducerande åtgärderna är införda och verifierade. Detta för att belägga att den tänkta effekten av riskreduceringen har infriats samt för att säkerställa att inga andra olycksrisker har påverkats negativt, att inga nya olycksrisker har tillförts och att balans erhålls mellan funktion och systemsäkerhet.

Även för olycksrisker som inte krävt någon riskreducerande åtgärd görs en förnyad riskvärdering för att bekräfta klassificeringen.

För att kunna göra en ny klassificering av en olycksrisk efter införande av riskreducerande åtgärder genomförs steg 8–12 där använda data, gjorda antaganden och bedömda resultat dokumenteras.

8. Identifiera olika förslag till riskreducerande åtgärder. Notera om förslagen påverkar sannolikhet/frekvens, konsekvensen eller både sannolikhet/frekvens och konsekvens.
9. Undersök om nya olycksrisker uppstår om viss riskreducerande åtgärd införs.
10. Fundera igenom om tidigare identifierade olycksrisker påverkas om viss riskreducerande åtgärd införs.
11. Välj riskreducerande åtgärd/åtgärder och upprepa steg 3–10 i avsnitt 15.8.1 tills önskvärd uppskattad riskminskning har uppnåtts.
12. Om den/de valda riskreducerande åtgärden/åtgärderna ändå inte är tillräckliga kan exponerings- och styrbarhetsfaktorer för personskador tillämpas. Upprepa steg 5–7 i avsnitt 15.8.1 tills önskvärd uppskattad riskreducering har uppnåtts.

16 Systemsäkerhetsvärdering

Syftet med detta kapitel är att visa hur olika aktörer genom systemsäkerhetsvärdering kan bygga upp och motivera hur betryggande säkerhet för tekniska system och produkter har uppnåtts. Systemsäkerhetsvärderingen används sedan som grund för ett hållbart ställningstagande i aktuellt systemsäkerhetsbeslut.

16.1 Genomförande av systemsäkerhets-värdering

Efter genomfört konstruktions- och/eller integrationsarbete sker verifiering respektive validering mot ställda krav för komponenter, produkter, delsystem och tekniska system uppströms av de olika aktörerna. Strävan är att finna argument och belägg starka nog för att kunna visa att betryggande säkerhet har uppnåtts mot kraven i aktuellt kravdokument.

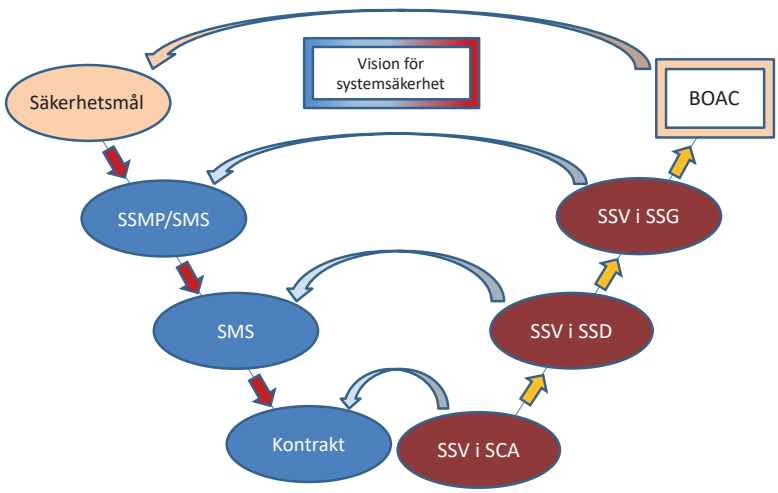


Bild 16.1 *Systemsäkerhetsvärderingen ska visa att systemsäkerhetskraven är uppfyllda i motsvarande kravdokument.*

De tillåtna vägvalen kan behöva omprövas om det visar sig att argument och belägg bedöms som för svaga för att kunna visa att ställda systemsäkerhetskrav är uppfyllda. Exempelvis kan ett godkännande mot en viss standard från ett

oberoende certifieringsorgan betraktas som starkare (objektivt bevis), än ett uttalande som grundar sig på egenverifiering mot samma standard. Vidare kan en systemsäkerhetsanalys med hjälp av ett felträd som visar att enkelfel inte kan inträffa betraktas som starkare än att åberopa drifterfarenheter från liknande tekniska system.

Argument som baseras på gjorda antaganden utifrån Försvarsmaktens verksamhet ska redovisas. Exempelvis kan etablerade arbetssätt såsom att soldaten alltid bär hjälm i ett stridsfordon vara ett sant antagande som kan åberopas. Argument som att användaren inte bedöms kunna göra vissa fel är däremot falska och får inte förekomma.

Systemsäkerhetsvärderingen är uppbyggd av argument och belägg hämtade från de tillämpade vägvalen (VV1–VV7) och ska formuleras av respektive aktör i dennes systemsäkerhetsbeslut samt vara strukturerat enligt nedan:

”Det tekniska systemet (produkten) är säkert därför att:”
– ...
– ...
– ...

Systemsäkerhetsvärderingen ska sammantaget visa vilken EU-rätt och svensk lagstiftning som är uppfylld och att ställda krav på systemsäkerhet är uppfyllda.

Systemsäkerhetsvärderingen kan redovisas i *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL) eller direkt i aktuellt systemsäkerhetsbeslut.

Försvarsmaktens definitiva ställningstagande om att det tekniska systemet eller produkten för avsedd användning är tillräckligt säker för att tas i bruk görs genom systemsäkerhetsbeslut, oftast i *Beslut om användning, central nivå* (BOAC).

16.2 Konstruktörens systemsäkerhetsvärdering

Med *konstruktör* avses den som utvecklar/tillverkar tekniska system och produkter utifrån lagstiftning och kontrakt och som därmed har ett produktsäkerhetsansvar enligt EU-direktiv/motsvarande. I EU-direktiven är detta den legale tillverkaren.

Inför leverans redovisar *konstruktören* ställningstagandet i *Systemsäkerhetsutlåtandet* (SCA) utifrån kontraktet och de förtydliganden och/eller justeringar som kan ha skett vid kontraktsgenomgången. Ställningstagandet är uppbyggt av argument och belägg hämtade från de tillämpade vägvalen (VV1–VV7), vilka redovisas i systemsäkerhetsvärderingen.

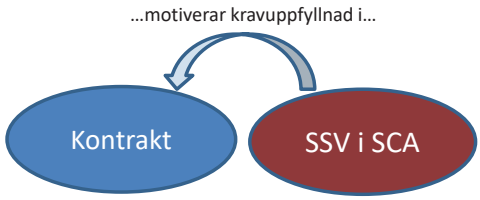


Bild 16.2 *Konstruktörens systemsäkerhetsvärdering ska visa att systemsäkerhetskraven i kontraktet är uppfyllda.*

16.2.1 SSV Vägval 1 – Författningsenliga krav

Med författningsenliga krav avses EU-rätt och svensk lagstiftning med sina förordningar och föreskrifter. Hit räknas även de harmoniserade standarderna som, när deras mer detaljerade krav uppfylls, presumeras uppfylla författningarnas motsvarande krav. Vägval (VV1) är ett obligatoriskt vägval.

Konstruktörens systemsäkerhetsvärdering kan omfatta följande:

- Att det tekniska systemet uppfyller lagstiftningen vid leveranstidpunkten och därmed är laglig att tas i bruk
- Att Försäkran om överensstämmelse (DoC), certifikat eller annat motsvarande dokument finns för exempelvis CE- eller rattmärkning
  - Om Anmält organ eller laboratorium använts för verifiering/certifiering ska dessa anges samt att det även ska styrkas att dessa organ är behöriga att verifiera kraven i aktuella harmoniserade och normativa standarder
- Att andra myndigheters beslut eller intyg finns och vad dessa omfattar

- Att den tekniska dokumentationen *(Technical file)* är refererad samt att verifieringen är utförd enligt de författningsenliga kraven inklusive de tillämpade standarderna. Om annat sätt har använts än de som standarderna kräver, för att verifiera uppfyllandet av de författningsenliga kraven, ska verifieringskriterierna och resultatet av verifieringen redovisas
- Om *CE-liknande process* har tillämpats redovisas hur detta har genomförts samt vad som har uppfyllts genom detta vägval och vad som har hanterats i annat vägval
- Att anvisningar för underhållsintervall finns och om möjligt är anpassade mot Försvarsmaktens underhållscykler
- Att Försvarsmaktens avsedda användning ryms inom ovanstående

16.2.2 SSV Vägval 2 – Godkänd av annan stat

Med annan stat avses främst en utländsk försvarsmyndighet. Vägval (VV2) är därför inte tillämpligt i *konstruktörens* (industrins) systemsäkerhetsvärdering eftersom denne inte kan ingå avtal med en utländsk försvarsmyndighet.

16.2.3 SSV Vägval 3 – Godkänd av annan part

Med annan part avses civil myndighet, klassningssällskap, ackrediterade laboratorier, certifierings- och kontrollorgan samt andra organ för validering och verifiering.

Konstruktörens systemsäkerhetsvärdering kan omfatta följande:

- Att använda ackrediterade laboratorier, certifierings- och kontrollorgan eller organ för validering och certifiering är erkända av relevant ackrediteringsorgan
- Att godkännanden omfattar den aktuella versionen av det tekniska systemet eller produkten finns, exempelvis:
  - Luftfartyg godkänt av civil myndighet
  - Fartyg godkänt av klassningssällskap
  - Vägfordon godkänt av kontrollorgan
  - Tryckkärl eller radio godkänt av tredjepartsorgan (Anmält organ)
- Att CE-märkt materiel, exempelvis en elektrisk produkt, där CE-märkningen bygger på verifiering av tillverkaren själv, men där beställaren kravställt att ett oberoende tredjepartsorgan behövs, exempelvis ett ackrediterat organ som certifierar produkten

- Att tillämpade standarder är relevanta för det tekniska systemet eller produkten och att verifieringen av kraven i standarderna har genomförts enligt praxis
- Att Försvarsmaktens avsedda användning ryms inom ovanstående

16.2.4 SSV Vägval 4 – Övriga standarder

Med övriga standarder avses branschstandarder som är etablerade och internationellt tillämpade samt *Allmänna råd* (AR) inom tillämpningsområdet.

Konstruktörens systemsäkerhetsvärdering kan omfatta följande:

- Att standarder tillämpats för att möjliggöra interoperabilitet, exempelvis i NATO
- Att motiv för valda standarder finns, exempelvis:
  - MIL-STD-882, DEF STAN 00-056, GEIA-STD-0010, ISO 12100, SS-EN 61508, SS-EN ISO 13849, DO 178C m fl
- Att tillämpade krav i standarder finns redovisade, exempelvis vald kritikalitetsnivå
- Att kriterier för verifiering finns samt att resultatet från utförd verifiering visar att kraven är uppfyllda

16.2.5 SSV Vägval 5 – Designregler

Med *Designregler* (DR) avses *Försvarsmaktens interna bestämmelser* (FIB), Försvarsmaktens *Designregler* (DR) samt FMV:s *Designregler* (DR) och handböcker (designregelsamlingar).

Konstruktörens systemsäkerhetsvärdering kan omfatta följande:

- Att motiv för valda *Designregler* (DR) och handböcker (designregelsamlingar) finns
- Att motiv för valda krav ur *Designregler* (DR) och handböcker (designregelsamlingar) finns
- Att kriterier för verifiering finns samt att resultatet från utförd verifiering visar att kraven är uppfyllda
- Att överenskommet förfarande för oberoende granskning är genomförd och att resultatet är dokumenterat

16.2.6 SSV Vägval 6 – Beprövat system

Med beprövat system avses att kunna åberopa trovärdiga och spårbara drifterfarenheter för det aktuella tekniska systemet eller för vissa delsystem.

Konstruktörens systemsäkerhetsvärdering kan omfatta följande:

- Att ursprungligt godkännande finns och att detta bedöms vara relevant för den framtida avsedda användningen
- Att drifterfarenheterna är trovärdiga och spårbara samt bedöms vara från en regelbunden och flerårig användning samt underhåll
- Att tidigare identifierade säkerhetsbrister under användning och underhåll har hanterats och att vidtagna åtgärder såsom omkonstruktioner, förändrat användningssätt eller underhåll finns dokumenterade
- Att aktuell materieldokumentation och tekniska data finns för den aktuella versionen av det tekniska systemet eller delsystemen

16.2.7 SSV Vägval 7 – Riskmatriser

Med riskmatriser avses olycksrisker som inte har kunnat omhändertas i tidigare vägval ska värderas mot krav på tolerabla risknivåer uttryckt i riskmatriser.

Konstruktörens systemsäkerhetsvärdering kan omfatta följande:

- Att alla kvarstående olycksrisker som inte har kunnat omhändertas i tidigare vägval är klassificerade i kravställda riskmatriser
- Att underlag finns som motiverar klassificeringen av samtliga olycksrisker i riskmatris
- Att principen för ALARP har tillämpats för olycksrisker i gult område *Begränsat tolerabel* (BT) och att motiven för ALARP är redovisade
- Att särskilt underlag finns redovisat för de olycksrisker som har klassificerats i rött område *Ej tolerabel* (ET)

16.3 Beställarens systemsäkerhetsvärdering

Med *beställare* avses den som anskaffar tekniska system och produkter utifrån EU-rätt och svensk lagstiftning samt *Systemmålsättning* (SMS 2).

Inför överlämning redovisar *beställaren* ställningstagandet i *Systemsäkerhetsdeklarationen* (SSD) utifrån krav i *Systemmålsättning* (SMS 2) och de förtydliganden och/eller justeringar som kan ha skett med *kravställaren.* Ställningstagandet är uppbyggt av argument och belägg hämtade från de tillämpade vägvalen (VV1–VV7), vilka redovisas i systemsäkerhetsvärderingen.

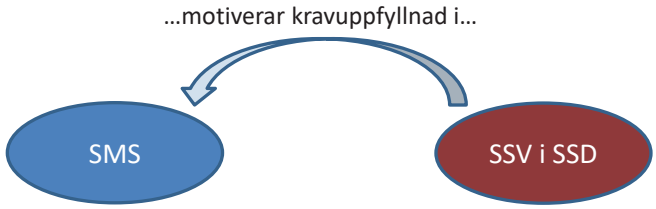


Bild 16.3 *Beställarens systemsäkerhetsvärdering ska visa att systemsäkerhetskraven i Systemmålsättningen (SMS 2) är uppfyllda.*

I *beställarens* systemsäkerhetsvärdering redovisas att:

- Systemsäkerhetskraven i kontraktet har följt inriktningen från *Systemmålsättning* (SMS 2)
- *Konstruktörens* eller *systemintegratörens* systemsäkerhetsarbete fortlöpande har följts upp för att säkerställa att systemsäkerhetsarbetet har följt överenskommen *Systemsäkerhetsplan* (SSPP)
- Materieldokumentation och tekniska data är fastställda
- *Konstruktörens* systemsäkerhetsarbete omfattar användning, underhåll, förrådshållning (transport) och avveckling
- *Konstruktörens* anvisningar för underhållsintervall överensstämmer eller är anpassade till Försvarsmaktens underhållscykler
- *Konstruktörens* argument och belägg för det tekniska systemet är hållbara och därmed visar att betryggande säkerhet har uppnåtts
- *Konstruktörens* tillämpning av vägvalen och uppfyllande av acceptanskriterier är i överensstämmelse med *Systemsäkerhetsplanen* (SSPP)
- Genomförd verifiering och validering visar att ställda systemsäkerhetskrav har uppfyllts

16.3.1 SSV Vägval 1 – Författningsenliga krav

Med författningsenliga krav avses EU-rätt och svensk lagstiftning med sina förordningar och föreskrifter. Hit räknas även de harmoniserade standarderna som, när deras mer detaljerade krav uppfylls, presumeras uppfylla författningarnas motsvarande krav. Vägval (VV1) är ett obligatoriskt vägval.

Beställarens systemsäkerhetsvärdering kan omfatta följande:

- Att det tekniska systemet uppfyller lagstiftningen och därmed är laglig att tas i bruk
- Att CE-, ratt- eller annan motsvarande märkning är korrekt utförd
- Om Anmält organ eller laboratorium har använts, att kontroll har skett att dessa organ är behöriga att verifiera kraven i aktuella harmoniserade och normativa standarder
- Att andra myndigheters beslut eller intyg finns, exempelvis:
  - Myndigheten för samhällsskydd och beredskap (MSB) för klassning av sprängmedel
  - Strålsäkerhetsmyndigheten (SSM) för tillstånd att hantera starka strålkällor
  - Livsmedelsverket (LMV) för veterinärintyg för hantering av livsmedel
  - Naturvårdsverket (NV) för användning av utarmat uran
- Om en *CE-liknande process* har accepterats, att den är korrekt redovisad för den materiel som hanterats enligt eventuellt undantag från CE-märkningen samt om annat sätt än enligt standarderna krävts för att verifiera uppfyllande av de författningsenliga kraven ska verifieringskriterierna och resultatet av verifieringen finnas
- Att Försvarsmaktens avsedda användning ryms inom ovanstående.

16.3.2 SSV Vägval 2 – Godkänd av annan stat

Med annan stat avses främst en utländsk försvarsmyndighet.

*Beställaren*s systemsäkerhetsvärdering kan omfatta följande:

- Att godkännandet från annan stat omfattar den aktuella versionen av det tekniska systemet eller produkten
- Att systemsäkerhetsarbetet har följt en etablerad systemsäkerhetsstandard
- Att systemsäkerhetsdokumentationen har granskats och bedömts trovärdig
- Att Försvarsmaktens avsedda användning ryms inom ovanstående

- Att systemsäkerhetsarbetet har följt en etablerad systemsäkerhetsstandard
- Att systemsäkerhetsdokumentationen har granskats och bedömts trovärdig
- Att Försvarsmaktens avsedda användning ryms inom ovanstående

16.3.3 SSV Vägval 3 – Godkänd av annan part

Med annan part avses civil myndighet, klassningssällskap, ackrediterade laboratorier, certifierings- och kontrollorgan samt andra organ för validering och verifiering.

Beställarens systemsäkerhetsvärdering kan omfatta följande:

- Att använda ackrediterade laboratorier, certifierings- och kontrollorgan eller organ för validering och certifiering är erkända av relevant ackrediteringsorgan
- Att godkännanden omfattar den aktuella versionen av det tekniska systemet eller produkten, exempel på godkännanden kan vara:
  - Luftfartyg godkänt av civil myndighet
  - Fartyg godkänt av klassningssällskap
  - Vägfordon godkänt av kontrollorgan
  - Tryckkärl eller radio godkänt av tredjepartsorgan (Anmält organ)
- Att CE-märkt materiel, exempelvis en elektrisk produkt, där CE-märkningen bygger på verifiering av tillverkaren själv, men där beställaren kravställt att ett oberoende tredjepartsorgan behövs, exempelvis ett ackrediterat organ som certifierar produkten
- Att tillämpade standarder är relevanta för det tekniska systemet eller produkten och att verifieringen av kraven i standarderna har genomförts enligt praxis
- Att Försvarsmaktens avsedda användning ryms inom ovanstående.

16.3.4 SSV Vägval 4 – Övriga standarder

Med övriga standarder avses branschstandarder som är etablerade och internationellt tillämpade standarder samt *Allmänna råd* (AR) inom tillämpningsområdet.

Beställarens systemsäkerhetsvärdering kan omfatta följande:

- Att standarder tillämpats för att möjliggöra interoperabilitet, exempelvis i NATO
- Att motiv för valda standarder finns, exempelvis:

  - SS-EN 61508, SS-EN ISO 13849, DO 178C m fl
- Att tillämpade krav i standarder finns redovisade, exempelvis vald kritikalitetsnivå för ingående datorsystem och programvara
- Att kriterier för verifiering finns samt att resultatet från utförd verifiering visar att kraven är uppfyllda

16.3.5 SSV Vägval 5 – Designregler

Med *Designregler* (DR) avses Försvarsmaktens interna bestämmelser (FIB), Försvarsmaktens *Designregler* (DR) samt FMV:s *Designregler* (DR) och handböcker (designregelsamlingar).

Beställarens systemsäkerhetsvärdering kan omfatta följande:

- Att motiv för valda FIB, *Designregler* (DR) och handböcker (designregelsamlingar) finns
- Att motiv för valda krav ur *Designregler* (DR) och handböcker (designregelsamlingar) finns
- Att kriterier för verifiering finns samt att resultatet från utförd verifiering visar att kraven är uppfyllda
- Att överenskommet förfarande för oberoende granskning är genomförd och att resultatet är dokumenterat
- Att konstruktionen uppfyller råden från FMV:s Rådgivningsgrupper inom vapen- och ammunitionssäkerhetsområdet i enlighet med Handbok Vapen- och ammunitionssäkerhet (H VAS) och att de formellt avgivna råden av FMV:s Rådgivningsgrupper är omhändertagna

16.3.6 SSV Vägval 6 – Beprövat system

Med beprövat system avses att kunna åberopa trovärdiga och spårbara drifterfarenheter för det aktuella tekniska systemet eller för vissa delsystem.

Beställarens systemsäkerhetsvärdering kan omfatta följande:

- Att ursprungligt godkännande finns och att detta bedöms vara relevant för den framtida avsedda användningen
- Att drifterfarenheterna är trovärdiga och spårbara samt bedöms vara från en regelbunden och flerårig användning samt underhåll

- Att tidigare identifierade säkerhetsbrister under användning och underhåll har hanterats och att vidtagna åtgärder såsom omkonstruktioner, förändrat användningssätt eller underhåll finns dokumenterade
- Att aktuell materieldokumentation och tekniska data finns för den aktuella versionen av det tekniska systemet eller delsystemet

16.3.7 SSV Vägval 7 – Riskmatriser

Med riskmatriser avses olycksrisker som inte har kunnat omhändertas i tidigare vägval ska värderas mot krav på tolerabla risknivåer uttryckt i riskmatriser.

Beställarens systemsäkerhetsvärdering kan omfatta följande:

- Att alla kvarstående olycksrisker som inte har kunnat omhändertas i tidigare vägval är klassificerade mot kravställda riskmatriser
- Att underlag finns som motiverar klassificeringen av samtliga olycksrisker i riskmatris
- Att principen för ALARP har tillämpats för olycksrisker i gult område *Begränsat tolerabel* (BT) och att motiven för ALARP är redovisade
- Att redovisningen för olycksrisker vilka har klassificerats i rött område *Ej tolerabel* (ET) är fullständigt och att Försvarsmaktens svar på hemställan om avsteg från ställda systemsäkerhetskrav finns.

16.4 Kravställarens systemsäkerhetsvärdering

Försvarsmakten i rollen som *kravställare* genomför sin systemsäkerhetsvärdering med stöd av *Vägvalsmodellen* (VVM). Systemsäkerhetsvärderingen genomförs ur ett antal perspektiv och det slutliga ställningstagandet dokumenteras i ett *Systemsäkerhetsgodkännande* (SSG).

16.4.1 Värdering ur perspektivet tekniskt designansvar

Vid systemöverlämningen (SÖL) kontrollerar Försvarsmakten att mottagen *Systemsäkerhetsdeklaration* (SSD) med tillhörande bilagor uppfyller ställda systemsäkerhetskrav i *Systemmålsättning* (SMS 2) och *Systemsäkerhetsledningsplan* (SSMP).

Aktuellt ställningstagande granskas för att säkerställa att det visar att betryggande säkerhet för det tekniska systemet har uppnåtts, är heltäckande och att det inte

innehåller några otillbörliga friskrivningar. Argumenten och beläggen i systemsäkerhetsvärderingen granskas i syfte att hitta ogiltiga eller alltför svaga argument. Vidare hanteras eventuella restriktioner för kvarstående olycksrisker genom att förslag till verksamhetsregler tas fram.

Underlaget kan behöva kompletteras med motsvarande underlag för andra produkter som ligger utanför aktuell *Systemsäkerhetsdeklaration* (SSD). Exempelvis kan underlag för befintlig materiel eller från andra leverantörer tillsammans utgöra det tekniska system som *Systemsäkerhetsgodkännande*t (SSG) ska omfatta.

16.4.2 Värdering ur perspektivet verksamhetsansvar

En värdering ur perspektivet verksamhetsansvar är en kontroll och kvalitetsgranskning att verksamheten är redo att kunna hantera det tekniska systemet eller produkten på ett säkert sätt. Teknik som levereras har alltid begränsningar vilket gör att utbildning, metod och organisation samt förvaltning är avgörande komponenter för en säker användning och uppfyllande av gällande lagstiftning.

När värdering ur perspektivet tekniskt designansvar har genomförts granskas underlaget för att säkerställa att betryggande säkerhet för det tekniska systemet har uppnåtts, är heltäckande och att förslag till verksamhetsregler finns för eventuella restriktioner för kvarstående olycksrisker.

Vidare kontrolleras att underlaget med tillhörande bilagor uppfyller ställda systemsäkerhetsmål i *Systemsäkerhetsledningsplan* (SSMP) och därmed ryms inom de fastställda systemsäkerhetsmålen.

Underlaget kan behöva kompletteras med motsvarande underlag för anläggningar, vilket kan ligga utanför aktuellt tekniskt systems leveranser. Exempelvis kan underlag från Fortifikationsverket tillsammans med det tekniska systemet utgöra det totala tekniska system som *Systemsäkerhetsgodkännandet* (SSG) ska omfatta.

16.4.3 Systemsäkerhetsgodkännande

Efter genomförda värderingar sammanställs underlaget tillsammans med aktuella bilagor till ett *Systemsäkerhetsgodkännande* (SSG). Innan fastställande säkerställs granskning av stående instanser och eventuella samråd tecknas. Därefter fattas beslut om S*ystemsäkerhetsgodkännande* (SSG).

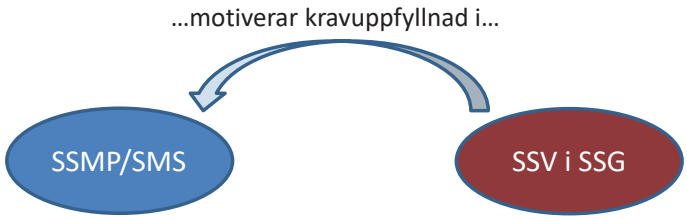


Bild 16.4 *Kravställarens systemsäkerhetsvärdering i Systemsäkerhetsgodkännandet (SSG) ska visa att systemsäkerhetskraven i Systemsäkerhetsledningsplanen (SSMP) och Systemmålsättning (SMS 2) är uppfyllda.*

17 Systemsäkerhetsbeslut

Syftet med detta kapitel är att beskriva beslutssystemet för samtliga aktörer i dess olika roller såsom kravställare, beställare och konstruktör. Vidare beskrivs vissa specialfall som hamnar utanför de formella systemsäkerhetsbesluten.

17.1 Olika systemsäkerhetsbeslut

Systemsäkerhetsbeslut är ett samlingsbegrepp *för Systemsäkerhetsutlåtande* (SCA), *Systemsäkerhetsdeklaration* (SSD) och *Systemsäkerhetsgodkännande* (SSG), vilka är beslut som överräckes ifrån en roll till nästa. Dessa systemsäkerhetsbeslut ligger till grund för *Beslut om användning, central nivå* (BOAC) och *Beslut om användning, lokal nivå* (BOAL).

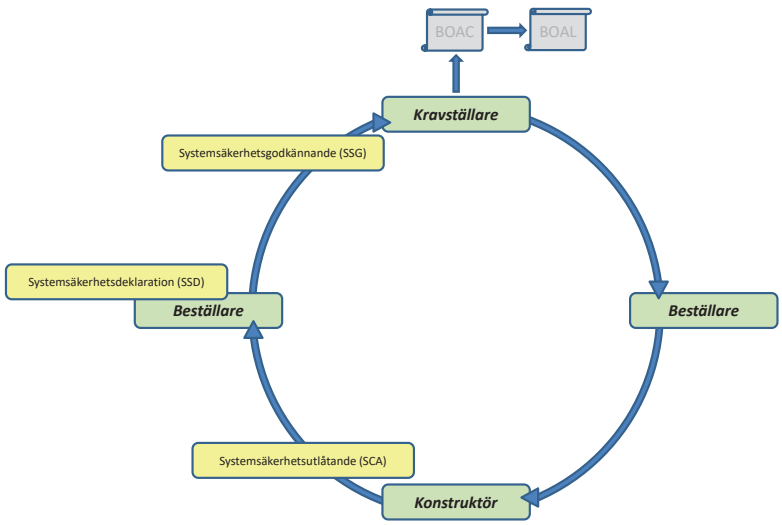


Bild 17.1 Systemsäkerhetsbeslut för överlämning mellan olika roller.

Systemsäkerhetsbeslutet ska vidimera att det tekniska systemet eller produkten under givna förutsättningar är redo att tas i bruk vid Försvarsmakten. Genom systemsäkerhetsbeslutet bekräftas dels att lagstiftningen, dels att ställda krav på systemsäkerhet är uppfyllda och att det tekniska systemet, med dess samlade tekniska dokumentation, erbjuder betryggande säkerhet.

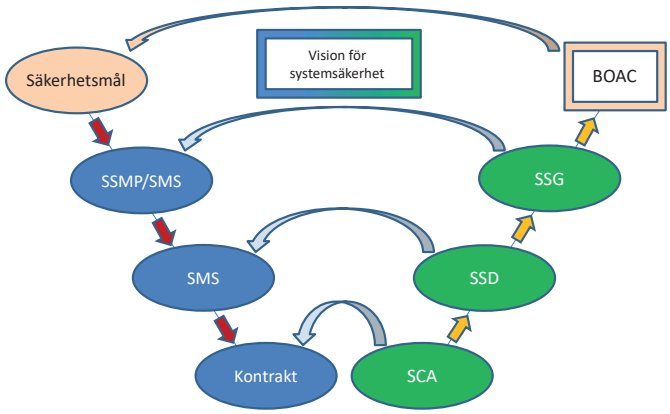


Bild 17.2 *Ett systemsäkerhetsbeslut ska dels visa att lagstiftningen är uppfylld, dels att ställda systemsäkerhetskrav på motsvarande nivå är uppfyllda.*

Försvarsmaktens *Systemsäkerhetsgodkännande* (SSG), som grund för *Beslut om användning, central nivå* (BOAC) och *Beslut om användning, lokal nivå* (BOAL), ska normalt fattas för alla tekniska system och produkter. Det kan dock finnas motiv för viss dispositivitet kring besluten genom att slå ihop vissa av dem för mindre riskfyllda produkter eller när en ändring (modifiering) kan anses ingå i överordnat redan fattat beslut. Exempelvis kan en ändring (modifiering) som tas i ett *Systemsäkerhetsgodkännande* (SSG) rymmas inom befintligt *Beslut om användning, central nivå* (BOAC). Motiv för att detta ska framgå i *Systemsäkerhetsgodkännandet* (SSG).

17.2 Allmänt om systemsäkerhetsbeslut

Rubriken i systemsäkerhetsbeslutet ska vara ren och inte innehålla epitet såsom tillfälligt, temporärt, tidsbegränsat, interimistiskt eller för försöksvis användning. Eventuella behov av begränsningar regleras under aktuella rubriker i systemsäkerhetsbeslutet.

I systemsäkerhetsbeslutet definieras entydigt det tekniska systemets eller produktens tillåtna konfigurationer, dess användningsmiljöer samt krav på gränsytor till samverkande system och anläggningar. Vidare framgår det i materieldokumentationen och genom märkning hur systemet får användas, underhållas, förrådshållas (transporteras) och avvecklas.

För kvarstående olycksrisker där överenskomna riskreducerande åtgärder ännu inte är införda i det tekniska systemet ska restriktioner redovisas samt vilka kriterier som gäller för att restriktionerna kan hävas.

Den samlade mängden information som har bärighet på systemsäkerheten kan fördelas mellan systemsäkerhetsbeslutet, *Systemsäkerhetsrapporten* (SAR), *Riskloggen* (RL) och övrig riskdokumentation. För produkter som exempelvis är CE-märkta/rattmärkta, godkända av annan part eller tillhör kategorin COTS kan all information finnas i systemsäkerhetsbeslutet.

I systemsäkerhetsbeslutet ska det finnas ett ställningstagande om att lagstiftning och ställda krav på systemsäkerhet vid leveranstidpunkten är uppfyllda. Systemsäkerhetsbeslutet ska vara tydligt och transparent samt inte innehålla friskrivningar.

Ett systemsäkerhetsbeslut fattas av behörig person som dessutom inte personligen ska ha deltagit i systemsäkerhetsarbetet som har resulterat i beslutsunderlaget.

17.3 Systemsäkerhetsutlåtande

Försvarsmakten eller industrin, i rollen som *konstruktör*, ska utfärda ett *Systemsäkerhetsutlåtande* (SCA) med tillhörande riskdokumentation. *Systemsäkerhetsutlåtandet* (SCA) ska uppfylla kraven i kontraktet (eller motsvarande).

Försvarsmakten eller FMV, i rollen som *beställare*, granskar *konstruktörens Systemsäkerhetsutlåtande* (SCA) utifrån att:

- *Systemsäkerhetsutlåtandet* (SCA) är signerat av behörig person
- Ställningstagandet utifrån de givna förutsättningarna är tydligt formulerat och är fri från friskrivningar
- Systemsäkerhetsvärderingen visar att systemsäkerhetskraven i kontraktet är uppfyllda genom vägval (VV1–VV6) samt att hanterade olycksrisker i vägval (VV7) ryms inom *Tolerabel risknivå* (TR)
- Systemsäkerhetsvärderingen med sina argument och belägg bedöms vara hållbara och sanna
- Tillåtna konfigurationer av tekniskt system är definierade

- Tillåtna ändringsbara parameterintervall är definierade
- Användningsmiljöer och gränsytor finns beskrivna
- Bruksanvisningar, underhållsinstruktioner och varselmärkningar finns
- Utbildning och/eller utbildningsmaterial finns
- Tillämplig lagstiftning är uppfylld vid leveranstidpunkten och att eventuella undantag för militär materiel finns dokumenterade
- Erforderliga myndighetsbeslut finns för att få ta systemet i bruk
- Märkningar såsom CE-, CIP- eller rattmärkning finns och att intyg såsom DoC, CoC eller CA finns bifogat, alternativt refereras till
- Säkerhetsdatablad för kemiska produkter finns
- Tillämpade civila och militära säkerhetsrelaterade standarder finns dokumenterade
- Riskreducerande åtgärder är införda samt att detta finns dokumenterat i *Riskloggen* (RL)
- Restriktioner finns för kvarstående olycksrisker där riskreducerande åtgärder ännu inte är införda

17.4 Systemsäkerhetsdeklaration

Försvarsmakten eller FMV, i rollen som *beställare*, ska utfärda en S*ystemsäkerhets-deklaration* (SSD). *Systemsäkerhetsdeklarationen* (SSD) ska uppfylla kraven i *Systemmålsättning* (SMS 2).

Försvarsmakten i rollen som kravställare granskar beställarens *Systemsäkerhets-deklaration* (SSD) utifrån att:

- *Systemsäkerhetsdeklarationen* (SSD) är signerad av behörig person
- Ställningstagandet utifrån de givna förutsättningarna är tydligt formulerat och är fri från friskrivningar
- Systemsäkerhetsvärderingen visar att systemsäkerhetskraven i *Systemmål-sättning* (SMS 2) är uppfyllda genom vägval (VV1–VV6) samt att hanterade olycksrisker för vägval (VV7) ryms inom *Tolerabel risknivå* (TR)
- Systemsäkerhetsvärderingen med sina argument och belägg bedöms vara hållbara och sanna
- Tillåtna konfigurationer av tekniskt system är definierade

- Tillåtna ändringsbara parameterintervall är definierade
- Användningsmiljöer och gränsytor finns beskrivna
- Materieldokumentation och varselmärkningar för användning och underhåll är fastställda
- Utbildning och/eller utbildningsmaterial finns
- Tillämplig lagstiftning är uppfylld vid leveranstidpunkten och att eventuella undantag för militär materiel finns dokumenterade
- Erforderliga myndighetsbeslut finns för att få ta systemet i bruk
- Märkningar såsom CE-, CIP- eller rattmärkning finns och att intyg såsom DoC, CoC eller CA finns bifogat
- Säkerhetsdatablad för kemiska produkter finns
- Tillämpade civila och militära säkerhetsrelaterade standarder finns dokumenterade
- Riskreducerande åtgärder är införda samt att detta finns dokumenterat i *Riskloggen* (RL)
- Förslag till restriktioner finns för kvarstående olycksrisker där riskreducerande åtgärder ännu inte är införda
- Eventuellt protokoll från granskning av *Systemsäkerhetsutlåtandet* (SCA) finns
- Om det tekniska systemet innehåller vapen, ammunition eller explosiv vara ska:
    - Protokoll från FMV:s Rådgivningsgrupper finns och att råden är kommenterade och motiverade
    - Förteckning över godkänd ammunition som får användas i vapensystemet finnas, alternativt att ammunitionen är godkänd mot vissa vapensystem

17.5 Systemsäkerhetsgodkännande

Försvarsmakten i rollen som *kravställare* ska utfärda ett *Systemsäkerhetsgodkännande* (SSG). Detta beslut bekräftar att *beställarens Systemsäkerhetsdeklaration* (SSD) är tillfyllest samt att eventuella förslag till restriktioner för kvarstående olycksrisker är rimliga och är omhändertagna genom tillfälliga verksamhetsregler.

Kravställaren bereder *Systemsäkerhetsgodkännandet* (SSG) genom att säkerställa att:

- Lagstiftningen är uppfylld och att eventuella undantag för militär materiel och/eller militär användning finns dokumenterat
- Eventuellt säkerhetsledningssystem finns
- Erforderliga myndighetstillstånd finns
- Verksamhetsregler finns, exempelvis underlag till SäkR
- Restriktioner för kvarstående olycksrisker finns
- Materieldokumentation för användning och underhåll finns
- Det tekniska systemet finns registrerat i olika förvaltningssystem
- Utbildningsunderlag för utbildning av instruktörer och användare finns
- Krav på gränsytor mot andra tekniska system och produkter finns och att ställda krav är uppfyllda.
- Krav på anläggningstekniska basresurser, lokaler och/eller utrustning anges och att ställda krav är uppfyllda
- Säkerhetsdatablad för kemiska produkter är registrerade i förvaltningssystem
- *Arbetsgrupp för systemsäkerhet* (SSWG) finns
- Drifterfarenheter kan rapporteras
- Ammunitionsövervakning är etablerad

Kravställaren formulerar ett ställningstagande om att både systemsäkerhetskraven i *Systemsäkerhetsledningsplanen* (SSMP) för produktområdet och *Systemmålsättnin*g (SMS 2) för det tekniska systemet är uppfyllda.

I de fallen Försvarsmakten integrerar materiel i anläggningar byggda av Fortifikationsverket krävs ett kompletterande systemsäkerhetsarbete för integrationen. Försvarsmakten har att infordra byggnadstekniska handlingar över basresurser såsom el, kraft, värme, kyla, ventilation, vatten och avlopp från Fortifikationsverket. Utöver anläggningens fysiska ytter- och innermått kan även

olika vikter och placering på golv eller andra ytor begränsa användningen. När befintlig eller ny materiel integreras till dessa basresurser och/eller inom ramen för fysiska begränsningar kan integrationsrisker uppstå. Vidare behöver den totala brandbelastningen analyseras och utrymningsmöjligheter provas. Detta systemsäkerhetsarbete dokumenteras i en *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL) och biläggs till *Systemsäkerhetsgodkännandet* (SSG).

17.6 Beslut om användning, central nivå

Försvarsmakten i rollen som *kravställare* ska i beslutsgrind *Beslut om användning, central niv*å (BOAC), även inkludera systemsäkerhet.

Systemsäkerhetsunderlaget ska visa att:

- Eventuellt godkännande från *Delegationen för folkrättslig granskning av vapenprojekt* finns
- Systemsäkerhetsmål i *Systemsäkerhetsledningsplan* (SSMP) är uppfyllda
- Systemsäkerhetskrav i *Systemmålsättning* (SMS 2) är uppfyllda
- *Systemsäkerhetsgodkännande* (SSG) är fastställt

Om *Systemsäkerhetsgodkännande* (SSG) inte beslutats ska motsvarande underlag och ställningstaganden redovisas i *Beslut om användning, central nivå* (BOAC).

I *Beslut om användning, central nivå* (BOAC) styrs vad som ska omhändertas i *Beslut om användning, lokal nivå* (BOAL). Det kan exempelvis vara krav på utbildning av personal eller tillgång till anläggningstekniska basresurser, lokaler eller utrustning. Om *Beslut om användning, lokal nivå* (BOAL) inte är nödvändigt ska detta framgå av underlaget i *Beslut om användning, central nivå* (BOAC).

17.7 Beslut om användning, lokal nivå

Försvarsmaktens chef för organisationsenhet (C OrgE) i rollen som arbetsgivare med delegerat arbetsmiljöansvar ska utfärda ett *Beslut om användning, lokal nivå* (BOAL), vilket är ett lokalt beslut som även inkluderar systemsäkerhet.

I beslutsgrinden kan krav från *Beslut om användning, central nivå* (BOAC) behöva omhändertas, exempelvis att:

- Rutiner för riskhantering vid införande av ny materiel och/eller metoder finns
- Materieldokumentation och SäkR finns tillgängliga
- Eventuella restriktioner är kända och förstådda av användare och underhållspersonal
- Hantering av farliga ämnen, inklusive explosiva varor kan ske
- Hantering av förväntade programvaruuppdateringar kan genomföras
- Genomförande av utbildning för användare och underhållspersonal kan ske löpande
- Återrapportering av drifterfarenheter, till exempel i form av driftdata, sker

För materiel som Försvarsmakten har tekniskt designansvar för genomförs ändring (modifiering) och teknisk anpassning med teknisk order (TO), beslutad av tekniskt designansvarig. Hantering av detta sker enligt interna rutiner i organisationen och kan i slutänden leda fram till nytt *Beslut om användning, lokal nivå* (BOAL).

I det fallen anskaffning av tekniska system eller produkter sker i OrgE egen regi, ska chef för organisationsenhet (C OrgE) fatta ett *Beslut om användning, lokal nivå* (BOAL) som till sin omfattning och innehåll motsvarar ett *Systemsäkerhetsutlåtande* (SCA).

17.8 Övriga fall utanför de formella systemsäkerhetsbesluten

Syftet med detta avsnitt är att beskriva vissa specialfall som faller utanför de formella systemsäkerhetsbesluten.

17.8.1 Systemsäkerhetsmeddelande

Systemsäkerhetsmeddelande (SSM) används av den aktör som vill informera Försvarsmakten i rollen som *kravställare* om en säkerhetsbrist i ett tekniskt system eller produkt, eller om brister och felaktigheter i dess användning, underhåll eller hantering, utan att återta ett utfärdat systemsäkerhetsbeslut. Ett *Systemsäkerhetsmeddelande* (SSM) gäller till dess att säkerhetsbristen är hanterad.

Ett *Systemsäkerhetsmeddelande* (SSM) bör minst omfatta:

- Identifiering av tekniskt system eller produkt
- Analys av det inträffade eller det observerade
- Riskbedömning
- Förslag till rekommendationer

Om flera olika händelser eller observationer finns för samma tekniska system eller produkt rekommenderas att ett *Systemsäkerhetsmeddelande* (SSM) utfärdas per observation. Detta förenklar administrationen vid beslut om att säkerhetsbristen är hanterad.

Om ett *Systemsäkerhetsmeddelande* (SSM) innebär att information för att förtydliga, upplysa eller påminna användaren om förhållanden med koppling till avsedd användning, förändrat användningssätt inklusive normglidning eller att verksamhetsregler behöver skärpas, kan ärendet stängas av ordförande i *Arbetsgrupp för systemsäkerhet* (SSWG), utan att nya systemsäkerhetsbeslut utfärdas.

Om ett *Systemsäkerhetsmeddelande* (SSM) innebär att en Teknisk order (TO) för ändring (modifiering) behöver tas fram, utfärdas nya systemsäkerhetsbeslut.

Ett *Systemsäkerhetsmeddelande* (SSM) kan återtas av utfärdaren om säkerhetsbristen inte längre anses vara aktuell. Ett sådant återtagande dokumenteras av ordförande i *Arbetsgrupp för systemsäkerhet* (SSWG) i protokoll eller mötesanteckningar.

17.8.2 Systemsäkerhetsintyg

Systemsäkerhetsintyg (SSI) utfärdas inför verifiering och validering av tekniska system och produkter. Det finns ett flertal olika metoder för både objektiva och subjektiva utvärderingar.

Ett *Systemsäkerhetsintyg* (SSI) ska till sin omfattning och innehåll motsvara en *Systemsäkerhetsdeklaration* (SSD), men vara begränsad till planerad verksamhet beskriven i ett visst provprogram eller provplan.

Den egna provnings- eller försöksorganisationen granskar *Systemsäkerhetsintyget* (SSI) utifrån att:

- *Systemsäkerhetsintyget* (SSI) är signerad av behörig person
- Provprogram eller provplan finns
- Provobjekt, med dess tillåtna konfigurationer och ändringsbara parameterintervall, är fastställd för planerad verksamhet
- *Systemsäkerhetsrapport* (SAR) finns med identifierade olycksrisker och förslag till restriktioner, vilket kan baseras på konstruktörens S*ystemsäkerhetsutlåtande* (SCA)
- Användningsmiljöer och gränsytor finns beskrivna
- Erforderlig materieldokumentation och varselmärkningar för användning finns
- Säkerhetsdatablad för kemiska produkter finns

Om det tekniska systemet innehåller vapen, ammunition eller explosiv vara ska protokoll från FMV:s Rådgivningsgrupp finnas med och föreslagna råd vara hanterade.

Systemsäkerhetsintyg (SSI) kan utfärdas för organisations- och metodförsök som genomförs i Försvarsmaktens regi.

Säkerhetsintyg utfärdas för örlogsfartyg som genomför provverksamhet med ett Provturskommande (PTK). Säkerhetsintygets innehåll och omfattning regleras i särskild ordning.

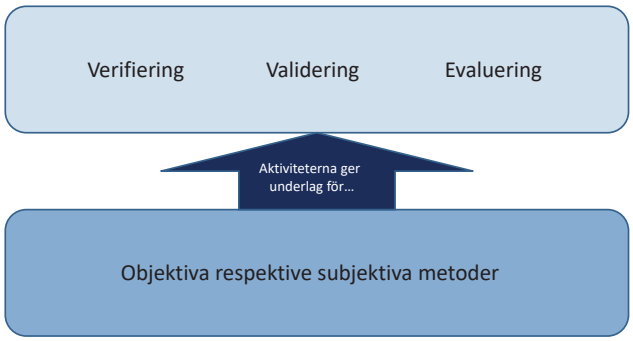


Bild 17.3 *Ett systemsäkerhetsbeslut ska dels visa att lagstiftningen är uppfylld, dels att ställda systemsäkerhetskrav på motsvarande nivå är uppfyllda.*

17.8.3 Utlåning av materiel från FMV till Försvarsmakten

Om Försvarsmakten lånar materiel från FMV innan systemöverlämning (SÖL) genomförs bör en överenskommelse mellan parterna tas fram. Överenskommelsen bör innehålla:

- Verksamhetsbeskrivning
- Datum (period) och förband
- Tekniskt utförande (typkonfiguration) inklusive materieldokumentation
- Individbeteckningar, alternativt antal produkter om individbeteckning saknas
- *Systemsäkerhetsutlåtande* (SCA)
- *Beställarens Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL)
- Restriktioner för kvarstående olycksrisker
- Behov av personlig skyddsutrustning (PPE)
- Utbildning
- Ansvarsfördelning mellan aktörerna
- Rutiner för samordningsmöten (exempelvis SSWG)

17.8.4 Utlåning av materiel till annan myndighet eller kommun

Om Försvarsmakten lånar ut materiel, utan medföljande personal, till en annan myndighet eller kommun i syfte att främja samhällets säkerhet behöver denna organisation få information om eventuella undantag för militär materiel eller militär användning. De behöver även erforderlig materieldokumentation samt upplysas om andra saker såsom riskområden, behov av personlig skyddsutrustning (PPE) eller krav på utbildning. Annan myndighet eller kommun ges då möjlighet

att vidta egna åtgärder för att kompensera för Försvarsmaktens undantag för militär materiel eller militär användning. Försvarsmakten meddelar eventuella undantag och annan relevant information i lånehandlingar.

17.8.5 Tekniskt designansvar vid export, uthyrning och utlåning

Om Försvarsmakten, eller annan organisation såsom FMV, tillhandahåller materiel till en annan stat blir denna organisation tekniskt designansvarig. I de fallen det är en exportkonfiguration krävs det att det finns en *Systemsäkerhetsledningsplan* (SSMP). Vid behov kan även en *Systemsäkerhetsplan* (SSPP) tas fram för det förväntade systemsäkerhetsarbetet inför olika ändringar (modifieringar) och leveranser till annan stat.

Med tillverkarens underlag som grund kan Försvarsmakten, eller annan organisation såsom FMV, utfärda ett *Systemsäkerhetsgodkännande* (SSG) för exportkonfigurationen av det tekniska systemet. Systemsäkerhetsbeslut och riskdokumentation utfärdas på det språk som avtalats i kontrakt med aktuell stat (annan försvarsmyndighet).

17.8.6 Systemintegratörens systemsäkerhetsarbete

Systemintegratören genomför systemsäkerhetsarbete i enlighet med *beställarens Systemsäkerhetsplan* (SSPP) för att omhänderta kombinerade tekniska system och produkter såsom programvaror eller fysiska produkter. Ett sådant system-av-system innebär ny funktionalitet och nya kombinationer av fysiska produkter. Systemsäkerhetsarbetet dokumenteras i *Systemsäkerhetsrapport* (SAR). *Systemsäkerhetsanalysen* utgår ifrån aktiviteten *Riskanalys för system-av-system* (SoSHA).

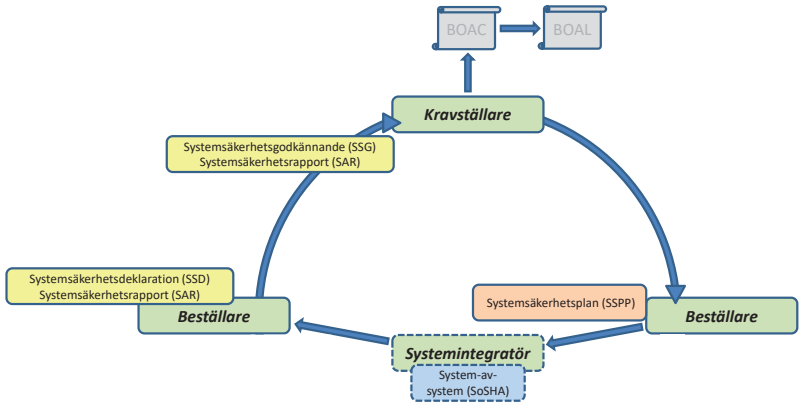


Bild 17.4 *Systemintegratörens systemsäkerhetsarbete.*

18 Ändring och modifiering av tekniska system

Syftet med detta kapitel är att beskriva olika varianter av ändringar (modifieringar) och inrikta omfattningen av det systemsäkerhetsarbete som behöver genomföras.

18.1 Grunder för ändringar (modifieringar)

Med ändringar avses dels modifieringar av tekniska system, dels förändringar av verksamhetsregler, materieldokumentation, underhåll, utbildning, förrådshållning, transportsätt med mera för det tekniska systemet.

Med modifieringar avses specifikt det tekniska systemets utförande (konfiguration) med avseende på mekaniska delar, elektronik, programvara eller andra delar. Modifieringar kan innebära prestandahöjningar av befintligt tekniskt system eller att nya delsystem med ny funktionalitet tillförs.

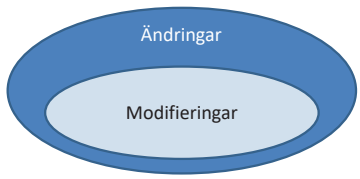


Bild 18.1 Modifieringar är en delmängd av ändringar.

Det kan också finnas ändringar (modifieringar) som införs tillfälligt och i begränsad omfattning för viss verksamhet eller vid omhändertagande av tekniska system i stridslinjen.

18.2 Orsaker till ändringar (modifieringar)

Försvarsmakten har tekniskt designansvar för alla tekniska system och produkter samt ansvarar för att leda systemsäkerhetsverksamheten så att de kan bibehålla betryggande säkerhet under hela dess livslängd. Detta kan ske genom nödvändiga eller förutbestämda ändringar (modifieringar). Alla tekniska system och produkter

överlämnade till (mottagna av) Försvarsmakten räknas regulatoriskt som tagna i bruk, det vill säga betraktas som begagnade.

Behov av ändringar (modifieringar) kan uppstå av många olika skäl såsom ny lagstiftning, åtgärda identifierade säkerhetsbrister, hantera förändrat användningssätt inklusive normglidning, ändrad utbildning, annan omgivningsmiljö, ändrade underhållsintervall eller att reservdelar av ursprungligt utförande inte längre finns. Ändringar (modifieringar) kan även införas utifrån förändrade krav för att förbättra tillgänglighet eller åstadkomma ändrad funktionalitet för att ge ökad förmåga hos förbanden.

Innan ändrade (modifierade) tekniska system kan tas i bruk ska dessa ha genomgått erforderligt systemsäkerhetsarbete och beslutats vara tillräckligt säkra för den tänkta (avsedda) användningen

18.3 Permanenta ändringar, ny Systemmålsättning

Med en ny utgåva av *Systemmålsättning* (SMS 2) fastställs förändrade krav på det tekniska systemet. För sådana förutbestämda ändringar (modifieringar) genomförs motsvarande systemsäkerhetsverksamhet som vid anskaffning av nya tekniska system eller produkter. Nya systemsäkerhetsbeslut behöver utfärdas.

18.4 Permanenta ändringar, ursprunglig Systemmålsättning

Vid ändring (modifiering) av befintliga tekniska system eller produkter, med avsikt att över tid bibehålla teknisk förmåga och prestanda, det vill säga inom ursprunglig *Systemmålsättning* (SMS 2), behöver systemsäkerhetsarbetet anpassas till ändringens (modifieringens) inverkan på befintlig systemsäkerhetsvärdering och de vägvalen (VV) den bygger på.

Om ändringen (modifieringen) sker inom ramen för ett tidigare godkännande enligt vägval (VV1 exempelvis avseende CE-märkning, VV2 eller VV3) behöver inget systemsäkerhetsarbete utföras om det kan påvisas att ändringen

(modifieringen) ligger inom ramen för detta godkännande och att godkännandet fortfarande är fullt giltigt och ryms inom Försvarsmaktens tänkta (avsedda) användning. Beslut om så är fallet fattas i samband med fastställandet av Teknisk Order (TO).

Om ändringen inte ryms inom tidigare godkännanden för vägval (VV–VV3), behöver detta utredas i särskild ordning.

Ändringar (modifieringar) regleras normalt genom Teknisk Order (TO). I Teknisk Order (TO) redovisas eller refereras till grunder för fastställande med avseende på systemsäkerhet. Där redovisas befintliga eller nya systemsäkerhetsbeslut samt motiveringar för att systemsäkerhetsarbetet är tillfyllest. Systemsäkerhetsarbetet ska dels omhänderta den nya konfigurationen av det tekniska systemet, dels visa att arbetsgången under det praktiska arbetet vid införandet av ändringen (modifieringen) är säker. Notera att nya systemsäkerhetsbeslut kan behövas från de olika aktörerna i rollerna som *konstruktör*, *beställare* och *kravställare* beroende på ändringens beskaffenhet.

18.5 Ändring (modifiering) av produkter som verifierats enligt civila regelverk

I de fallen en begagnad produkt som tidigare har verifierats enligt civila regelverk avses att ändras (modifieras), kan exempelvis CE-märkningen behöva göras om. Ändringen kan regulatoriskt vara *ej väsentlig ändring (minor/non-significant change)* eller *väsentlig ändring (significant/substantial change).* Detta får avgöras från fall till fall med stöd av EU:s guider och eventuellt med stöd av den tillverkare som utförde verifieringen, exempelvis CE-märkningen eller rattmärkningen.

Erfarenhetsmässigt har det visat sig att de flesta ändringar (modifieringar) av maskiner bedömts vara *ej väsentlig ändring*, varför den befintliga CE-märkningen fortsatt ansetts vara giltig. Vid ändring (modifiering) av en produkt ska alltid riskreducerande åtgärder vidtas för de identifierade olycksriskerna. Verifiering ska ske mot EU-direktivens krav och resultatet dokumenteras. Detta görs även om slutsatsen är att CE-märkningen inklusive uppfyllande av de grundläggande hälso- och säkerhetskraven, inte har påverkats genom ändringen (modifieringen). En sådan ändring (modifiering) betecknas då som en *ej väsentlig ändring.*

En *väsentlig ändring* medför att sättet som produkten uppfyller EU-direktivets grundläggande hälso- och säkerhetskrav har förändrats, varför bedömning om överensstämmelse och CE-märkningen behöver göras om. Detta är normalt svårt och omständligt. I tveksamma fall rekommenderas att en kontakt tas med tillverkaren som utförde CE-märkningen för en diskussion om den planerade ändringen (modifieringen) innan den införs.

18.6 Tillfälliga ändringar (modifieringar) som införs av Försvarsmakten

Vid tillfälliga ändringar (modifieringar) såsom teknisk anpassning, tillfällig reparation eller krigsskadereparation behöver beslutsunderlag avseende systemsäkerhet tas fram för den aktuella situationen i nödvändig omfattning.

18.6.1 Teknisk anpassning

Med teknisk anpassning avses en tillfällig ändring (modifiering) av ett tekniskt system som direkt efter avslutad verksamhet ska återställas till ursprunglig och fastställd konfiguration. Teknisk anpassning genomförs via Teknisk order (TO) beslutad av av tekniskt designansvarig.

Teknisk anpassning bör ur systemsäkerhetssynvinkel omfatta följande:

- Krav på beslutsunderlag (beskrivning av syftet med teknisk anpassning, alternativa möjliga åtgärder, för- och nackdelar med respektive alternativ)
- Minimikrav på systemsäkerhetsanalys
- Minimikrav på dokumentation av genomförd åtgärd
- Minimikrav på materieldokumentation till användaren
- Hur rapportering av genomförd åtgärd för tekniskt system (visst exemplar) ska ske
- När och hur beslut tas om återställande av tekniskt system
- Hur rapportering ska ske av att tekniskt system (visst exemplar) återställts efter teknisk anpassning.

18.6.2 Tillfällig reparation eller krigsskadereparation

Med tillfällig reparation eller krigsskadereparation avses en alternativ reparation med icke ordinarie metod och/eller med reparationskomponenter (ersättning för originalreservdel) i avvaktan på ordinarie reparation.

Tillfällig reparation eller krigsskadereparation kan vara aktuell vid exempelvis omhändertagande av tekniska system som behöver flyttas i avvaktan på bärgning eller bogsering till verkstad.

Försvarsmakten beslutar fortlöpande om alternativa reparationsmetoder. Beslut om reperationsmetoder utanför fastställda underhållsinstruktioner bör ur systemsäkerhetssynvinkel omfatta följande:

- Beslutsrätt
- Krav på beslutsunderlag (beskrivning av inträffad händelse/skada/trend, alternativa möjliga åtgärder, för- och nackdelar med respektive alternativ)
- Minimikrav på systemsäkerhetsanalys
- Minimikrav på dokumentation av genomförd åtgärd
- Minimikrav på materieldokumentation till användare
- Hur rapportering av genomförd åtgärd för tekniskt system (visst exemplar) ska ske
- När och hur beslut tas om återställande av tekniskt system
- Hur rapportering av att tekniskt system (visst exemplar) återställts efter tillfällig reparation/krigsskadereparation

18.7 Äldre materiel som saknar systemsäkerhetsbeslut

Försvarsmakten fattade år 1996 beslut om att alla nya eller modifierade tekniska system och produkter ska ha systemsäkerhetsbeslut. Systemsäkerhetsbeslut krävs dels för att Försvarsmakten ska ta emot materielen, dels för att materielen ska kunna tas i bruk ute på förband. Tekniska system och produkter som tagits i bruk före 1996 betraktas som *de facto* godkända (beprövat system) och kräver normalt inga systemsäkerhetsbeslut så länge de används och underhålls i enlighet med de drifterfarenheter som finns.

Om det finns materiel i bruk som inför ändring (modifiering) saknar systemsäkerhetsbeslut så behöver detta hanteras av Försvarsmakten innan konfigurationsöverlämningen (KÖL).

Försvarsmakten kan välja att retroaktivt genomföra ett komplett systemsäkerhetsarbete för det kompletta tekniska systemet eller att endast ställa krav på att genomföra systemsäkerhetsarbete på de delar som omfattas av ändringen (modifieringen). Systemsäkerhetsbesluten kommer då att få den omfattning som väljs enligt ovan.

Om Försvarsmakten väljer att genomföra ett retroaktivt systemsäkerhetsarbete för det kompletta tekniska systemet så behöver om möjligt den ursprungliga dokumentationen tas fram som en gång i tiden godkände materielen för att tas i bruk. Med denna dokumentation som grund kan ett fullständigt systemsäkerhetsarbete genomföras.

Alternativt kan det tekniska systemet hanteras som ett beprövat system, där trovärdiga och spårbara drifterfarenheter åberopas. Detta kan bland annat omfatta att analysera tidigare olycks-, tillbuds- och felrapporter. Resultatet av systemsäkerhetsanalysen dokumenteras i en *Systemsäkerhetsrapport* (SAR) och är underlag till aktuella systemsäkerhetsbeslut.

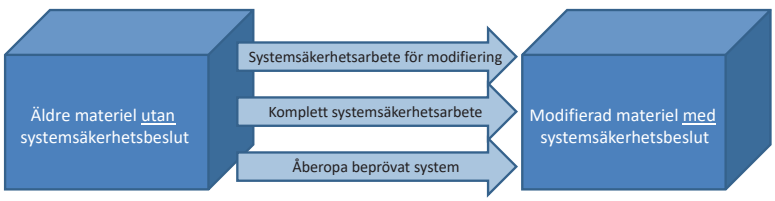


Bild 18.2 *Tre alternativa sätt att hantera systemsäkerhetsarbetet vid modifiering av äldre materiel.*

19 Avveckling av tekniska system

Syftet med detta kapitel är att beskriva omfattningen av det systemsäkerhetsarbete som behöver genomföras beroende på vilket sätt som tekniska system och produkter ska avvecklas.

19.1 Bakgrund till avvecklingsarbetet

Försvarsmakten är ägarföreträdare för statens försvarsmateriel. Tekniska system med undantag för militär materiel innehåller ofta komponenter med stora energier eller med flera dolda/inbyggda riskkällor. Försvarsmakten behöver därför identifiera de olycksrisker som kan inträffa under den fysiska avvecklingen av aktuellt tekniskt system.

Det är Försvarsmaktens ansvar att upplysa den som förvärvar materiel för fortsatt användning eller tar emot materiel för destruering/skrotning, om vilka dessa olycksrisker är och vilka egenskaper aktuella riskkällor har. Det gäller främst sådana egenskaper som normalt inte finns på materiel utan undantag för militär materiel. Försvarsmakten bör således se till att materielen erbjuder betryggande säkerhet.

All materiel som avvecklas är att se som tagen i bruk, det vill säga att den betraktas som begagnad. Försvarsmakten beslutar om totalavveckling, delutgallring eller kassation av materiel. Avveckling av materiel kan ske på olika sätt såsom överlåtelse, försäljning eller destruktion. Materielen kan även överlåtas som museiföremål eller uppvisningsföremål. Överlåtelse- och exportrestriktioner kan finnas för viss materiel som exempelvis klassats som krigsmateriel.

19.2 Slutförbrukning

Med slutförbrukning, innan totalavveckling sker, innebär att produkterna, exempelvis ammunition eller batterier, används tills de tar slut. Om driftprofiler förändras kan behov finnas att utfärda uppdaterade *Systemsäkerhetsgodkännanden* (SSG).

19.3 Genomförande av systemsäkerhetsanalys inför avveckling

Försvarsmakten tillser att en *Riskanalys inför avveckling av system* (RADS) genomförs. Syftet med denna systemsäkerhetsanalys (RADS) är att identifiera och analysera olycksrisker som kan inträffa vid den fysiska avvecklingen. Olycksriskerna är relaterade till materielen eller till avvecklingsmetoden (inklusive verktyg och arbetsoperationer). Om det tekniska systemet är relativt modernt, det vill säga att systemsäkerhetsanalys har genomförts vid anskaffning, finns mycket information om det tekniska systemets potentiella olycksrisker i samband med planerad avveckling redan identifierad. Vidare kan materieldokumentation i form av reparationshandböcker och reservdelskataloger nyttjas i *Riskanalys inför avveckling av system* (RADS) samt användas vid borttagning av delsystem och komponenter.

Om Försvarsmaktens systemsäkerhetsmetodik inte har följts vid anskaffning kommer *Riskanalys inför avveckling av system* (RADS) att bli mer omfattande. Detta gäller också om det finns brister i dokumentation om typkonfiguration eller om materielen otillbörligt har modifierats under vidmakthållandeskedet och dokumentation för detta saknas eller är bristfällig. Försvarsmakten genomför konfigurationsöverlämningen (KÖL) till aktör som genomför destruktionen.

Nedan beskrivs det systemsäkerhetsarbete som behöver genomföras under avvecklingsskedet beroende på det tekniska systemets komplexitet, beskaffenhet och riskinnehåll.

19.3.1 Överlåtelse

Med överlåtelse menas att tekniska system eller produkter överlämnas (ges bort) av Försvarsmakten till en ny ägare såsom statliga eller kommunala verksamheter alternativt till humanitära och frivilliga organisationer. Försvarsmakten behöver dokumentera status/brister på varje exemplar eller produkt samt att tillräcklig produktinformation för typkonfigurationen finns tillgänglig. Produktinformation kan utgöras av materieldokumentation för användning och underhåll inklusive underhållsdokumentation, scheman, ritningar, säkerhetsdatablad, systemsäkerhetsanalyser och utbildningsmateriel. Information behöver lämnas om sådana egenskaper hos materielen som normalt inte finns på militär materiel.

Vissa undantag för militär materiel som är direkt kopplade till Försvarsmaktens användning kan upphöra att gälla, vilket beror på hur undantaget har formulerats i aktuellt regelverk. Det blir den nye ägarens ansvar att undersöka vilka konsekvenser detta får, exempelvis om nya verifieringar respektive godkännanden behövs eller om användningen får begränsningar.

Utöver eventuellt slutanvändarintyg kan det även finnas överlåtelse- och exportrestriktioner.

19.3.2 Försäljning

Med försäljning menas att tekniska system eller produkter säljs till juridiska personer (företag, organisationer) eller envar. Försvarsmakten behöver dokumentera statusen/brister på varje exemplar eller produkt samt att tillräcklig produktinformation finns tillgänglig. Produktinformation ska minst utgöras av materieldokumentation för användning och underhåll. Till juridiska personer bör även scheman, ritningar, säkerhetsdatablad, systemsäkerhetsanalyser och utbildningsmateriel överlämnas. Information behöver lämnas om sådana egenskaper hos materielen som normalt inte finns på militär materiel.

Vissa undantag för militär materiel som är direkt kopplade till Försvarsmaktens användning kan upphöra att gälla, vilket beror på hur undantaget har formulerats i aktuellt regelverk. Det blir den nye ägarens ansvar att undersöka vilka konsekvenser detta får, exempelvis om nya verifieringar respektive godkännanden behövs eller om användningen får begränsningar.

Äldre produkter (som om de vore nya skulle omfattas av CE-märkning/rattmärkning) som inte är CE-märkta/rattmärkta kan försäljas, men man bör vara medveten om att de är mindre attraktiva på marknaden, särskilt för ny ägare som är arbetsgivare då denne exempelvis har att beakta föreskrifter (AFS 2006:4) Användning av arbetsutrustning, som även ställer vissa tekniska krav. Produkter som är maskiner får hanteras från fall till fall.

Detta kan betyda att möjligheter till intäkter till Försvarsmakten går förlorade och kostnader för avveckling får tas. Att i efterhand försöka CE-märka/rattmärka en produkt kan kosta mycket stora belopp, om det ens är möjligt att få fram de tekniska data som erfordras.

CE-märkning/rattmärkning bör därför eftersträvas då materielen anskaffas. Detta innebär även att den som frivilligt eller ej, CE-märker/rattmärker en sådan produkt i efterhand är att betrakta som legal tillverkare med allt vad det innebär av ansvar och förpliktelser.

19.3.3 Destruktion

Med destruktion menas att tekniska system eller produkter destrueras. Notera dock att vissa delsystem och komponenter kan omhändertas av Försvarsmakten innan destruktion om de kan återanvändas i liknande tekniska system.

Ett tekniskt system förbereds genom att det töms på farliga ämnen, strålkällor avlägsnas, spända fjädrar/tryckkärl eller andra konstruktioner avlastas samt att främmande föremål såsom kvarglömd ammunition eller andra främmande föremål tas bort. Komponenter som omfattas av producentansvar sorteras ut och lämnas till de insamlingssystem som producenterna tillhandahåller. Försvarsmakten kan genom Destruktionsintyg informera om ovanstående och låta den aktör som genomför destruktionen hantera detta.

Information om farliga ämnen/ytbehandlingar som är dolda eller svåra att upptäcka, exempelvis ämnen enligt artikel 33 i EU-förordningen REACH och som finns på dess kandidatförteckning, ska lämnas till destruktören genom Försvarsmaktens försorg. Sådan information kan finnas angiven i Återvinningsmanual eller motsvarande dokument.

Försvarsmakten administrerar Destruktionsintygen.

19.3.4 Museiföremål

Med museiföremål menas att tekniska system eller produkter överlåts för att ställas ut till allmän beskådan på museum eller motsvarande. Ett museum är att se som ny ägare av materielen såvida muséet inte finns organiserat vid ett förband.

Komplett produktinformation, om sådan finns tillgänglig, överlämnas till muséet och kan utgöras av materieldokumentation för användning och underhåll inklusive underhållsdokumentation, scheman, ritningar, säkerhetsdatablad, systemsäkerhetsanalys och utbildningsmateriel. Information behöver lämnas om sådana egenskaper hos materielen som normalt inte finns på motsvarande civil materiel.

Vid förfrågan om överlämning av museiföremål till annat land kan det, utöver eventuellt slutanvändarintyg, även finnas överlåtelse- och exportrestriktioner, exempelvis för en del farliga ämnen eller för militära konstruktioner.

19.3.5 Uppvisningsföremål

Ett uppvisningsföremål är kvar i Försvarsmaktens ägo och kan exempelvis placeras ut vid ett förband. Uppvisningsföremålet ska normalt tömmas på allt innehåll, exempelvis motor, farliga ämnen och inredningar. Rörliga delar såsom dörrar och luckor bör svetsas igen och utstickande delar tas bort.

Begrepp

I denna handbok används ett stort antal begrepp som ur systemsäkerhetsperspektiv används för att förklara olika sammanhang. I de fallen handboken har egna ordförklaringar (egna formuleringar eller justerade från annan litteratur) anges ”H SystSäk 2022”.

Begrepp	Referens	Ordförklaringar
Aktivitet	FOI-R-3546-SE ISSN 1650-1942	En definierad mängd arbete som ska utföras, inklusive eventuella krav på indata och utdata.
ALARP	H SystSäk 2022	Begreppet ALARP (rimligen praktiskt genomförbart) innebär att man väger en olycksrisk mot de problem, den tid och de pengar som behövs för att reducera olycksrisken till en så låg nivå som det är praktiskt möjligt utifrån god praxis, dvs att etablerade standarder och *Designregler* (DR) har följts utifrån dagens tekniknivå.
Allmänna råd	H SDH 2021	Format för icke bindande regler i form av generella rekommendationer om tillämpningen av en författning som anger hur någon kan eller bör handla i ett visst hänseende.
Anläggningstekniska basresurser	H SystSäk 2022	Exempelvis resurser som el, kraft, värme, kyla, ventilation, vatten och avlopp.
Anmält organ	EU:s Blå bok 2016	Certifieringsorgan som utför uppgifter i samband med bedömning av överensstämmelse enligt EU-förordningar/EU-direktiv/EG-direktiv när en tredje parts deltagande är nödvändigt. Ibland tillåts frivillig användning av Anmält organ.
Anskaffning	H SystSäk 2022	Samlingsbegrepp för upphandling, inköp, lån, hyra, leasing, Foreign Military Sales (FMS), gåva, övertagande samt krigsbyte.
Användare	FOI-R-3546-SE ISSN 1650-1942	Någon som med behörighet avsiktligt interagerar med systemet för att uppnå ett syfte. Primära eller direkta användare interagerar direkt med systemet, medan sekundära användare interagerar med systemet via direkta användare
Användbarhet	Baserat på definitionen i ISO 9241-11	Den grad i vilken specifik användare i givna sammanhang kan bruka en produkt för att uppnå specifika mål på ett ändamålsenligt, effektivt och för användaren tillfredsställande sätt.

Begrepp	Referens	Ordförklaringar
Avveckling	H SystSäk 2022	Kvittblivning av materiel genom slutförbrukning, försäljning, överlåtelse eller destruktion/deponi.
Arbetsmiljö	WHO	En sammanfattande benämning på biologiska, medicinska, fysiologiska, psykologiska, sociala och tekniska faktorer som i arbetssituationen eller i arbetsplatsens omgivning påverkar individen.
Begränsning	H SystSäk 2022	Permanent inskränkning i det tänkta nyttjandet.
Betryggande säkerhet	H SystSäk 2022	Samhällets accepterade risknivå uppnås genom att följa lagstiftning och etablerade standarder.
Begränsat tolerabel (BT)	H SystSäk 2022	För olycksrisk i gult område ska beställaren förvissa sig om att den högsta skadeklassen av olycksrisken bedöms rymmas inom *Tolerabel risknivå* (TR) genom att granska att argument och belägg samt att de särskilt ställda kraven på ALARP avseende gula cellerna är uppfyllda.
Belägg	H SystSäk 2022	Bevis eller andra uppgifter som helt eller delvis styrker olika argument.
Beslutsgrind	FOI-R-3546-SE ISSN 1650-1942	Kontrollpunkt mellan olika livscykelskeden. De principiella, övergripande besluten baserade på fördefinierade beslutskriterier, som tas vid respektive beslut.
Beställare	H SystSäk 2022	Aktör som genomför anskaffning och som överlämnar materiel till kravställaren.
Bidragande orsaker	H SystSäk 2022	Förhållanden som tillsammans med en riskkälla ger förutsättningar för en vådahändelse.
CE-märkning	EU:s Blå bok 2016	Märkningen, som görs av tillverkaren, anger att produkten överensstämmer med den EU-lagstiftning (överförd till nationell lagstiftning) som är tillämplig på produkten och att den därmed kan släppas ut på den inre marknaden.
COTS-produkter	H SystSäk 2022	Till COTS-produkter (Commercial off the shelf) hör komplexa produkter som redan finns på marknaden och som kan vara godkända av ackrediterat organ mot internationella standarder.
Designregler	H SystSäk 2022	Konstruktionspåverkande krav.
Distributör	Tradepartners-Sweden	En distributör är en ekonomisk aktör som köper in varor och säljer därefter själv varorna till kunden. Distributören har sitt eget lager, skickar till och fakturerar själv sin kund.
Ej tolerabel (ET)	H SystSäk 2022	För olycksrisk i rött (ET) område i riskmatris ska riskeliminering/-reducering ske för att underskrida krav på *Tolerabel risknivå* (TR).

Begrepp	Referens	Ordförklaringar
Ergonomi	IEA, International Ergonomics Association	Vetenskaplig disciplin som handlar om att förstå interaktioner mellan människor och andra delar av ett system samt profession i vilken man tillämpar teori, principer, data och metoder för att i design optimera människors välbefinnande och övergripande systemprestanda.
Evaluering	H SystSäk 2022	Undersökning av vilka egenskaper ett tekniskt system har samt hur det kan användas och komma till nytta i andra sammanhang.
Exponeringsfaktor	H SystSäk 2022	Sannolikheten för att en användare ej är närvarande och blir exponerad för vådahändelse när den inträffar.
Fas	SAM0 2020	En indelning av ett tekniskt systems livscykel som anges i regeringens direktiv för investeringsplanering.
Farliga ämnen	Wikipedia	Är enligt europeisk lagstiftning kemikalier som är svårnedbrytbara, koncentreras i näringskedjan (bioackumulativa) och har en eller flera giftiga egenskaper.
Farligt tillstånd	H SystSäk 2022	En fysisk situation som kan leda till en olycka.
Förband	H SystSäk 2022	Är personellt och materiellt del av Försvarsmaktens bas- eller insatsorganisation och som bär Försvarsmaktens olika förmågor.
Förfrågningsunderlag	H SystSäk 2022	Innehåller en beskrivning som tydligt visar vad beställaren vill ha. Kan omfatta Teknisk specifikation (TS) och Verksamhetsåtagandespecifikation (VÅS).
Försök	H SystSäk 2022	Användning av fastställd materiel i syfte att utvärdera dess lämplighet i en given användningssituation.
Funktionssäkerhet	Svensk standard SS 441 05 05, Tillförlitlighet	Förmågan hos ett system (enhet) att utföra en krävd funktion under givna förhållanden under ett givet tidsintervall.
Föreskrift (FFS)	H SDH 2021	Format för bindande rättsregler som kännetecknas av att de inte avser ett enskilt fall utan har generell tillämplighet. Försvarsmaktens föreskrifter publiceras i Försvarets författningssamling (FFS). En föreskrift kräver alltid ett bemyndigande i en förordning och kan gälla både inom och utom Försvarsmakten.
Förmåga	H MÅL FÖRB 2011	Förhållandet att någon (ett förband) förmår eller kan göra/uträtta något.

Begrepp	Referens	Ordförklaringar
Försäkran om överensstämmelse	EU:s Blå bok 2016	Det dokument där tillverkaren anger och intygar att produktindividen uppfyller alla relevanta krav i tillämplig lagstiftning. Kallas även för EU/EG-försäkran om överensstämmelse.
Handbok	H SDH 2021	Handlingstyp för anvisningar med förklaringar och beskrivningar avseende en viss verksamhet eller administration och förvaltning. I en handbok får man återge lagar, förordningar, föreskrifter, reglementen och manualer. En handbok får även innehålla riktlinjer, råd och rekommendationer med bilder för tillämpning av regler och bestämmelser. I en handbok kan även rutiner och processer beskrivas, vilka kan publiceras separat på Försvarsmaktens intranät. De rutiner, processer, råd, riktlinjer och rekommendationer m.m. som anges bör alltid följas om inte särskilda skäl föreligger att genomföra verksamheten på annat sätt.
Hantering	H SystSäk 2022	Användning (utbildning, övning och insats), underhåll, förrådshållning (transport) samt avveckling.
Harmoniserad standard	EU:s Blå bok 2016	En europeisk standard som antagits på grundval av ett mandat från EU-kommissionen för tillämpning av en rättsakt i unionens harmoniseringslagstiftning, t.ex. ett visst EU-direktiv, och angivits i EU:s gemensamma tidning. Harmoniserad standard är frivillig att tillämpa, om inte annat avtalas.
Humanfaktorer	Wikipedia	Tillämpningen av psykologiska och fysiologiska principer på konstruktion av produkter, processer och system.
Insats	FOI-R-3546-SE ISSN 1650-1942	Avgränsad verksamhet som utförs i syfte att uppnå strategiska, operativa eller taktiska mål.
Integrerad/inbyggd säkerhet	Maskindirektivet, bilaga I.	(Olycks-)risker ska undanröjas, reduceras i en viss prioriteringsordning där åtgärder i konstruktion, är första steget. Förfarandet kallas integration av säkerheten, (Integration of Safety).
Interna bestämmelser (FIB)	H SDH 2021	Format för bindande rättsregler som kännetecknas av att de inte avser ett enskilt fall utan har generell tillämpning där ett bemyndigande i förordning saknas. Interna bestämmelser gäller enbart inom Försvarsmakten.
Interoperabilitet	FOI-R-3546-SE ISSN 1650-1942	Förmåga till extern kommunikation och resurshantering syftande till att kunna fungera effektivt tillsammans med andra.

Begrepp	Referens	Ordförklaringar
Komponent	FOI-R-3546-SE ISSN 1650-1942	En enhet, med diskret struktur inom ett system, som interagerar med andra komponenter i systemet och därmed bidrar på lägsta nivå till systemets egenskaper och karakteristika.
Koncept	FOI-R-3546-SE ISSN 1650-1942	En bärande idé eller grundläggande föreställning om hur olika delar ska kombineras eller samordnas.
Konstruktör	Boverket Wikipedia	Leverantör som uppfyller ställda kontraktskrav genom att konstruera eller uppfinna något samt även den som utför konstruktionsritningar och genomför beräkningar.
Kontrakt	H SystSäk 2022	Dokument som bland annat refererar till specificerade systemsäkerhetskrav (Teknisk specifikation och/eller Verksamhetsåtagandespecifikation) mellan beställare och konstruktör.
Krav	FOI-R-3546-SE	Specificerar vad system ska åstadkomma. Krav kan delas in i funktionella och icke-funktionella krav där de funktionella kraven beskriver vad som ska åstadkommas medan de icke-funktionella kraven beskriver vilka egenskaper systemet måste ha.
Kravställare	FOI-R-3546-SE ISSN 1650-1942	Aktör som möjliggör en samordnad, integrerad och helhetsbaserad beskrivning av efterfrågade förmågor hos framtida tekniska system. Aktören kontrollerar kravuppfyllnad och fattar erforderliga beslut.
Livscykel	FOI-R-3546-SE ISSN 1650-1942	Evolution av ett system, produkt, tjänst, projekt eller någon annan mänskligt tillverkad entitet från skapelse till avveckling.
Militär materiel	H SystSäk 2022	Militär materiel ur systemsäkerhetsperspektiv har konstruerats och tillverkats (även genom integration till ett system-av-system) för militärt ändamål, där regelverk kan medge undantag eller där civila standarder saknas.
Militär materiel särskilt konstruerad och tillverkad för visst militärt ändamål	H SystSäk 2022	Är ur systemsäkerhetsperspektiv är när ett tekniskt system har konstruerats och tillverkats (även genom integration till ett system-av-system) för att i sin militära funktion (organiserad väpnad strid) ha en direkt förstörelsebringande effekt.
Militärt ändamål	H SystSäk 2022	Avser militär verksamhet som endast är tillåten att genomföras av Försvarsmakten under övning och insats.

Begrepp	Referens	Ordförklaringar
MOTS-produkter	H SystSäk 2022	Till MOTS-produkter (Military off the shelf) hör kommersiellt tillgängliga färdiga produkter såsom hårdvara eller programvara, för användning av militären Produkterna kan inte köpas av envar.
Mål	FOI-R-3546-SE ISSN 1650-1942	Ett mätbart resultat (läge) vilket ska uppnås vid en bestämd angiven tidpunkt.
Olycka	H SystSäk 2022	En olycka inträffar då person, egendom och/eller yttre miljö skadas av riskkällan som följd av att vådahändelsen inträffar.
Omgivningsmiljö	H SystSäk 2022	Utgörs av andra tekniska system och produkter (även farliga ämnen), anläggningar samt natur och klimat. Det tekniska systemets gränsytor mot omgivningsmiljön kan vara mekaniska, elektriska eller informationsteknologiska.
Personer	H SystSäk 2022	Individer behövs för att hantera ett tekniskt system och utgörs exempelvis av användare, underhålls-, förråds- och transportpersonal, vilka kan inneha en militär eller civil anställning, vara anslutna till Hemvärnet, tillhöra en frivillig försvarsorganisation eller vara värnpliktiga.
Produktansvar	Produktansvarslagen, SFS 1992:18	Det ansvar en ekonomisk aktör har för skador som en produkt kan orsaka på grund av en säkerhetsbrist. Avser enbart ekonomisk ersättning (skadestånd) när en produkt har orsakat en skada. Produkten ska vara i omlopp, dvs släppt på marknaden.
Produktsäkerhetsansvar	EU:s direktiv för olika produkter, cirka 25 st. EU:s Blå bok 2016	Det ansvar en Tillverkare (Importör) har för en produkt så att den är tillräckligt säker när den släpps på marknaden. Ansvaret innefattar att korrekt utföra ett flertal aktiviteter, inklusive eventuell certifiering, innan produkten märks med t.ex. CE-märkning. I EU-direktiven finns även ett ansvar för eftermarknaden då produkten distribueras, används. I denna handbok är produktanvändaren att betrakta som professionell.
Rattmärkning	EU:s direktiv 2014/90/EU	Märkningen, som görs av tillverkaren, anger att produkten överensstämmer med EU:s direktiv 2014/90 om marin utrustning (motsvarande nationell lagstiftning).

Begrepp	Referens	Ordförklaringar
Reglemente	H SDH 2021	Handlingstyp för bindande bestämmelser om ledning och genomförande av, eller förhållningssätt för, verksamhet inom Försvarsmakten. Ett reglemente får innehålla detaljerade och vägledande förklaringar samt beskrivningar och bilder.
Restriktion	H SystSäk 2022	Tillfällig inskränkning i det tänkta nyttjandet.
Riskkälla	H SystSäk 2022	Farlig egenskap som kan leda till skada på person, egendom eller yttre miljö. Kan även vara ett naturfenomen.
Riskmedvetande	FHS, Ledarskapsinstitutionen Räddningsverkets handlingsprogram	Kännedom, kunskap och förhållningssätt till olycksrisker och lämpliga åtgärder.
Risknummer	H SystSäk 2022	Unika löpnummer på enskilda olycksrisker för ett visst tekniskt system.
Riskreducering	H SystSäk 2022	Riskreducerande åtgärderna som redovisas med belägg för att kunna flytta olycksrisker i riskmatrisen efter åtgärd.
Skadeklass	H SystSäk 2022	Personskada: Dödsfall, allvarlig personskada, mindre allvarlig personskada och försumbar personskada. Ekonomisk skada: Katastrofal egendomsskada, kritisk egendomsskada, allvarlig egendomsskada, försumbar egendomsskada. Miljöskada: Katastrofal miljöskada, kritisk miljöskada, allvarlig miljöskada, försumbar miljöskada.
Slutförbrukning	H SystSäk 2022	Produkterna, t.ex. ammunition i förråd, används tills de tar slut.
Släppa ut på marknaden	EU:s Blå bok 2016	En produkt släpps ut på marknaden när den tillhandahålls i EES/inre marknaden, t.ex. i medlemsstaten Sverige, för första gången, för att kunna tas i bruk. Avser varje individuell produkt. Begreppet avser en tidpunkt. Tillhandahållande inkluderar försäljning, lån, hyra, gåva mm.
Styrbarhetsfaktor	H SystSäk 2022	Med styrbarhetsfaktorer menas att användaren själv kan påverka ett farligt tillstånd genom att stoppa händelsekedjan eller ta visst skydd innan vådahändelsen inträffar.

Begrepp	Referens	Ordförklaringar
System-av-system	Baserat på definitionen i FOI-R-1830-SE	Flera system som samverkar, men saknar gemensamma ägare och policys. För de ingående tekniska systemen finns olika systemsäkerhetsbeslut utfärdade och dessa tekniska system kan vara godkända mot olika krav.
Systemintegratör	Baserat på definitionen i FOI-R-3546-SE ISSN 1650-1942	Aktör med uppgift att kombinera tekniska system, programvaror, eller både och, till ett system-av-system.
Systemmålsättning	FOI-R-3546-SE ISSN 1650-1942	Systemmålsättningar tas fram för att bestämma Försvarsmaktens krav på ett tekniskt system som avses anskaffas för att tillgodose ett identifierat behov, företrädesvis med grund i en eller flera förbandsmålsättningar. Systemmålsättningar kan också vara relativt fristående förbandsmålsättningar, exempelvis avseende försvarsmaktsgemensamma materiel såsom uniformssystem och ammunition.
Systemsäkerhetsvärdering (SSV)	H SystSäk 2022	Redovisning av argument och belägg för att bekräfta att ställda systemsäkerhetskrav är uppfyllda för använda vägval enligt Vägvalsmodellen. Det tekniska systemet (produkten) är säkert därför att:
Systemsäkerhet	H SystSäk 2022	Egenskapen hos ett tekniskt system att inte oavsiktligt orsaka skada på person, egendom eller yttre miljö.
Systemsäkerhetsanalys	H SystSäk 2022	Att systematiskt använda sig av tillgänglig information för att beskriva och utreda olycksrisker.
Systemsäkerhetsarbete	H SystSäk 2022	Det totala arbetet som bedrivs för ett visst tekniskt system under samtliga livscykelskeden i syfte att identifiera, analysera, värdera och klassificera olycksrisker, eliminera eller reducera dessa mot ställda krav.
Systemsäkerhetsbeslut	H SystSäk 2022	Ett samlingsbegrepp för systemsäkerhetsutlåtande, systemsäkerhetsdeklaration och systemsäkerhetsgodkännande.
Systemsäkerhetsmål	H SystSäk 2022	Systemsäkerhetsmål är de mål ett produktområde eller tekniskt system har för att uppfylla Tolerabel risknivå (TR) för att kunna uppfylla sin del i en funktionskedja. Systemsäkerhetskraven som följer blir då beroende av om produktområdet ingår i ett säkerhetsmål som definieras per arena.

Begrepp	Referens	Ordförklaringar
Systemsäkerhets-verksamhet	H SystSäk 2022	Det totala arbetet som bedrivs för tekniska system och produkter under samtliga livscykelskeden i syfte att ställa krav, genomföra systemsäkerhetsarbete och fatta systemsäkerhetsbeslut.
Säkerhetsdatablad	Kemikalieinspektionen	Ett dokument som innehåller information om kemiska produkters farliga egenskaper, risker och vilka skyddsåtgärder som ska vidtas. (Safety Data Sheet, SDS).
Säkerhetsmål	H SystSäk 2022	Säkerhetsmål är den övergripande inriktningen avseende vilken tolerabel risk en verksamhet kan acceptera. Säkerhetsmålen definierar vilka risker organisationen och omgivningen utsätts för när tekniken inom en funktionskedja inte fungerar som avsett. Säkerhetsmål definieras utifrån de mest säkerhetskritiska funktionskedjorna inom respektive teknisk arena (armén, marinen, flyg, ledning och logistik) som Försvarsmakten behöver upprätthålla för att kunna genomföra de uppdrag som anges i förordningen med instruktion till Försvarsmakten.
Ta i bruk	EU:s Blå bok 2016	Sker då produkten används inom EES, t.ex. i Sverige, av slutanvändaren för första gången och för de ändamål som produkten är avsedd för. Avser varje individuell produkt. Begreppet avser en tidpunkt. När produkten tas i bruk av en arbetsgivare och ska användas av anställda anses arbetsgivaren vara slutanvändaren.
Teknisk Order	H SDH 2021	Dokumentgrupp för skriftlig order som avser reglering av konfiguration, teknisk tjänst, tekniska system och materiel, innefattande drift, underhåll, vård och modifiering av förnödenheter.
Tekniskt system	H SystSäk 2022	Utgörs av komponenter, förbrukningsmateriel och programvaror samt materieldokumentation och tekniska data organiserade för att uppnå ett eller flera syften i en given omgivningsmiljö.
Tekniskt designansvar	SAM0 FM – FMV 2020	Tekniskt designansvar innebär att fastställd design för tillåtna konfigurationer av tekniska system (inklusive underhållslösningar) uppfyller lagkrav, fastställda målsättningar och övriga krav bl a avseende prestanda, funktion, informations- och systemsäkerhet över hela livscykeln.

Begrepp	Referens	Ordförklaringar
Test/försök	19FMV1007-2:1	Den verksamhet som genomförs under exempelvis utveckling/integration, för att utröna om och hur en lösning fungerar intill dess att ställda krav formellt ska verifieras och/eller valideras i en typlik konfiguration. Begreppen test/försök omfattas inte i begreppet VoV.
Tillbud	H SystSäk 2022	Med tillbud menas att en vådahändelse inträffar men den orsakar ingen skada. (En incident är exempelvis när främmande makt kränker svenskt luftrum och har ingenting med systemsäkerhet att göra).
Tillhandahållen materiel	H SystSäk 2022	Produkter som redan finns i Försvarsmaktens förvaltningssystem och som ställs till förfogande för integration. (Government Furnished Equipment, GFE).
Tillverkare	H SystSäk 2022	Fysisk eller juridisk person som konstruerar och/eller tillverkar, eller som låter konstruera och/eller tillverka en produkt och som ansvarar för att produkten överensstämmer med gällande produktlagstiftning i syfte att släppa ut den produkten på marknaden, i eget namn eller under eget varumärke. Tillverkning omfattar även den som sätter ihop, förpackar, bearbetar, märker eller väsentligt ändrar en produkt eller dess användning så uppfyllande av de väsentliga säkerhetskraven påverkas.
Tolerabel (T)	H SystSäk 2022	För olycksrisk i grönt område ska beställaren förvissa sig om att den högsta skadeklassen av olycksrisken bedöms rymmas inom Tolerabel risknivå (TR) genom att granska argument och belägg.
Tolerabel risk (för flygsäkerheten)	FM R LML	Flygvapenchefens (FVC) beslut om hur stora flygsäkerhetsrisker som kan tillåtas för en definierad verksamhet inom det militära luftfartssystemet i Försvarsmakten, dvs hur stora flygsäkerhetsrisker som kan accepteras i det militära luftfartssystemet under alla konfliktnivåer, såväl vid fredsproduktion som vid insatser.
Tolerabel risknivå (TR)	H SystSäk 2022	Försvarsmaktens accepterade risknivå för olycksrisker som behöver värderas i en riskmatris och där acceptansnivån kan vara både högre eller lägre än betryggande säkerhet.
Tredje person/ persons egendom	H SystSäk 2022	Person och/eller dennes egendom som inte är involverad i pågående verksamhet.

Begrepp	Referens	Ordförklaringar
Tredjepartsorgan	Bl.a. EU:s Blå bok 2016	Kompetent organ/laboratorium fristående från tillverkare, användare, myndighet som utför bedömning av produkter (personer) och/eller kvalitetssystem; ofta i samband med bedömning av överensstämmelse med regelverk. Exempelvis ackrediterade organ som arbetar som anmälda organ.
Underhålls-instruktioner	H SystSäk 2022	Svensk översättning av engelskans servicemanual och är avsedd för teknisk personal som ska underhålla, reparera eller kalibrera produkten. Teknisk personal kan finnas inom tillverkarens egen organisation eller hos annan aktör.
Utlösande faktor	H SystSäk 2022	En utlösande faktor är en mekanism som tillsammans med en riskkälla och bidragande orsaker åstadkommer en vådahändelse.
Validering	19FMV1007-2:1	Bekräftelse genom att framlägga bevis på att krav för en specifik, avsedd användning eller tillämpning har uppfyllts.
Verifiering	19FMV1007-2:1	Bekräftelse genom att framlägga bevis på att specificerade krav har uppfyllts.
Verksamhetsregler	H SystSäk 2022	Begränsningar eller restriktioner i användningen av tekniska system eller produkter i syfte att hantera kvarstående olycksrisker.
Verksamhets-säkerhet	H SystSäk 2022	Ur systemsäkerhetsperspektiv avses Försvarsmaktens förmåga att hantera olycksrisker vid all verksamhet så att de författningsenliga kraven på arbetsmiljö och säkerhet för Försvarsmaktens personal samt säkerhet för tredje person, egendom och yttre miljö uppfylls.
Vision	FOI-R-3546-SE ISSN 1650-1942	Beskrivning av önskade egenskaper utan de krav på precision som mål och krav ska innehålla och avser som oftast att beskriva långsiktiga önskemål.
Vådahändelse	H SystSäk 2022	En vådahändelse inträffar oavsiktligt och utan uppsåt och kan resultera i olycka eller tillbud.
Ändringar	H SystSäk 2022	Inkluderar modifieringar (permanenta eller tillfälliga), ändrade verksamhetsregler, ändrad materieldokumentation för användning och underhåll, ändrad omgivningsmiljö samt ändrad utbildning.
Ändringsbara parameterintervall	H SystSäk 2022	Godkända intervall för programvaruinställningar samt tillåtna uppdateringar av enskilda data eller databaser.

Akronymer/förkortningar

Akronym/förkortning	Förklaring
AFS	Arbetsmiljöverkets författningssamling
ALARP	As Low as Reasonably Practicable
ANSI	American National Standard Institute
AOP	Allied Ordnance Publication (NATO)
AP	Allied Publications (NATO)
ASIL	Automotive Safety Integrity Level
BAAINBw	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr. Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (Tyskland)
BOAC	Beslut om användning, central nivå
BOAL	Beslut om användning, lokal nivå
BRI	Brand- och räddningsinstruktion
BT	Begränsat tolerabel
C OrgE	Chef för organisationsenhet
CAS	Chemical Abstract Service
CDR	Critical Design Review Kritisk konstruktionsgranskning
CE	Conformité Européenne Europeisk överensstämmelse/efterlevnad (EES)
CEN	European Committee for Standardization
CENELEC, CLC	Committee for Electrotechnical Standardization (Europa)
CI	Critical Item Kritisk egenskap
CIP	Commission Internationale Permanente pour l'épreuve des armes à feu portatives; Permanent International Commission for Firearms Testing
CIL	Critical Item List
CLP	Classification, Labelling and Packaging (of substances and mixtures)
COTS	Commercial Off the Shelf
DEF-STAN	Defence Standard; Brittisk försvarsstandard
DID	Data Item Descriptions; dokumentvägledningar (USA)
DoC	Declaration of Conformity Försäkran om överensstämmelse
DoD	Department of Defense (USA)

Akronym/förkortning	Förklaring
DoDI	Department of Defense Instruction (USA)
DR	Designregel
EASA	European Aviation Safety Agency
EDA	European Defence Agency
EES	Europeiska ekonomiska samarbetsområdet
EGT	EU:s /EG:s gemensamma tidning
EHA	Miljörelaterad riskanalys Environmental Hazard Analysis
EHAR	Miljörelaterade riskanalysrapport
ELSÄK-FS	Elsäkerhetsverkets författningssamling
EMAR	European Military Airworthiness Requirements
EMCD	Electromagnetic Compatibility Directive
EN	European Norm; europeisk standard
ET	Ej tolerabel
ETSI	European Telecommunications Standards Institute
FBD	Funktionella blockdiagram
FFS	Försvarets författningssamling
FHA	Funktionell riskanalys Functional Hazard Analysis
FHS	Försvarshögskolan
FIB	Försvarsmaktens interna bestämmelser
FIHM	Försvarsinspektören för hälsa och miljö
FLYGI	Militära flyginspektionen
FM	Försvarsmakten
FM BMTS	Försvarsmaktens beslutssystem för tekniska system
FMECA	Feleffektanalys Failure Mode and Effects Analysis
FMS	Foreign Military Sales
FMUK	Försvarsmaktens undersökningskommission
FMV	Försvarets materielverk
FORTV	Fortifikationsverket
FoT	Forskning och teknikutveckling
FRACAS	Felrapporteringssystem Failure Reporting Analysis and Corrective Action System
FSD	Svensk försvarsstandard (publikation) respektive Försvarsstandardiseringssekretariatet (enhet vid FMV)

Akronym/förkortning	Förklaring
FSI	Flygsäkerhetsinspektören
FTA	Felträdsanalys Fault Tree Analysis
GAO	Government Accountability Office (USA)
GEIA	Government Electronics & Information Technology Association (SAE)
GFE	Government Furnished Equipment, Av staten tillhandahållen materiel
HFI	Hälsorelaterad riskanalys Human Factors Integration
HHA	Hälsorelaterad riskanalys Health Hazard Analysis
HHAR	Hälsorelaterad riskanalysrapport
HL	Risklista Hazard Log
HMAR	Hazard Management Assessment Report
HMI	Human Machine Integration
HMMP	Hazardous Material Management Plan
HMP	Hazard Management Plan
HMPR	Hazard Management Progress Report
HTS	Riskhanteringssystem Hazard Tracking System
HUD	Head up display
IACS	International Association of Classification Societies
IEC	International Electrotechnical Commission
IPT/WG	Integrated Product Team / Working Group support
ISO	International Organization for Standardization
ITAA	Information Technology Association of America
ITS	Svenska Informations- och Telekommunikationsstandardiseringen
ITU	International Telecommunication Union
IVDR	In-Vitro Devices Regulation, Förordning (EU) 2017/746 om medicintekniska produkter för in-vitro diagnostik
JSP	Joint Service Publication (UK)
KBV	Kustbevakningen
KÖL	Konfigurationsöverlämning
LC	Leveranscertifikat
LEDS	Ledningsstaben i högkvarteret

Akronym/förkortning	Förklaring
LFV	Luftfartsverket
LOU	Lag om offentlig upphandling
LUFS	Lag om upphandling på försvars- och säkerhetsområdet
LVD	Low Voltage Directive; lågspänningsdirektivet. Numera EU-direktiv om elektrisk utrustning
MCS	Minimal Cut Set
MD	Machinery Directive
MDR	Medical Devices Regulation, Förordning (EU) 2017/745 om medicintekniska produkter
MED	Marine Equipment Directive
MIFOR	Militära fordonsregistret
MIL-SPEC	Military Specifications (USA)
MIL-STD	Military Standard (USA)
MOA	Materielområdesansvarig
MOTS	Military off the shelf
MSB	Myndigheten för samhällsskydd och beredskap
MSBFS	Myndighetens för samhällsskydd och beredskap författningssamling
MTO	Människa, teknik och organisation
MTP	Medicinteknisk produkt
MTRF	Militärtrafikförordningen
MÖL	Materielöverlämning
NATO	North Atlantic Treaty Organization Nordatlantiska fördragsorganisationen
NSPA	NATO Support and Procurement Agency
O&SHA	Riskanalys inför hantering Operating and Support Hazard Analysis
O&SHAR	Riskanalysrapport för hantering
OJ	Official Journal; EG:s gemensamma tidning, EGT
ORM	Olycksriskmodellen
PARP	Partnership for Peace Planning and Review Process
PDR	Preliminär konstruktionsgranskning Preliminary Design Review
PHA	Riskkälleanalys Preliminary Hazard Analysis
PHL	Riskkällelista Preliminary Hazard List

Akronym/förkortning	Förklaring
PPE	Personal Protective Equipment Personlig skyddsutrustning
PTK	Provturskommando
PTS	Post- och telestyrelsen
PTSFS	Post- och telestyrelsens författningssamling
RADS	Riskanalys inför avveckling av system Risk Assessment Prior to Disposal of Systems
RADSR	Riskanalysrapport inför avveckling av system
REACH	Registration, Evaluation, Authorisation and restriction of Chemicals
RED	Radio Equipment Directive
RFP	Request for Proposal (förfrågningsunderlag)
R LML	Reglemente Ledning av Militär Luftfart
RML	Regler för militär luftfart
RMS	Regler för militär sjöfart
SAAMI	Sporting Arms and Ammunition Manufacturers' Institute
SAE	Society of Automotive Engineers (USA)
SAE ARP	Society of Automotive Engineers Aerospace Recommended Practice
SAMÖ	Samordningsöverenskommelse
SAR	Systemsäkerhetsrapport Safety Assessment Report
SCA	Systemsäkerhetsutlåtande Safety Compliance Assessment
SCF	Säkerhetskritiska funktioner Safety Critical Functions
SDB	Säkerhetsdatablad
SDS	Safety Data Sheet, (se SDB)
SE	Landsförkortning för Sverige
SE-EMAR	European Military Airworthiness Requirements endorsed in Sweden
SEK	Svensk elstandard. Tidigare Svenska Elektriska Kommissionen
SEMP	Systems Engineering Management Plan
SEP	System Engineering Plan
SFS	Svensk författningssamling
SGRA	Support of Government Reviews/Audits

Akronym/förkortning	Förklaring
SHA	Riskanalys för system System Hazard Analysis
SHAR	Riskanalysrapport för system
SHK	Statens haverikommission
SI	Säkerhetsföreskrifter Safety Instructions
SIA	Säkerhetsföreskriftsanalys Safety Instructions Analysis
SIL	Safety Integrity Level
SIS	Svenska institutet för standarder
SMS	Systemmålsättning
SoS	System-av-system System-of-Systems
SoSHA	Riskanalys för system-av-system System-of-Systems Hazard Anlysis
SoSHAR	Riskanalysrapport för system-av-system
SR	Ändringsgranskning Safety Review
SRHA	Systemsäkerhetskravanalys System Requirements Hazard Analysis
SRHAR	Systemsäkerhetskravanalysrapport
SS	Svensk standard
SSB	Systemsäkerhetsbedömning
SSD	Systemsäkerhetsdeklaration System Safety Declaration
SSG	Systemsäkerhetsgodkännande System Safety Approval
SSHA	Riskanalys för delsystem Subsystem Hazard Analysis
SSHAR	Riskanalysrapport för delsystem
SSI	Systemsäkerhetsintyg System Safety Certificate
SSKB	Systemsäkerhetskonceptbedömning System Safety Concept Evaluation
SSM	Systemsäkerhetsmeddelande System Safety Announcement
SSMP	Systemsäkerhetsledningsplan System Safety Management Plan

Akronym/förkortning	Förklaring
SSP	Systemsäkerhetsprogram System Safety Program
SSPP	Systemsäkerhetsplan System Safety Program Plan
SSK	Systemsäkerhetskrav System Safety Requirement
SSV	Systemsäkerhetsvärdering
SSWG	Arbetsgrupp för systemsäkerhet System Safety Working Group
STANAG	Standardization Agreement (NATO)
SV	Systemsäkerhetsverifiering Safety Verification
SVR	Systemsäkerhetsverifieringsrapport
Swedac	Styrelsen för ackreditering och teknisk kontroll. Tidigare betydelse: Swedish Board for Accreditation and Conformity Assessment
SÄKINSP	Försvarsmaktens Säkerhetsinspektion
SäkR	Försvarsmaktens Reglemente Verksamhetssäkerhet
SÖL	Systemöverlämning
T	Tolerabel
TC	Teknisk chef
TDir	Teknisk direktör
TEP	Riskanalys inför provning Test and Evaluation Participation
THR	Tekniska handlingsregler
ToR	Terms Of References
TR	Tolerabel risknivå
TS	Transportstyrelsen
TSFS	Transportstyrelsens författningssamling
TSR	Handhavande och utbildning Training Safety Regulations
TVK	Teknik- och vidmakthållandekontor
UK	United Kingdom
UK MOD	UK Ministry of Defence Försvarsdepartementet i Storbritannien
UKCA	UK Conformity Assessed; överensstämmelse bedömd
VoV	Verifiering och Validering

Akronym/förkortning	Förklaring
VTR	Vägtrafikregistret
VVM	Vägvalsmodellen
WBS	Work Breakdown Structure
WG	Working Group
ÖB	Överbefälhavare

Bilaga 1

EU-rätt och svensk lagstiftning

Syftet med denna bilaga är att beskriva den EU-rätt, svensk lagstiftning och andra civila regelverk som har påverkat innehållet i denna handbok.

Civila regelverk

CE-märkning

För specificerade produktkategorier enligt EU:s regelverk är CE-märkning obligatorisk. Andra produktkategorier, vilka inte omfattas av EU:s direktiv med CE-märkning, ska inte och får därmed inte CE-märkas. Produkter särskilt framtagna för visst militärt eller polisiärt ändamål kan vara undantagna från CE-märkning enligt aktuellt EU-direktiv. De ska inte CE-märkas enligt just detta EU-direktiv. Däremot kan det finnas andra EU-direktiv som kräver CE-märkning. Om produkten är särskilt framtagen för militärt ändamål och då råkar ha ett undantag från CE-märkning och samtidigt erbjuds marknaden med ett civilt ändamål (dubbla användningsområden, s.k. *dual use product*), då ska produkten CE-märkas.

CE-märkning ska appliceras varaktigt på produkten och i medföljande dokument m.m.

CE

Bilaga 1, bild 1 *CE-märkning, där CE står för europeisk efterlevnad (Conformité Européenne).*

Tillämpning av CE-märkning

Genom CE-märkningen intygar den legala tillverkaren att produkten överensstämmer med de lagstadgade kraven på säkerhet, hälsa och miljö, det vill säga att samtliga tillämpbara EU-direktiv är uppfyllda. EU-direktiven är olika till produktomfattning *(scope)*, vissa verkar enskilt, andra parallellt medans vissa olycksrisker ingår i andra EU-direktiv som gör att EU-direktiv B tar över från EU-direktiv A för aktuell produkt. Exempelvis täcks elektriska olycksrisker

numera av maskindirektivet vilket gör att lågspänningsdirektivet (LVD) inte längre ska tillämpas för en komplett elektrisk maskin utan enbart maskindirektivet. Parallellt verkar dock EMC-direktivet på den elektriska maskinen i fråga.

Med legal tillverkare avses den som har fullt produktsäkerhetsansvar, men är inte nödvändigtvis den som fysiskt tillverkar produkterna.

Ibland intygas även andra produktegenskaper såsom prestanda. Den legala tillverkaren ansvarar också för att produkten som är avsedd att släppas ut inom EU/EES har konstruerats, tillverkats och kontrollerats enligt regelverket. För de flesta produkter räcker det att tillverkaren själv säkerställer att produkten uppfyller alla krav, men för vissa produkter som anses särskilt riskfyllda krävs att tillverkaren låter ett oberoende tredjepartsorgan, så kallat Anmält organ (*Notified Body*), kontrollera produkten. Beroende på EU-direktiv så kan detta avse produktens konstruktion, produktens tillverkning, tillverkarens kvalitetssystem eller en kombination av dessa. När Anmält organ har använts ska CE-märkningen åtföljas av organets fyrsiffriga ID-nr.

Som en del av CE-märkningen ska tillverkaren också upprätta teknisk dokumentation *(Technical File, Technical Construction File)* för produkten samt utfärda en Försäkran om överensstämmelse (*Declaration of Conformity, DoC*). Den tekniska dokumentation som avses är den dokumentation varigenom tillverkaren visar att EU-direktivets krav är uppfyllda. Denna dokumentation är en delmängd av det totala konstruktions- och tillverkningsunderlaget för en produkt. Den CE-märkta produkten ska också åtföljas av en bruksanvisning som innehåller all väsentlig information för att produkten ska kunna användas och hanteras för avsett ändamål på ett säkert sätt. Vid leverans till slutkund ska produkten åtföljas av en bruksanvisning samt Försäkran om överensstämmelse (DoC), på mottagarlandets språk. Språkkravet gäller även märkning och skyltar som produkten ska ha.

Den person som har ansvar för utsläppandet på den gemensamma inre marknaden eller idrifttagande av en utrustning för första gången, måste uppfylla alla skyldigheter oavsett om denna person är en ekonomisk aktör (legal tillverkare, importör, auktoriserad representant, distributör) eller användare. Även distributörer, exempelvis grossister och återförsäljare, ska ha grundläggande

kunskaper om tillämplig lagstiftning, såsom vilka produkter som ska vara CE-märkta och vilken information som måste åtfölja dem.

Tillverkare ska hålla sig informerade om uppdatering av tillämpade standarder för att bedöma om aktuell produkttyp fortfarande anses uppfylla direktivets krav eller om åtgärder behövs för nya exemplar som ska tillverkas. På motsvarande sätt bör tillverkare övervaka ifall direktivet, eller dess ingående krav, revideras och om åtgärder i så fall behöver vidtas för nytillverkade exemplar av produkten.

Undantag från CE-märkning

Produkter framtagna för visst militärt eller polisiärt ändamål kan vara undantagna från CE-märkning. Exempelvis gäller inte EU:s maskindirektiv för vapen, inklusive skjutvapen, eller för maskiner som är särskilt konstruerade och tillverkade för militära eller polisiära ändamål. Däremot omfattas vanliga maskiner använda av militär eller polis av maskindirektivet. Notera att även om ett direktiv råkar ha ett undantag för aktuell produkt så kan ett eller flera andra direktiv vara obligatoriska. Exempelvis ska ett utbildningssystem som inte är avsett att användas i organiserad väpnad strid CE-märkas precis som en lyftkran/ett lyftdon som sätts på en stridsvagn, även om stridsvagnens användning i sig har en förstörelsebringande effekt. Se även avsnittet om Rattmärkning.

UKCA-märkning

Storbritannien införde år 2021 en produktsäkerhetsmärkning *UK Conformity Assessed* (UKCA) i samband med att Storbritannien lämnade EU. Därmed lämnade Storbritannien även EU-rätten inklusive CE-märkning.

Storbritanniens UKCA-märkning motsvarar CE-märkning genom att tillverkaren deklarerar att de grundläggande hälso- och säkerhetskraven är uppfyllda. Notera att särskilda regler gäller för Nordirland.

UK
CA

Bilaga 1, bild 2 *UKCA-märke, där UKCA står för United Kingdom Conformity Assessed.*

En produkt som omfattas av produktsäkerhetsdirektiven inom EU får inte släppas ut på EU:s inre marknad (EES) utan CE-märkning. På motsvarande sätt får inte heller en CE-märkt produkt släppas ut på den brittiska marknaden utan UKCA-märkning. Notera att produktsäkerhetsdirektiven inom EU ställer krav på att bruksanvisning och märkning är på korrekt språk för det land där produkten ska användas.

Det finns brittisk lagstiftning som bland annat motsvarar direktivet för elektromagnetisk kompatibilitet (EMCD) och lågspänningsdirektivet (LVD). Maskiner, hissar, mätinstrument och radioutrustning är exempel på produkter som är föremål för UKCA-märkning. För vissa produktgrupper kan det finnas särskilda regler som avviker från EU-direktiven.

Så länge som de tekniska kraven är desamma inom EU och Storbritannien innebär reglerna oftast enbart en administrativ uppgift. På en produkt som är avsedd för båda marknaderna kommer det att finnas både CE- och UKCA-märkning.

Observera att i de fallen ett Anmält organ inom EU har använts så ska motsvarande brittiska godkända organ dessutom användas för att få släppa ut produkten på den brittiska marknaden.

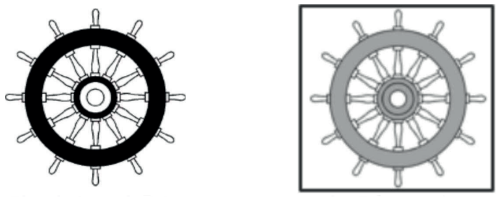
Rattmärkning

EU-rätten syftar till att förbättra sjösäkerheten, hälsan och förebygga föroreningar till sjöss genom krav på hur marin utrustning ska vara tillverkad och kontrollerad. Rattmärkning används för att visa att utrustning som omfattas av EU-direktivet 2014/90/EU om marin utrustning (MED) uppfyller gällande krav. För specificerade produktkategorier enligt EU-rätten är rattmärkning obligatorisk, men endast produkter för vilka det föreskrivs om sådan märkning får rattmärkas. Produkter särskilt framtagna för militärt ändamål kan vara undantagna från rattmärkning. Försvarsmaktens tillämpning av bestämmelserna om marin utrustning regleras i Regler för militär sjöfart (RMS).

Tillämpning av Rattmärkning

EU-direktiv 2014/90/EU om marin utrustning är satt i kraft genom lagen (SFS 2016:768) om marin utrustning och förordningen (SFS 2016:770) om marin utrustning tillsammans med Transportstyrelsens föreskrifter TSFS 2016:81 om marin utrustning. En produkt som är typgodkänd/motsvarande av ett Anmält organ i en medlemsstat inom EU, får placeras på ett EU-fartyg, oavsett vilken flagg det för, vilket främjar fri rörlighet för marin utrustning på den inre marknaden.

Utrustning som regleras av EU-direktivet för marin utrustning (huvudsakligen för fartygets sjösäkerhet samt för vatten- och luftrening) ska rattmärkas och inte CE-märkas. Rattmärket visar att produkten uppfyller kraven enligt EU-direktivet genom att tillverkaren genomför en certifiering (typgodkännande eller jämförbar angiven procedur) utförd av Anmält organ. I EU-direktivet fastställs gemensamma regler i syfte att undanröja skillnader vid genomförandet av internationella konventioner genom att ha en tydligt identifierad uppsättning krav och enhetliga certifieringsförfaranden. Enligt regler från Sjösäkerhetsinspektionen (SJÖI)/ Marinens fartygsinspektion (MFI) ska EU-direktivet tillämpas för angiven marin utrustning. Detta EU-direktiv med rattmärkning ersätter därmed andra EU-direktiv med CE-märkning för sådan utrustning som anges ovan. Notera att det finns andra produkter ombord på fartyg som omfattas av EU-direktiv med CE-märkning. Användning av CE-märkta produkter ombord på örlogsfartyg regleras i Regler för militär sjöfart (RMS).



1234 = det Anmälda organets ID-nr
YYYY eller YY = årtal då märkningen applicerades

Bilaga 1, bild 3 *Exempel på rattmärkning.*

EU-direktivet ska tillämpas på utrustning som är placerad eller avsedd att placeras på ett EU-fartyg, om det enligt vissa internationella konventioner på sjöfartsområdet krävs att den stat, vars flagga fartyget för, godkänner utrustningen. Lagstiftningen innehåller bestämmelser om krav på marin utrustning och skyldigheter för tillverkare och andra ekonomiska aktörer som tillhandahåller sådan utrustning på marknaden. Vidare finns bestämmelser om marknadskontroll för att se till att marin utrustning uppfyller föreskrivna krav och om sanktionsavgifter för det fall kraven inte följs.

Undantag från Rattmärkning

På mindre fartyg (deplacement under 40 ton) använder Försvarsmakten olika typer av kommersiella produkter. För de minsta båtarna används ofta så kallade fritidsbåtsprodukter. Produkterna kan vara enklare typer av radaranläggningar och sjökortsplottrar. Produkter som är certifierade enligt EU-direktivet och därmed rattmärkta är framtagna för större fartyg. Tekniska begränsningar hos mindre fartyg och båtar kan medföra att rattmärkta produkter inte är lämpliga att integreras. Rattmärkta produkter är ofta både tyngre och fysiskt större. Exempelvis kan mindre båtar behöva ha inbyggd antenn för att undvika att verksamheten hindras. Mindre båtar har oftast öppna styrplatser och produkterna måste därför vara vattentäta, vilket inte är fallet med flertalet av de rattmärkta produkterna. Sjösäkerhetsinspektören kan därför, efter bedömning, behöva medge undantag från rattmärkning för enskilda produkter.

CIP-märkning

Skyldigheten att märka vapen anges i EU-direktiv 2021/555/EU om kontroll av förvärv och innehav av vapen. Utöver detta har ett antal stater enats om ett gemensamt märknings- och kontrollsystem. Svenska tillverkare och importörer av vapen rekommenderas att tillämpa CIP-systemet, vilket uppfyller kraven enligt EU-direktivet.

CIP *(Commission Internationale Permanente pour l'Epreuve des Armes à Feu PortativesPermanent International Commission for Firearms Testing)* är en statlig internationell organisation som består av ett antal länder som är överens om ömsesidigt erkännande av provningskontrollmärkningen *(proof-test)* av skjutvapen samt ammunition som har passerat säkerhetsprovningen. CIP:s avsikt är att garantera säkerheten för civila skjutvapen, kommersiell ammunition och all annan utrustning som nyttjar explosiva ämnen för defensiva syften som sport och jakt.

Det finns även en motsvarande amerikansk sammanslutning för ammunitions- och vapentillverkare som går under namnet SAAMI *(Sporting Arms and Ammunition Manufacturers' Institute)*, som är ett standardiseringsorgan för vapen och ammunition.

Tillämpning av CIP-märkning

CIP-konventionen har följande huvudföreskrifter:

- Att det finns ömsesidigt erkännande av varje lands provningskontrollmärkning som intygar identiteten av skjutvapen och att tillfredsställande provning genomförts i enlighet med de fastställda reglerna
- Att provning standardiseras för att garantera säkerheten
- Att minst en statligt kontrollerande (ackrediterad) nationell provnings-anläggning finns i varje medlemsland (Sverige är inte medlem i CIP och saknar därför ackrediterad provningsanläggning)
- Att varje medlemsland stiftar lagar som gör det obligatoriskt att utföra provning i enlighet med de metoder, begränsningar och förfaranden som fastställts av konventionen

Undantag från CIP-märkning

Då militär tillämpning avsevärt skiljer sig från civil tillämpning är CIP-märkning i regel inte tillfyllest för militära finkalibervapen och ammunition. NATO använder andra procedurer för att styra säkerhet och kvalitet för militära finkalibriga vapen och dess ammunition, NATO EPVAT, exempelvis för 7,62 mm används STANAG 2310. I övrigt tillämpas FMV Handbok Vapen- och ammunitionssäkerhet (H VAS).

Åtgärder på eftermarknaden samt marknadskontroll

Tillverkare och övriga ekonomiska aktörer har även ett visst ansvar (skiljer sig åt mellan olika EU-direktiv) för eftermarknaden, det vill säga när produkten väl befinner sig på marknaden. De ska exempelvis ta hand om klagomål, säkerhetsbrister, hantera eventuella olyckor och tillbud med produkterna samt kunna spåra produkterna uppströms och nedströms till övriga ekonomiska aktörer. Detta för att kunna informera om, åtgärda eller återkalla farliga eller bristfälliga produkter.

Vissa EU-direktiv ställer även krav på att misstänkt farliga produkter, liksom olyckor och tillbud ska rapporteras av tillverkare och övriga ekonomiska aktörer till ansvarig myndighet. En tillverkare eller importör kan även behöva genomföra stickprovskontroll av levererade produkter för att förvissa sig om att produkterna uppfyller ett EU-direktivs krav.

Vidare ska medlemsstaterna genomföra marknadskontroll i enlighet med bestämmelser i EU-förordning 765/2008 om ackreditering och marknadskontroll. Marknadskontroll innebär att ansvarig myndighet vidtar åtgärder för att säkerställa att produkter som redan finns på marknaden uppfyller gällande lagstiftning och att de är kontrollerade och märkta på föreskrivet sätt. Den omfattar således inte förhandskontroll av produkter. Den är en led i kedjan att säkerställa ett tillfredställande skydd för konsumenter och arbetstagare, folkhälsa samt miljö. Den ska även motverka snedvridning av konkurrens mellan företag. Regeringen har pekat ut 17 statliga myndigheter som ansvariga för marknadskontrollen. Flertalet av dessa myndigheter är även föreskrivande myndighet för de produkter eller produktegenskaper de har marknadskontrollansvar för.

FMV är tillsynsmyndighet för EMC (enligt förordning SFS 2016:363 om elektromagnetisk kompatibilitet) avseende produkter inom Försvarsmakten, Fortifikationsverket, Försvarets radioanstalt och Försvarets forskningsinstitut. Elsäkerhetsverket är marknadskontrollmyndighet samt utövar tillsyn avseende övriga produkters EMC.

När det gäller rattmärkta produkter ska Transportstyrelsen ta hänsyn till särdragen i sektorn för marin utrustning, exempelvis om en utrustning kan antas utgöra en risk för sjösäkerheten.

För explosiva varor, inklusive ammunition, men exklusive vapen, är Myndigheten för samhällsskydd och beredskap (MSB), ansvarig för marknadskontroll.

Myndigheten ska ingripa mot de ekonomiska aktörer vars produkter inte uppfyller ställda krav. Ingripandena som kan bli aktuella är till exempel informationsplikt, produktåtgärder, försäljningsförbud eller återkallande av produkter från marknaden eller slutanvändare. Detta kan ske i form av information, planerade kontroller (tillsyn, inspektion) hos tillverkare, importörer och återförsäljare för produkter som finns släppta på marknaden. Den kan även ske med anledning av rapporterade olyckor, tillbud eller efter varningar via

EU-kommissionens databaser eller myndigheter i andra länder.

Tillverkaren, importören eller distributören, ska bistå marknadskontrollmyndigheten i dess tillsyn, exempelvis genom att ge tillgång till erforderliga, nödvändiga delar av den tekniska dokumentationen *(Technical file)*.

Marknadskontrollrådet är ett nationellt samordningsorgan för denna marknadskontroll. Styrelsen för ackreditering och teknisk kontroll, Swedac, svarar för samordning av de svenska marknadskontrollmyndigheterna. Arbetet består främst av lagstiftning, tolkning och metodutveckling samt informationsutbyte. Rådet ska också underlätta allmänhetens kontakter med myndigheterna och samråda med företrädare för bland annat näringsliv och konsumenter.

Försvarsmakten behöver ha spårbarhet över CE-märkta och rattmärkta produkter om tillverkaren eller marknadskontrollmyndigheter vidtar åtgärder såsom modifieringar, varningar, användningsförbud eller om produkterna ska återkallas.

Miljölagstiftning

Miljöbalken (SFS 1998:808) syftar till att främja en hållbar utveckling som innebär att nuvarande och kommande generationer tillförsäkras en hälsosam och god yttre miljö. Miljöbalken 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.

Kemiska produkter och kemiska ämnen i varor regleras framförallt i två EU-förordningar, REACH (Registrering, utvärdering, godkännande och begränsning av kemikalier), EU 1907/2006, och CLP (Klassificering, märkning och förpackning av ämnen och blandningar), EU 1272/2008. I REACH finns regler kring information om farliga ämnen i distributionskedjan, exempelvis om säkerhetsdatablad. Den som tillverkar, importerar eller distribuerar varor eller kemiska produkter inom EES/EU måste kontrollera om varorna eller de kemiska produkterna innehåller något ämne på kandidatförteckningen eftersom det kan innebära särskilda krav på hanteringen i enlighet med EU-förordningen REACH. I CLP styrs hur farliga ämnen ska klassificeras, förpackas och märkas.

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 miljö. 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.

Enligt Arbetsmiljöverkets föreskrifter AFS 2011:19, om kemiska arbetsmiljörisker, ska riskbedömningar göras inför arbete som inkluderar hantering av kemiska produkter.

Ett stort antal centrala, regionala och lokala myndigheter har särskilt utpekade uppgifter då det gäller miljöbalken, inklusive ansvar för vägledning och tillsyn. Inom Försvarsdepartementets ansvarsområde utövar Försvarsinspektören för hälsa och miljö (FIHM) tillsyn över miljöbalkens tillämpning vid Försvarsmakten, FMV, Fortifikationsverket och Försvarets radioanstalt. Försvarsinspektören för hälsa och miljö (FIHM) är den funktion som granskar miljöfarlig verksamhet, hälso- och sjukvård, tandvård, smittskydd, livsmedelssäkerhet och djurskydd.

Elsäkerhetslagstiftning inklusive lågspännings-direktivet

Den första ellagen infördes 1902 och reviderades grundligt till ny ellag (SFS 1997:857). Med tanke på elektricitetens risker (osynlig, dödlig/skadlig effekt, brand) och ökade användning beslutade Riksdagen dessutom om Sveriges första elsäkerhetslag (SFS 2016:732).

Elsäkerhetslagen reglerar bland annat följande skyldigheter:

- För innehavare av elektriska anläggningar
- För den som tillverkar, importerar, distribuerar eller installerar en elektrisk utrustning
- Angående utförande av elinstallationsarbete
- För den som innehar eller använder en elektrisk utrustning

Två centrala definitioner finns i elsäkerhetslagen:

- Elektriska anläggningar (elanläggningar) består av enskilda elektriska utrustningar som byggs ihop för att föra fram el till uttag/anslutningsdosor där elektriska utrustningar (elektrisk materiel/elmateriel) ansluts för förbrukning av el. En elanläggning förbrukar ingen el, den möjliggör förbrukning. En elektrisk anläggning kan inte köpas som en färdig enhet av en tillverkare utan den måste byggas på den plats där den ska användas.
- Elektriska utrustningar tillverkas av en tillverkare och släpps ut på marknaden (levereras) som en färdig produkt. Tillverkaren har ett tydligt ansvar för att utrustningen uppfyller gällande säkerhetskrav i EU-direktiven.

Begreppet elanläggning har tidigare ofta använts som ett paraply-begrepp även för elektriska utrustningar. Detta har fått till följd att kravdokument vid upphandling har upplevts otydliga liksom kraven på kompetens för den personal som ska utföra skötseln.

Elsäkerhetslagstiftningen i Sverige är målrelaterad och anger hur elanläggningar och elektriska utrustningar ska vara konstruerade för att vara säkra att bruka. Krav på utrustningars säkerhet respektive hur den uppfylls, hanteras via EU-direktiv och de harmoniserade standarder som EU fastställt för att uppfylla EU-direktivens grundläggande hälso- och säkerhetskrav.

Standarder har alltid varit viktiga för elprodukter som ett sätt att uppfylla lagstiftningens krav. Standarder arbetas huvudsakligen fram inom IEC för att sedan överföras till EN-standard och harmoniserad standard.

Försvarsmaktens interna bestämmelser (FIB) fastställer hur man ska hantera elsäkerhetslagens krav.

FMV har på uppdrag av Försvarsmakten gjort ett omfattande utredningsarbete hur kraven på säkerhet för Försvarsmaktens personal uppfylls då tekniska system används i fältmiljö och det saknas tillgång till fast eldistributionsnät och det som föreskrifterna definierar som systemjordtag (s.k. godkänt jordtag). Det resulterade i *Designregel – Försvarsmaktens elektriska anläggningar i fältmiljö* (FMEAF).

FMEAF är ett fastställt begrepp inom Försvarsmakten. Det är en sammanfattande benämning för anläggningar som upprättas med utrustningar för produktion

och distribution av el i fältmiljö, det vill säga transportabla generatoraggregat, elcentraler och anslutningskablar.

Genom att tillämpa etablerad standard tillsammans med dokumenterad riskbedömning i designregeln, uppfylls lagstiftningens krav på person- och anläggningssäkerhet. Designregeln påverkar även konstruktionen av elektriska utrustningar (förbrukare) som ansluts till FMEAF eftersom de ingår som en del i jordningssystemet.

För mer information, se FMV Handbok Säkra elektriska produkter och system (H SEPS) och Försvarsmaktens handbok för elsäkerhet (H ELSÄK).

Elektrisk materiel (elektrisk utrustning) ska CE-märkas enligt EU:s LVD (s.k. lågspänningsdirektivet) 2014/35/EU, om den är konstruerad för att drivas med, eller avge, en spänning om 50-1000V AC eller 75-1500V DC. EU-direktivet är överfört genom Elsäkerhetsverkets föreskrifter ELSÄK-FS 2016:1. Grundkravet är att elektrisk utrustning ska ha en hög skyddsnivå avseende människors och husdjurs hälsa och säkerhet samt ge skydd för egendom. Tillverkaren kan själv verifiera att grundkraven är uppfyllda för produkterna. Det finns inget krav på certifiering, det vill säga godkännande av tredje part (Anmält organ). Ackrediterat organ kan dock anlitas frivilligt.

I dagsläget finns inga undantag för militär materiel. Villkorade undantag finns för utrustning på fartyg, flygplan och tåg.

Fordonslagstiftning

Ett fordon får brukas i trafik endast om det är tillförlitligt ur trafiksäkerhetssynpunkt och i övrigt lämpligt för trafik. 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. Trafikvärdighet uppnås genom att fordon godkänns vid en registreringsbesiktning samt vid periodiskt återkommande kontroller. Registreringsbesiktning och provning inför ett enskilt godkännande kan utföras av ett ackrediterat kontrollorgan eller av militär besiktningsingenjör. Försvarsmakten får meddela särskilda föreskrifter om detta.

Vid anskaffning hänvisas till aktuella EU-förordningar, till exempel ”*Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon*”. Vilka undantag som kan ges med hänsyn till svenska regelverk får bestämmas av militär besiktningsingenjör i varje enskilt fall.

EU-förordningen ovan pekar på ECE-reglementen (*ECE Regulations*). Dessa är bilagor till 1958 års globala FN-överenskommelse om att anta enhetliga tekniska föreskrifter för hjulförsedda fordon eller för utrustning och komponenter som kan monteras eller användas på sådana fordon. Varje ny bestämmelse träder i kraft för alla de parter som har uppgett för FN:s generalsekretariat att de godkänner reglementet. ECE-reglementen tillämpas av cirka 60 länder. EU och Sverige har dock inte antagit alla reglementen.

Med stöd av Fordonslagen (SFS 2002:574) ges Fordonsförordningen (SFS 2009:211) och Militärtrafikförordningen (SFS 2009:212) ut. För militära fordon tillämpas dessa förordningar parallellt. Militärtrafikförordningen (MTRF) innehåller särskilda bestämmelser om beskaffenhet och utrustning för fordon som tillhör staten och som brukas av Försvarsmakten, FMV och Försvarets radioanstalt (FRA). Militärtrafikförordningen (MTRF) ger även Försvarsmakten möjlighet till vissa undantag från trafiklagstiftningen.

Försvarsmakten får meddela föreskrifter om fordon som tillhör staten och är tillverkade för särskilda militära ändamål. Detta framgår av Försvarsmaktens föreskrifter om militär trafik (FFS 2021:2).

I Transportstyrelsens författningssamlingar ges fordon som är registrerade i militära fordonsregistret (MIFOR) och som brukas av Försvarsmakten, FMV och Försvarets radioanstalt (FRA) undantag avseende viss utrustning för fordon. Ytterligare undantag för enskilt fordon kan sökas hos Transportstyrelsen av militär besiktningsingenjör.

Övriga författningssamlingar som kan påverka fordons utrustning och beskaffenhet är:

– Myndigheten för samhällsskydd och beredskap (MSB) författningssamling, MSBFS

– Arbetsmiljöverkets författningssamling, AFS
– Transportstyrelsens författningssamling (TSFS), t.ex. TSFS 2019:19

Vissa maskiner som faller under AFS 2008:3 om Maskiner kan även klassificeras som fordon och därför vara registreringspliktiga enligt Militärtrafikförordningen (MTRF). Dessa kan även omfattas av ytterligare föreskrifter från Transportstyrelsen. Detta gäller exempelvis för truckar, motorredskap och snöskotrar.

FMV Handbok Fordonssäkerhet (H FordonSäk) är ett komplement till fordonslagstiftningen och beskriver undantag och tillägg samt ger förslag på krav för säkra konstruktioner. Vidare finns förslag på krav för exempelvis installationer av vapen- och ledningssystem i fordon.

Sjöfartlagstiftning

För fartyg och dyksystem finns ett omfattande regelverk. Fartygssäkerhetslagen (SFS 2003:364) ställer krav på alla typer av fartyg, men gäller endast örlogsfartyg i den mån Regeringen föreskriver det. Ytterligare lagstiftning finns som reglerar arbetsmiljön ombord på fartyg. Nedan redovisas ett urval av de författningar som är styrande för denna reglering.

Förordning (SFS 2003:440) om säkerheten på örlogsfartyg reglerar vilka delar av Fartygssäkerhetslagen (SFS 2003:364) som gäller för örlogsfartyg, och ger Transportstyrelsen (TS), tidigare Sjöfartsverket, bemyndigande att både föreskriva ytterligare regler samt utöva tillsyn över den militära sjöfarten. Vidare ska Försvarsmakten ha ett system för kontroll av sjövärdighet och säkerhet på örlogsfartyg som är godkänt av Transportstyrelsen.

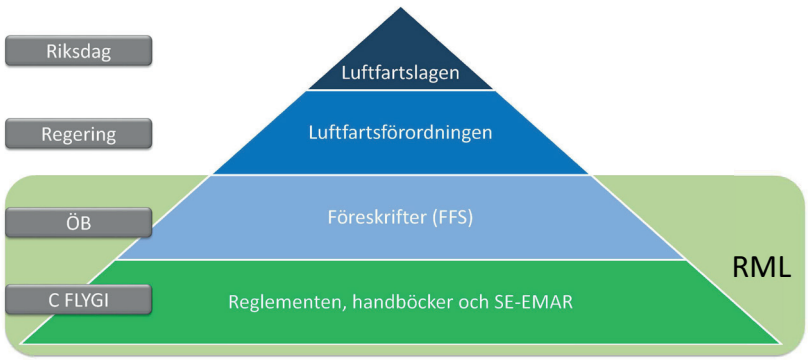
I förordning (SFS 2003:440) om säkerheten på örlogsfartyg regleras att Transportstyrelsen får utarbeta regler för sjövärdigheten hos örlogsfartyg. I samma förordning regleras också att Transportstyrelsen får föreskriva om arbetsmiljön på örlogsfartyg. De arbetsmiljöregler som finns i Transportstyrelsens föreskrifter TSFS 2011:91 och allmänna råd om arbetsmiljö på örlogsfartyg, består till del av fartygsspecifika regler och till del av ett antal av Arbetsmiljöverkets föreskrifter (AFS) sätts i kraft på örlogsfartyg. Denna reglering innebär att en AFS endast är tillämplig på örlogsfartyg om den finns medtagen i TSFS 2011:91.

Luftfartslagstiftning

All verksamhet som anses som luftfartsverksamhet är tillståndspliktig enligt luftfartslagen (SFS 2010:500). 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. EASA (*European Aviation Safety Agency*) styr över den civila luftfarten inom unionens område. Detta inflytande utövas bland annat genom EU-direktiv som direkt eller indirekt gäller för den civila luftfarten.

För det militära luftfartssystemet har regeringen genom luftfartsförordningen (SFS 2010:770) bemyndigat Försvarsmakten att utfärda föreskrifter och utöva tillsyn.



Bilaga 1, bild 4 *Hierarki mellan lagar, förordningar, föreskrifter inklusive Försvarsmaktens regelverk.*

Överbefälhavaren (ÖB) ansvarar för militär flygsäkerhet inom det militära luftfartssystemet. Bestämmelser för den militära luftfarten framgår av Försvarsmaktens föreskrifter om militär luftfart FFS 2019:10.

Av luftfartslagen (SFS 2010:500) framgår att det militära luftfartssystemet består av system för flygdrift, flygplatser och flygbaser samt för luftrum. I Försvarsmaktens

reglementen och handböcker för militär luftfart finns närmare bestämmelser om tillämpningen av Försvarsmaktens föreskrifter om militär luftfart. Chefen för Militära flyginspektionen (FLYGI) får fatta beslut om reglementen, handböcker och SE-EMAR *(European Military Airworthiness Requirements)* för den militära luftfarten.

En statlig myndighet som bedriver militär luftfart inom ett eller flera verksamhetsområden ska ha ett godkännande utfärdat av Flygsäkerhetsinspektören (FSI). En statlig myndighet som bedriver militär luftfart ska anmäla till Militära flyginspektionen (FLYGI) inom vilket eller vilka verksamhetsområden myndigheten avser bedriva verksamhet och på vilket sätt sökanden uppfyller tillämpliga krav enligt Försvarsmaktens föreskrifter om militär luftfart. Verksamhetsutövare annan än staten ska ha tillstånd för att bedriva verksamhet i det militära luftfartssystemet. En ansökan om tillstånd att bedriva verksamhet i det militära luftfartssystemet (verksamhetstillstånd) ska göras hos Militära flyginspektionen (FLYGI). Ett verksamhetstillstånd och ett beslut om godkänt verksamhetsområde meddelas i ett militärt luftfartsdokument som utfärdas av Flygsäkerhetsinspektören (FSI).

Ett militärt luftfartyg får endast flygas om det är luftvärdigt. Ett militärt luftfartyg anses luftvärdigt om det är konstruerat, tillverkat, utprovat, utrustat och underhållet eller ändrat på ett sådant sätt, samt har sådana flygegenskaper, att den militära flygsäkerhetens krav är uppfyllda. Det är verksamhetsutövaren som ska visa att ett militärt luftfartyg är luftvärdigt.

Av luftfartsförordningen (SFS 2010:770) framgår att Flygsäkerhetsinspektören (FSI) utövar tillsyn över att bestämmelserna i luftfartslagen (SFS 2010:500) och föreskrifter som meddelats med stöd av lagen (som Försvarsmaktens föreskrifter om militär luftfart FFS 2019:10) följs i fråga om militär luftfart. Militära flyginspektionen (FLYGI) i Försvarsmaktens högkvarter ska stödja Flygsäkerhetsinspektören (FSI) avseende denna tillståndsprövning och tillsynsverksamhet.

Lagstiftning om brandfarliga och explosiva varor

Lag (SFS 2010:1011) om brandfarliga och explosiva varor (LBE) gäller hantering och import av brandfarliga och explosiva varor. Lagens syfte är att förhindra att sådana varor orsakar brand eller explosion som inte är avsedd, samt att förebygga och begränsa skador på liv, påverkan på hälsa, yttre miljö eller egendom genom brand eller explosion vid hantering av sådana varor.

För utformnings- och granskningskrav avseende ammunition för militärt ändamål (militär ammunition) finns särskilda regler. Förordningen (SFS 2007:936) om folkrättslig granskning av vapenprojekt anger att granskning av projekt ur folkrättslig synvinkel ska ske av *Delegationen för folkrättslig granskning av vapenprojekt.* Förordningen ställer krav på att Försvarsmakten snarast möjligt ska anmäla till Delegationen varje projekt som avser studier, utveckling, nyanskaffning eller modifiering av vapen eller stridsmetoder.

FMV Handbok Vapen- och Ammunitionssäkerhet (H VAS) omfattar ammunition avsedd för militärt ändamål och redovisar krav på säkerhetsegenskaper hos de funktioner som förekommer i militär ammunition. Vidare finns även specifika krav för militär ammunition som följer av folkrättskrav.

Lagstiftning inom övriga säkerhetsområden

Tekniska system och produkter kan omfattas av särskild lagstiftning, föreskrifter och/eller standarder, exempelvis för, laser, strålkällor, farliga ämnen eller medicintekniska produkter (MTP). Detta gäller även för teknikoberoende riskkällor såsom joniserande och icke joniserande strålning, buller, vibrationer och hygieniska gränsvärden för farliga ämnen. För vissa produkter, exempelvis laser, kan Försvarsmakten ha vissa undantag.

För viss materiel såsom förbindelsemateriel (broar) kan det finnas särskilda föreskrifter, standarder och/eller designregler.

För produkter som omfattas av egna regler och som konstruerats och provats/verifierats i enlighet med dessa, anses det oftast vara tillräckligt. Den samlade dokumentationen avseende konstruktion och provning blir en del av underlaget som ingår i systemsäkerhetsvärderingen.

För vissa tekniska system och produkter krävs att en annan part såsom ackrediterade laboratorier, certifierings- och kontrollorgan samt organ för validering och verifiering intygar att lagar, föreskrifter och standarder är uppfyllda innan produkter får släppas ut på marknaden. Även detta blir en del av underlaget som ingår i systemsäkerhetsvärderingen.

Vid förflyttning av tekniska system och produkter på landsväg och järnväg samt för flyg- och sjötransporter kan begränsningar finnas avseende fysiska mått, vikter och viktfördelning samt för enskilda varor såsom farliga ämnen, batterier och explosiva varor.

Människans begränsningar för exponering av teknikoberoende riskkällor finns ofta kravställd i tekniska standarder eller i branschspecifika vägledningar. Där finns även vedertagna provningsmetoder för att verifiera standardernas krav.

Ett till säkerhetsområdet närliggande område som har stor betydelse och en indirekt påverkan, är produkters förmåga att fungera tillsammans utan att störa eller bli störda, det viss säga elektromagnetisk kompatibilitet.

Elektrisk materiel (elektriska produkter) ska CE-märkas enligt EMC-direktivet 2004/108/EU. EU-direktivet är överfört genom Elsäkerhetsverkets föreskrifter ELSÄK-FS 2016:1. Grundkrav är att elektrisk materiel ska uppfylla skyddskrav vad gäller emission och tålighet. I princip omfattas allt elektriskt från 0Hz till 1THz (egentligen ingen övre gräns) oavsett märkspänning. Skyddskrav framgår av harmoniserade standarder. Elmiljö, kravnivåer i regelverket/standarder är begränsad/ej så stränga, jämfört med vad som finns i militära EMC-standarder.

Tillverkaren kan själv verifiera att skyddskraven är uppfyllda för produkterna. Det finns inget krav på certifiering, det vill säga godkännande av tredje part (Anmält organ). Anmält organ kan dock anlitas frivilligt.

I dagsläget finns inga undantag för militär materiel. Undantag finns för vissa luftfartsprodukter och för komponenter som inte har en egen funktion *(intrinsic function)* och som därigenom inte stör eller blir störda, exempelvis kablar, transformatorer och induktionsmotorer. Om materielen faller under radioutrustningsdirektivet (RED, 2014/53/EU), marinutrustningsdirektivet (MED, 2014/90/EU) eller de medicintekniska EU-förordningarna, så ska dessa regelverk tillämpas istället för EMC-direktivet, då de förra inkluderar EMC-krav.

Produktsäkerhets- respektive produktansvars-lagstiftning

Denna beskrivning av de båda produktlagstiftningarna görs för att ge allmän information i denna handbok. Ett slutfört systemsäkerhetsarbete enligt metodiken i denna handbok kan utgöra ett viktigt underlag för enskild tillverkare/leverantör.

Produktsäkerhetslagstiftningen ställer krav på att alla varor och tjänster som företag erbjuder ska vara säkra. En vara eller tjänst är säker om den vid normal användning inte innebär någon olycksrisk, eller låg olycksrisk, för människors hälsa och säkerhet. EU-direktiven i tidigare avsnitt är exempel på specialiserad produktsäkerhetslagstiftning.

Produktansvarslagstiftningen inträder efter det att en olycka har inträffat. Lagstiftningen syftar till att utkräva ansvar och ge möjlighet till ekonomisk kompensation åt konsumenter och är därför inte förebyggande och påverkar ej heller konstruktionen av en vara innan denna släpps ut på marknaden. Lagstiftningen ställer bland annat krav på återkallelse och varningsinformation till konsumenter om en allvarlig säkerhetsbrist har identifierats.

Produktsäkerhetslagen

Produktsäkerhetslagen (SFS 2004:451) i sig, gäller inte varor som enbart är avsedda för yrkeslivet (t.ex. inom Försvarsmakten) utan avser varor och tjänster för konsumenter. Dessa ska vara säkra när de erbjuds konsumenter. Även sakskador och miljöskador faller utanför denna lag. Förenklat kan sägas att lagen är en generell lag och att den inte gäller om det finns speciallagstiftning, såsom lagstiftning som överför ett mer specialiserat EU-direktiv, för en viss produkt eller olycksrisk. Tillverkaren eller distributören ska lämna säkerhetsinformation som gör att du som konsument kan bedöma olycksriskerna med varan eller tjänsten. Om olycksriskerna är uppenbara behöver tillverkaren eller distributören inte lämna information.

Konsumentverket är tillsynsmyndighet för Produktsäkerhetslagen (SFS 2004:451) och delar ansvaret med andra myndigheter som har tillsyn över särskilda varor eller olycksrisker. Till exempel har Elsäkerhetsverket tillsyn över de flesta elektriska olycksrisker och Kemikalieinspektionen har tillsyn över de flesta kemikalierelaterade olycksrisker.

Produktansvarslagen

Produktansvarslagen (SFS 1992:18) reglerar förutsättningar för skadestånd för skada som en produkt har orsakat på grund av en säkerhetsbrist. Här avses skada på enskild person eller enskild egendom och är därmed en lag för konsumentskydd. Lagen gäller endast då näringsidkare säljer till konsumenter, det vill säga inte till yrkesanvändare inom exempelvis Försvarsmakten. Skador på själva produkten ersätts inte.

En produkt som används av en person i dennes anställning omfattas i första hand av Arbetsmiljölagen samt av arbetsgivarens ansvar för en god och säker arbetsmiljö.

En produkt har en säkerhetsbrist om produkten inte är så säker som skäligen kan förväntas. Fel på produkter som beror på konstruktionen, tillverkningen eller en otydlig bruksanvisning kallas säkerhetsbrister. Säkerheten ska bedömas med hänsyn till hur produkten kunnat förutses bli använd och hur den har marknadsförts samt med hänsyn till bruksanvisningar, tidpunkt då produkten släppts på marknaden/satts i omlopp och övriga omständigheter.

Bilaga 2

Standarder

Syftet med denna bilaga är att beskriva de standarder som har påverkat innehållet i denna handbok.

Amerikanska försvarsstandarder, MIL-STD

USA:s försvarsstandarder delas upp i dels militär standard (MIL-STD), dels i försvarsspecifikation (MIL-SPEC). Enligt *Government Accountability Office* (GAO) beskriver en MIL-STD de önskvärda processer och arbetssätt som en leverantör bör tillämpa för att utveckla rätt tekniska system och produkter medan en MIL-SPEC beskriver fysiska och/eller operativa egenskaper hos ett tekniskt system eller produkt. Utöver detta kan det även finnas militära handböcker som främst är källor för sammanställd information eller vägledning.

MIL-STD-882E, (Systemsäkerhet)

Standarden MIL-STD-882E, *DEPARTMENT OF DEFENSE STANDARD PRACTICE SYSTEM SAFETY* utgiven den 11 maj 2012, är avsedd att användas av alla militära myndigheter inom *US Department of Defense* (DoD). Standarden överensstämmer med intentionerna i *Department of Defense Instruction (DoDI) 5000.02.*

Standarden innehåller krav på systemsäkerhetsverksamhet samt en beskrivning av en systemsäkerhetsprocess. Standarden ställer krav på att processen ska dokumenteras samt att samordning med övrig riskhantering inom *System Engineering (SE)* ska ske.

Standarden ger instruktioner för genomförande av systemsäkerhetsverksamhet inom S*ystem Engineering* (SE) i syfte att eliminera eller minimera olycksrisker relaterade till tekniska system, produkter, utrustning och infrastruktur under systemets alla livscykelskeden från utveckling till och med avveckling. Principen i standarden är att ett urval av de olika aktiviteterna *(tasks*) måste ske för aktuellt tekniskt system. Standardens olika aktiviteter är uppdelade i styrning *(management)*, analyser, utvärdering och verifiering. Av standarden framgår även

en lista på tillämpliga dokumentvägledningar (DID) för de olika rapporterna som är resultaten av de olika aktiviteterna.

Vådahändelser och/eller olycksrisker ska systematisk identifieras och dokumenteras i en risklogg (*Hazard Log*) samt värderas avseende konsekvens och sannolikhet. Det finns föreslagna konsekvens- och sannolikhetsklassningar samt exempel på riskmatris för bedömning.

Standarden innehåller även ett separat avsnitt som behandlar programvara i säkerhetskritiska tillämpningar. Det finns både utnyttjandekategorier (*Software control categories*) och kritikalitetsmatris (*Software safety criticality matrix*) samt en bedömningstabell avseende risknivån för programvaran.

Appendix A, *Vägledning till omfattningen för systemsäkerhetsarbetet*, ger en vägledning till hur urval av aktiviteter ska ske, samt när de lämpligen utförs. Vidare ges ett exempel på kvantitativa sannolikhetsdefinitioner. Appendix B, *Säkerhetsverksamhet för programvara*, ger en vägledning till verksamheten kring säkerhetsrelaterad programvara. För mer detaljerad beskrivning hänvisas till:

- *Joint Software Systems Safety Engineering Handbook*
- *Allied Ordnance Publication (AOP-52), Guidance on Software Safety Design and Assessment of Munition-Related Computing Systems*

MIL-STD-1472H, (Humanfaktorer)

Standarden MIL-STD-1472H, *Department of Defense Design Criteria Standard, Human Engineering* utgiven den 15 september 2020, är avsedd att användas av alla militära myndigheter inom *US Department of Defense* (DoD).

Standarden anger kriterier för *Human Machine Integration* (HMI) och principer som ska tillämpas vid konstruktion av militära system, delsystem, utrustningar och anläggningar. HMI-verksamhet kan bedrivas baserat på en *Human Engineering Program Plan* (HEEP), exempelvis utformad enligt MIL-STD-46855A.

Standarden tar hänsyn till människans inneboende förmågor och begränsningar baserat på antropometriska data för 90% av populationen av den antagna personalen (militärt klädd och utrustad) vid hantering av rattar, styrspakar och knappar. Vidare bedöms även nödvändiga manöverutrymmen.

Konstruktioner ska anpassas till tillämpliga system- och personsäkerhetsaspekter, som även omfattar potentiella mänskliga felhanteranden under användning och underhåll, särskilt att beakta under stress och vid icke rutinanvändning. Det finns detaljerade krav för olika utrustningsdelar såsom spakar, rattar, reglage, displayer, dataskärmar, märkningar, manöverutrymmen samt data över potentiella användares fysiska mått och styrkor. Vidare finns detaljregleringar avseende mått, krafter, färger, belysning mm.

Standarden innehåller exempel på andra tillämpbara standarder och handböcker, både militära och civila. Vidare innehåller den vad man bör tänka på avseende underhåll samt anger antropometriska mått (kroppsmått) som referensdata.

Brittiska försvarsstandarder, DEF-STAN

Brittiska försvarsstandarder (DEF-STAN) tillhandahåller bland annat specifikationer som stöd för leverans av militär kapacitet. De utvecklar och underhåller relevanta brittiska försvarsstandarder samt tillhandahåller tillhörande standardiseringsråd och vägledning, bland annat status, utveckling, urval och tillämpningen av de brittiska försvarsstandarderna. Samarbete sker även med NATO.

DEF STAN 00-056, (Systemsäkerhet)

Standarden DEF STAN 00-056, S*afety Management Requirements for Defence Systems, Issue* 7 utgiven den 28 februari 2017, är framtagen av *Safety Standards Review Committee vid Defence Equipment and Support* (DE&S) för *UK Ministry of Defence* (UK MOD). Standarden ska främst tillämpas av utvecklande industri i samverkan med Storbritanniens försvarsdepartement UK MOD.

Myndigheten UK MOD:s egna verksamheter styrs ofta av olika *Joint Service Publication* (JSP) dokument enligt deras egen anskaffningsmodell. Standarden ställer krav på systemsäkerhetsverksamhet för det tekniska systemets hela livslängd. Syftet med att tillämpa standarden är att åstadkomma säkerhet för användarna och övriga som kan exponeras vid användning av det tekniska systemet. Standarden kan även användas för riskhantering avseende befarade skador på egendom och yttre miljö.

Standarden är indelad i två delar. Del 1 anger krav på systemsäkerhetsverksamhet och del 2 är en vägledning till del 1. Vidare framgår det av standarden att både myndigheten

UK MOD och industrin måste följa både nationell lagstiftning inklusive EU-direktiv. Standarden rekommenderar att tillämpa civila öppna standarder med de eventuella tillägg som definieras i del 2 eller i andra definierade försvarsstandarder. Beträffande olycksrisken för personskada är begreppet ALARP *(As Low As Reasonably Practicable)* centralt. Begreppet är lagstadgat i Storbritannien. Det definieras och beskrivs när och hur ALARP ska tillämpas och resultatet bedömas. Vidare beskrivs tillämpningen av *Safety Case* och *Safety Case Report*.

Standarden kan tillämpas i samarbetsprojekt med Storbritannien, men den behöver kompletteras med Försvarsmaktens behov av systemsäkerhetsdokumentation.

DEF STAN 00-251 – del 3, (Humanfaktorer)

Standarden DEF STAN 00-251 – del 3, *Human Factors Integration for Defence Systems Part 3: Human Factors System Requirements,* utgiven den 5 februari 2016, av UK Ministry of Defence (UK MOD). Standarden ska främst tillämpas av utvecklande industri i samverkan med Storbritanniens försvarsdepartement UK MOD.

Syftet med standarden är att säkerställa att systemdesignen beaktar människans roll i det tekniska systemet, särskilt när det finns ett gränssnitt mellan människor, utrustning och processer. Standarden ger krav och vägledning för uppnåendet, försäkran och hantering av *Human Factors Integration (*HFI).

NATO:s försvarsstandarder, STANAG

NATO:s försvarsstandarder benämns STANAG *(NATO Standardization Agreement).* Tillhörande standarden kan det finnas en eller flera *Allied publications* (AP) och/eller civila publikationer. *Allied publications* (AP) reglerar processer, rutiner, villkor och förutsättningar för såväl gemensam militär verksamhet som för konstruktion och framtagning av militär materiel. *Allied publications* (AP) tillämpas av nationer som antingen är NATO-medlemmar eller på annat sätt samverkar med NATO.

Varje NATO-medlem ratificerar aktuella *Allied publications* (AP) och implementerar dem inom den egna försvarsmyndigheten. Genom att gemensamt tillämpa *Allied publications (*AP) kan varje medlemsstat dra fördel av en annan medlemsstats redan genomförda framtagnings- och anskaffningsarbete för ett visst tekniskt system då standardiseringen säkerställer att arbetet är i linje med de egna kraven. *Allied publications* (AP) ligger också till grund för den tekniska interoperabiliteten av kommunikation och information som är väsentliga för NATO och dess allierades verksamhet. Många *Allied publications* (AP) bygger i sin tur på olika civila standarder från exempelvis ISO. NATO:s försvarsstandarder och *Allied publications* (AP) publiceras på engelska och franska.

Eftersom STANAG oftast utgör ett ramdokument med överenskommelse om tillämpning för ett specifikt område, finns därför oftast ytterligare detaljerade beskrivningar och vägledningar i tillhörande dokument såsom AOP, AQAP, AECTP, AAS3P, AASTP m.fl. Relevant tillhörande dokument refereras till från aktuell STANAG.

Svenska försvarsstandarder, FSD

De svenska försvarsstandarderna (FSD) fastställs av FMV och består bland annat av standarder för provning, märkning, ritteknik och material. Materialstandarderna reglerar olika områden, exempelvis färg och lacker, förpackningar och distribution, järn och stål, smörjmedel och ytbehandling. Standarderna utarbetas i syfte att harmonisera de tekniska krav som ställs på försvarsmateriel.

Inom Försvarsmakten och FMV har det under flera år funnits en inriktning som anger att vid val av standarder ska strävan vara att minimera användning av svenska försvarsstandarder i syfte att säkerställa interoperabilitet.

FSD 9251, (Humanfaktorer)

Standarden FSD 9251, *Integration av humanfaktorer i försvarssystem*, utgiven den 25 juni 2018, ställer krav på och ger vägledning i hur integrationen av humanfaktorer uppnås, genomförs och följs upp i utvecklings- och anskaffningsprojekt gällande försvarssystem.

Standarden har sitt ursprung i Storbritanniens försvarsdepartement (UK MOD) första version av DEF STAN 00-251 daterad 5 februari 2016, och Sverige har av

Storbritannien fått tillåtelse att översätta och anpassa den till svenska förhållanden. DEF STAN 00-251 utarbetades av *Defence Equipment and Support* (DE&S). Standarden har översatts och anpassats av FMV inom ramen för organet för nationell försvarsstandardisering, FSD.

Standarden är avsedd att användas vid systemutformning av nya tekniska system och produkter, samt vid ändring (modifiering) av befintliga tekniska system. Standarden innehåller både användarkrav och tekniska krav för humanfaktorer.

Tyska försvarsstandarder

BAAINBw, (Systemsäkerhet)

Standarden *BAAINBw, System Safety Demonstration Manual (01/04/2014) är framtagen och utgiven av German Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw)*. Standarden finns på tyska, engelska och franska.

Standarden är i första hand avsedd att användas vid utveckling och modifiering av vapensystem. Termen vapensystem avses i standarden i dess vida bemärkelse att även omfatta vapenplattformar och annan utrustning, så benämningen systemsäkerhet kan anses mer relevant. Standarden anknyter till SS-EN 61508 (serie) och MIL-STD-882E avseende metodik och definitioner. Standarden omfattar både systemsäkerhet och vapensystemsäkerhet.

Definitioner av sannolikheter och allvarlighetsklasser finns tabellerade och baseras på exempel i MIL-STD-882E samt STANAG 4297/AOP-15. Vidare finns exempel på riskmatris. Allvarlighetsklassningen är uppdelad i tre olika materielkategorier som relateras till storlek av installationen, exempelvis för fartyg, stridsfordon, eller komponenter.

Standarder såsom DEF STAN 00-55 och IEC 61508 relateras som tillämpbara standarder, kompletterade med ytterligare delar som beskrivs. Vidare beskrivs hela programvaruframtagningsprocessen med konfigurationsstyrning, utvecklingsverktyg med metoder, verifiering och validering, samt problemställningar såsom modularitet, gränsytor, återanvändning och övervakning av funktioner.

Den tyska standarden hanterar även icke-tekniska faktorer för systemsäkerhet, främst utmaningar kring människans inverkan på, och samverkan med ett tekniskt system. Vägledning för analys av mänskligt felhanterande presenteras, såsom sannolikheter för felhantering.

Internationella elektrotekniska kommissionen, IEC

International Electrotechnical Commission (IEC) är ett internationellt, globalt standardiseringsorgan vars främsta syfte är att arbeta fram och fastställa internationella standarder inom elektroteknik och elektronik. Medlemmar är nationella standardiseringsorgan. Elområdet genom IEC har en lång tradition av att utarbeta globala standarder. IEC:s standarder kan tillämpas direkt men flertalet överförs till europeisk EN-standard genom CENELEC. Vissa IEC-standarder kan också överföras direkt som svensk standard (SS). Svensk medlem i IEC är Svensk elstandard (SEK). I vissa fall sker ett gemensamt standardiseringsarbete IEC-ISO under en parts ledning.

IEC 61508, (Elektriska/elektroniska/programmerbara elektroniska system)

Serien av standarder IEC 61508-x, *Säkerhetsfordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska systems funktion*, är globalt etablerade standarder för säkerhetskritiska system. Standarderna är utvecklade inom *International Electrotechnical Commission* (IEC) men har även antagits som europeiska och därmed också som svenska standarder och kallas då SS-EN 61508-x.

Standarderna är generiska, oberoende och berör hela livscykeln. De har ingen speciell civil eller militär aspekt. Standarderna gäller specifikt för säkerhetsfunktioner men många delar av dem, dock inte alla, kan användas för hela det tekniska systemet. Inga speciella krav finns avseende skador på egendom eller miljö. Ingen koppling görs heller till verksamhetsområden såsom mark, sjö eller luft. Ett område som undantas i standardserien är medicinsk utrustning som istället täcks av standarder i serierna IEC 60601 och IEC 80601 *Elektrisk utrustning för medicinskt bruk.* Standardserierna är inte harmoniserad med maskindirektivet, men flertalet europeiska överföringar (EN) i serien avses bli harmoniserade med EU-förordningarna (MDR, IVDR) om medicintekniska produkter.

Internationella standardiseringsorganisationen, ISO

International Organization for Standardization (ISO) är ett internationellt, globalt standardiseringsorgan, representerat av nationella standardiseringsinstitutioner. ISO arbetar inom det icke-elektriska området. ISO-standarder omfattar både krav på tekniska system, produkter och tjänster samt på verksamhetsledningssystem såsom kvalitet, miljö, arbetsmiljö och informationssäkerhet. CEN omvandlar relativt ofta ISO-standarder till europeisk standard (EN), vilka ska överföras såsom svensk standard (SS) utan ändringar. Svensk medlem i ISO och CEN är Svenska institutet för standarder (SIS). I vissa fall sker ett gemensamt standardiseringsarbete ISO-IEC under en parts ledning.

Standarder för maskinsäkerhet utvecklade av ISO

En teknisk standard för maskinsäkerhet fastställer bland annat mått och storlekar samt krav på funktion och egenskaper för produkter. Syftet med tekniska standarder är dels att harmonisera de gällande tekniska kraven för att uppnå ett starkt skydd för hälsa och säkerhet, dels att säkerställa fri rörlighet för produkter på olika marknader.

Standarderna för maskinsäkerhet är indelade i tre kategorier, A, B och C. De två första kategorierna A och B, omfattas av den tekniska kommittén för maskinsäkerhets arbetsområde medan C-standarderna utvecklas i respektive kommitté för den speciella maskintypen som standarderna avser.

A-standarder är övergripande standarder som definierar de grundläggande hälso- och säkerhetskraven för alla sorters maskiner. Exempel på A-standard är SS-EN ISO 12100, *Maskinsäkerhet – Allmänna konstruktionsprinciper – Riskbedömning och riskreducering.*

B-standarder är gruppstandarder för säkerhet som behandlar en säkerhetsaspekt eller en typ av säkerhetsrelaterad anordning som kan användas för en mängd maskiner. Ett exempel på B-standard är SS-EN ISO 13850, Maskinsäkerhet - *Nödstoppsutrustning – Konstruktionsprinciper.* Att den är en B-standard innebär att den kan appliceras på alla typer av maskiner där ett nödstopp undanröjer eller reducerar olycksrisker. Standarden tar bland annat upp symboler för nödstoppsanordningar, stoppkategorier och krav på själva manöverdonet.

För de maskiner som har stora riskkällor och som behöver detaljerade krav har det tagits fram C-standarder. C-standarder är säkerhetsstandarder för maskintyper som ger detaljerade säkerhetskrav med riskanalys, riskbedömning och riskreducering för en särskild maskin eller grupp av maskiner. Om en C-standard har motstridiga eller strängare krav än vad som anges i A- eller B-standarden, så är det C-standardens krav som är överordnade. Exempel på områden där det finns specifika C-standarder är lyftredskap och handhållna maskiner.

Standarden SS-EN ISO 12100, *Maskinsäkerhet – Allmänna konstruktionsprinciper –Riskbedömning och riskreducering,* är en internationellt vedertagen standard för säkerhetsbedömning av maskiner. Standarden hanterar endast personskador och inte skador på egendom eller yttre miljö. Den täcker inte heller in informationssäkerhetsaspekter.

Syftet med standarden är att förse en aktör med konstruktions- och produktionsansvar med allmänna riktlinjer och vägledning för att konstruera maskiner som är säkra vid avsedd användning. Den innehåller dessutom en strategi för utarbetande av normativa standarder.

Standarden anger grundläggande terminologi, principer och en metodik för att uppnå säker konstruktion av maskiner samt anger principer för riskbedömning och riskreducering. Standarden hänvisar till SS-EN IEC 60204-1, *Maskinsäkerhet – Maskiners elutrustning – Del 1: Allmänna fordringar*, vilken är nödvändig när denna standard ska tillämpas. Denna standard är harmoniserad under EU-direktivet för maskiner då detta numera inkluderar elektriska risker med maskiner.

Standarden SS-EN ISO 12100 kan tillämpas på alla typer av maskiner, under hela deras livscykel. Den beskriver utförligt vilken information som behövs för att genomföra en riskbedömning, och den beskriver metoder för att identifiera, uppskatta och utvärdera olycksrisker. Dessutom innehåller den vägledning om hur riskbedömningen och riskreduceringsprocessen bör dokumenteras och verifieras.

Skyddsåtgärder kan vara *konstruktionsinriktade* (inbyggd säkerhet), *tekniska skydd* och/eller *information* till användaren. Skyddsåtgärder ska vidtas i nämnda ordningsföljd (benämnt integrering av säkerheten) och information får inte vara den enda riskreducerande åtgärden. Användaren kan minska olycksrisken genom att praktisera föreskrivna användningssätt och användning av personlig

skyddsutrustning. Systemsäkerhetsanalysen ska ge den erforderliga information som krävs för riskvärdering och för att bedöma om en riskreducering har uppnåtts eller inte. Dessa bedömningar kan vara kvalitativa eller kvantitativa.

SS-ISO 26262, (Vägfordon)

Standardserien SS-ISO 26262-x, *Vägfordon – Funktionssäkerhet i el- och elektroniksystem* är en internationell standard avsedd för fordonsindustrin. Den behandlar hela livscykeln från konceptframtagning, till systemkonstruktion, hårdvaruutveckling, programvaruutveckling, utvärdering samt användning och underhåll. Standardserien består av tio delar.

Standardserien bygger i huvudsak på IEC 61508, men är sektorspecifika versioner för funktionssäkerhet för vägfordon. Standarderna beskriver processen ur ett livscykelperspektiv. Seriens delar hanterar olycksrisker beroende på felfunktion hos elektriska och elektroniska system, men hanterar inte klassiska olycksrisker såsom el, brand och rök. Serien är enbart inriktad på personers säkerhet och täcker inte skador på egendom, miljö eller informationssäkerhet.

SS-EN ISO 14971, (Medicintekniska produkter)

Standarden SS-EN ISO 14971, *Medicintekniska produkter – Tillämpning av ett system för riskhantering för medicintekniska produkter* och är i första hand avsedd att användas för medicintekniska produkter inklusive ingående eller fristående programvara. Standarden fastställer krav och beskriver en process för hur tillverkare kan identifiera, hantera (värdera, eliminera, reducera, informera) och övervaka olycksrisker förknippade med konstruktion/användning av medicintekniska produkter. Olycksriskerna är främst patientrelaterade, men kan även vara kopplade till operatörer, utrustning och miljö. Standarden omfattar alla stadier i en medicinteknisk produkts livscykel.

Internationella teleunionen, ITU

International Telecommunication Union (ITU) är ett globalt standardiseringsorgan för informations- och kommunikationsteknologi (IKT) och är ett fackorgan inom FN. Arbetet innefattar allokering av radiofrekvenser och villkor samt tekniska standarder för kommunikation på land, till sjöss och via satelliter. Publikationer inkluderar Radioreglementet (Radio Regulations) och standarder (Recommendations). Vissa publikationer och villkor kan göras tvingande genom

Post- och Telestyrelsen (PTS). Gällande spektrumanvändning finns särskilda regler för säkerhets- och totalförsvarsmyndigheter.

Europeiska standardiseringsorganisationer

Kommittén för europeisk standardisering, CEN

Comité Européen de Normalisation (CEN) är en av de tre europeiska standardiseringsorganisationer som erkänns av EU och Efta. CEN ansvarar för utveckling av EN-standarder inom alla områden och branscher utom elektroteknik och telekommunikation. EN-standarder ska överföras till svensk standard (SS) utan ändringar. CEN är en oberoende och icke-statlig organisation som företräds av sina standardiseringsorgan. SIS (Svenska institutet för standarder) företräder Sverige och är därmed medlem i CEN. CEN kan genom mandat från Kommissionen utarbeta harmoniserade standarder som innehåller detaljerade specifikationer av de väsentliga kraven i ett EU-direktiv. Mycket av arbetet bygger på motsvarande arbete och standarder framtagna globalt av ISO.

Kommittén för europeisk elektrostandardisering, CENELEC

Comité Européen de Normalisation Électrotechnique, CENELEC (även förkortat CLC) tar fram och fastställer EN-standard på det elektrotekniska området. EN-standarder ska överföras till svensk standard (SS) utan ändringar. CENELEC är en oberoende organisation som företräds av sina standardiseringsorgan. SEK (Svensk Elstandard) är svensk nationalkommitté i CENELEC. Även CENELEC kan efter mandat från Kommissionen ta fram harmoniserade standarder som specificerar de väsentliga kraven i ett EU-direktiv. Arbetet syftar i första hand till att fastställa global el-standard utarbetad inom IEC, som europeisk standard.

Europeiska institutet för standardisering inom telekommunikation

European Telecommunications Standards Institute (ETSI) är ett oberoende standardiseringsorgan för informations- och kommunikationsteknologi (IKT). Organisationens medlemmar utgörs bland annat av myndigheter, nätoperatörer, tjänsteleverantörer, tillverkare, forskningsorgan och användare. Svenska Informations- och Telekommunikationsstandardiseringen (ITS) är medlem i ETSI och sammanhåller standardiseringen för IKT i Sverige. På samma sätt som organen ovan, utarbetar ETSI harmoniserade standarder. ETSI har vissa kopplingar och tar vissa underlag från ITU.

Andra verksamhetsstandarder för systemsäkerhetsverksamhet

Det finns även andra branschorganisationer som ger ut standarder inom systemsäkerhetsområdet, såväl allmänna som sektorsspecifika.

GEIA-STD-0010A, (Systemsäkerhet)

Standarden GEIA-STD-0010A, *Standard Best Practice for System Safety Program Development and Execution* (October 2015) är framtagen och utgiven av *Information Technology Association of America* (ITAA) *G-48 System Safety Committee*. Standarden är tillika en *American National Standard Institute* (ANSI) standard.

Standarden GEIA-STD-0010A är en civil motsvarighet till MIL-STD-882E och kan i sin helhet tillämpas för militär materiel. Dock krävs vissa tillägg såsom aktiviteter för krav- och beslutsdokument. Standarden är avsedd att i första hand användas av en aktör med konstruktions- och produktionsansvar vid framtagning av tekniska system. Standarden innehåller definitioner av centrala termer och begrepp samt en modell för att summera olycksrisker för det tekniska systemet. Standarden anger ett antal minimikrav i form av element som alltid ska uppfyllas för alla system. Begreppet ALARP *(As Low As Reasonably Practicable)* används.

SAE ARP 4754A, (Flyg)

Standarden SAE ARP4754A, *Aerospace Recommended Practice – Guidelines for Development of Civil Aircraft and Systems* gäller för systemaspekter och refererar till DO-178C/ED-12C för utveckling av programvara och DO-254/ED-80 för utveckling av programmerbar logik (Airborne Electronic Hardware, *”Functions that are allocated to hardware”*) samt till SAE ARP 4761 för genomförande av systemsäkerhetsanalys. Standarden är framtagen i samarbete mellan tillverkare, myndigheter och forskningsinstitutioner i USA, Kanada och Europa. Standarden kan inte användas separat utan måste användas tillsammans med ovan nämnda associerade standarder. Standarden täcker inte in informationssäkerhetsaspekter.

Standarden SAE ARP 4754A är en civil standard för luftfartyg, men tillämpas ofta också för militära system. Standarden beskriver ett arbetssätt för utvecklingsarbetet där systemsäkerhetspåverkan (luftvärdighetspåverkan) av respektive funktion och komponent styr vilket arbete som ska genomföras och med vilken stringens.

Denna klassificering sker genom tilldelning av *Development assurance level,* FDAL till funktioner *(functions)* och IDAL till komponenter *(items*). Det beskrivs vilka kombinationer av *Development assurance level* (DAL) i ingående delar som kan accepteras för olika klasser av konsekvenser.

Bilaga 3

Beskrivning av systemsäkerhets-aktiviteter

Syftet med denna bilaga är att dels beskriva de unika svenska aktiviteterna, dels de aktiviteter som finns beskrivna i standarden MIL-STD-882E. Vidare beskrivs de anpassningar som behöver göras utifrån beskrivningar i standarden MIL-STD-882E för att passa för de svenska försvarsmyndigheternas arbete.

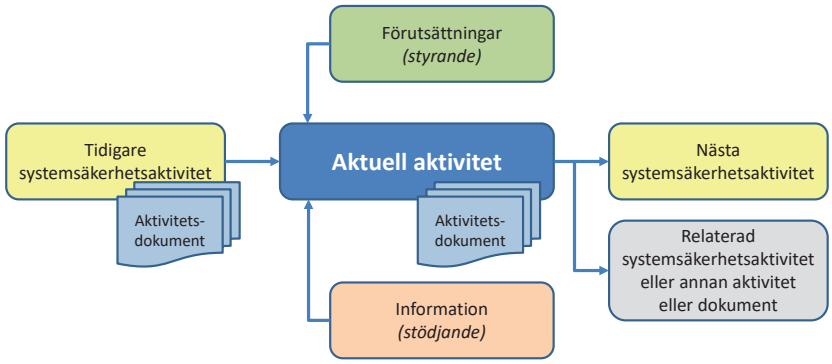
Aktivitetspresentation

De unika svenska aktiviteterna identifieras med bokstaven ”S” följt av ett två-siffrigt tal. De övriga aktiviteterna, vilka baseras på MIL-STD-882E, är i vissa fall anpassade för de svenska försvarsmyndigheternas systemsäkerhetsarbete.

Kursivt markerad aktivitet finns beskriven i MIL-STD-882E, men används inte i de svenska försvarsmyndigheternas systemsäkerhetsarbete.

För varje aktivitet är formeringen enligt nedan:

- *Syfte och aktivitetsbeskrivning* förklarar ändamålet med aktiviteten och hur aktiviteten lämpligen utförs. I vissa fall finns checklistor att följa. Här finns även dess svenska respektive engelska benämningar på aktiviteten och dokumentationen.
- *Indata, utdata och flödesbild* anger vilken information som behövs för att genomföra aktiviteten samt vilken dokumentation (aktivitetsdokument) som tas fram.



Bilaga 3, bild 1 *För varje aktivitet finns en bild som visar indata, aktivitet, aktivitets-dokument och utdata som stöd till kommande aktiviteter.*

Förutsättningar (grön ruta) betraktas som styrande för aktuell aktivitet, medan *Information* (orange ruta) betraktas som stödjande. Gråa rutor pekar på relaterade systemsäkerhetsaktiviteter, alternativt på andra aktiviteter eller dokument.

Processbeskrivning som utgår från kravställaren

Kravställare, beställare, systemintegratör och *konstruktör* kan i princip genomföra samma aktiviteter och i stort följa samma aktivitetsbeskrivningar. Aktiviteterna kan användas vid lite olika tillfällen under systemsäkerhetsarbetet, men även med lite skilda syften och omfattning. Detta innebär att indata, förutsättningar (styrande) och information (stödjande) kan skilja sig åt mellan rollerna, vilket innebär att mängden arbete och volymen utdata kan variera mellan *kravställare*, *beställare, systemintegratör* och *konstruktör.*

Aktiviteternas ordningsföljd och bilderna i respektive aktivitet ger i första hand stöd för *kravställarens* systemsäkerhetsverksamhet. Det finns även bilder för *beställare*, *systemintegratör* och *konstruktör* under flertalet av aktiviteterna, även om de inte alltid presenteras i ett logiskt processflöde för dessa roller.

Aktiviteter – SEKTION 100 – Planering/Styrning

TASK 101 – System Safety Program (SSP)

Denna aktivitet är ersatt av S11 – Systemsäkerhetsprogram (SSP), Task 102 - System Safety Program Plan (SSPP) samt kapitel 14 Riskmatris och tolerabel risknivå.

S11 – Systemsäkerhetsprogram (SSP)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att styra och inrikta *kravställarens* systemsäkerhetsverksamhet i ett livscykelperspektiv för stridskraftsområde, produktområde eller i vissa fall för komplexa tekniska system.

Den engelska benämningen på aktiviteten är *System Safety Program* (SSP) och utdata/dokumentation är *System Safety Management Plan* (SSMP). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetsledningsplan* (SSMP).

Kravställarens systemsäkerhetsverksamhet fastställs i en *Systemsäkerhetsledningsplan* (SSMP) och utgör därefter styrdokument ur systemsäkerhetsperspektiv för olika målsättnings- och kravdokument såsom *Systemmålsättning* (SMS) och *Förfrågningsunderlag* (RFP). Alla tekniska system och produkter ska omfattas av någon*Systemsäkerhetsledningsplan* (SSMP).

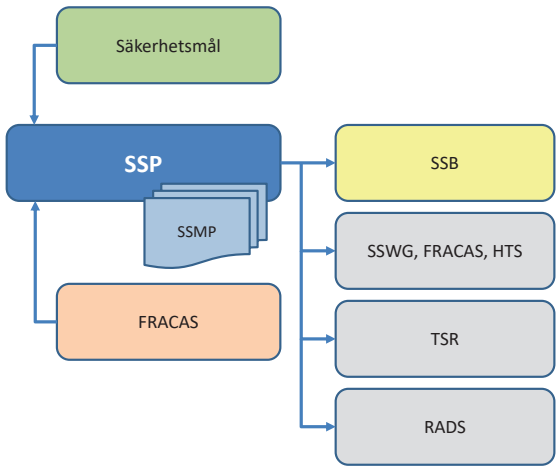
Kravställaren identifierar övergripande aktuell EU-rätt, svensk lagstiftning samt vilka domäner av standarder och andra regelverk som ska tillämpas. Vidare identifieras vanligt förekommande olycksrisker som har dimensionerande konsekvenser på aktuell materiel inom området. Krav på *Tolerabel risknivå* (TR) uttryckt i riskmatris ställs samt inriktning ges för hur systemsäkerhetsverksamheten ska genomföras utifrån de obligatoriska och de selektivt valda aktiviteterna. *Systemsäkerhetsledningsplanen* (SSMP) ger även instruktioner för arbetet som sker i *Arbetsgrupp för systemsäkerhet* (SSWG).

Systemsäkerhetsledningsplanen (SSMP) tillsammans med *Systemmålsättningar* (SMS) styr *beställarens* kommande systemsäkerhetsarbete för aktuella tekniska system.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsprogram* (SSP) utgörs av säkerhetsmål samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

Utdata är *Systemsäkerhetsledningsplan* (SSMP). Den ger indata till *Systemsäkerhetsbedömning* (SSB), *Arbetsgrupp för systemsäkerhet* (SSWG), *Handhavande och utbildning* (TSR) samt *Riskanalys inför avveckling av system* (RADS).



Bilaga 3, bild 2 *Systemsäkerhetsprogram (SSP).*

En *Systemsäkerhetsledningsplan* (SSMP) bör innehålla:

- Vilken arena, produktområde eller tekniskt system som omfattas
- En organisationsbeskrivning för systemsäkerhetsverksamheten och hur denna samverkar med övriga aktörer och andra intressenter
- Vilken systemsäkerhetsverksamhet som genomförs under hela livscykeln
- Inriktningar och acceptanskriterier för tillåtna vägval enligt *Vägvalsmodellen* (VVM)
- Vilken EU-rätt och svensk lagstiftning samt vilka domäner av standarder och andra regelverk som ska tillämpas
- Systemsäkerhetsmål inklusive krav på *Tolerabel risknivå* (TR) uttryckt i riskmatriser
- Krav på att *beställare* och/eller *konstruktörer i*nom Försvarsmakten tar fram *Systemsäkerhetsplaner* (SSPP) för systemsäkerhetsarbete vid ändring (modi-

fiering), arbete med system-av-system samt vid anskaffning av tekniska system och produkter
- Hur genomfört systemsäkerhetsarbete ska dokumenteras och rapporteras
- Kriterier för när systemsäkerhetsbeslut ska utfärdas
- Hur säkerhetsbrister på tekniska system och produkter omhändertas
- En arbetsbeskrivning för *Arbetsgrupp för systemsäkerhet* (SSWG)
- Hantering av underlag från olyckor, tillbud och felrapportering
- Hur olycksrisker hanteras som kan inträffa vid avveckling
- En lista över vanligt förekommande olycksrisker inom produktområdet
- Revision av S*ystemsäkerhetsledningsplanen* (SSMP)

S12 – Systemsäkerhetsbedömning (SSB)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att prioritera, rangordna och/eller beskriva för- och nackdelar med alternativa koncept eller tekniklösningar ur systemsäkerhetssynpunkt.

Den engelska benämningen på aktiviteten är *System Safety Evaluation* (SSB) och utdata/dokumentation är *System Safety Concept Evaluation* (SSKB). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetskonceptbedömning* (SSKB).

Systemsäkerhetsbedömning (SSB) genomförs innan kravställning av tekniska system påbörjas för att identifiera, analysera och väga dimensionerande systemsäkerhetsaspekter mot andra generella faktorer såsom verkan och övrig prestanda. Aktiviteten avser att ge stöd vid utarbetande av *Systemmålsättningar* (SMS), men den kan även tillämpas i verksamheten *Forskning- och teknikutveckling* (FoT).

Kravställaren identifierar potentiellt svårhanterliga systemsäkerhetsaspekter utifrån att bedöma möjligheten att kunna omhänderta dessa olycksrisker i tekniska system eller i verksamheten. Exempelvis bör oprövad teknik, hanterbarhet av vissa olycksrisker samt miljöbelastning vid användning och avveckling beaktas.

Kravställaren identifierar farliga tillstånd och situationer som kan inträffa. Därutöver förtecknas farliga delsystem, produkter och kemiska produkter. *System-*

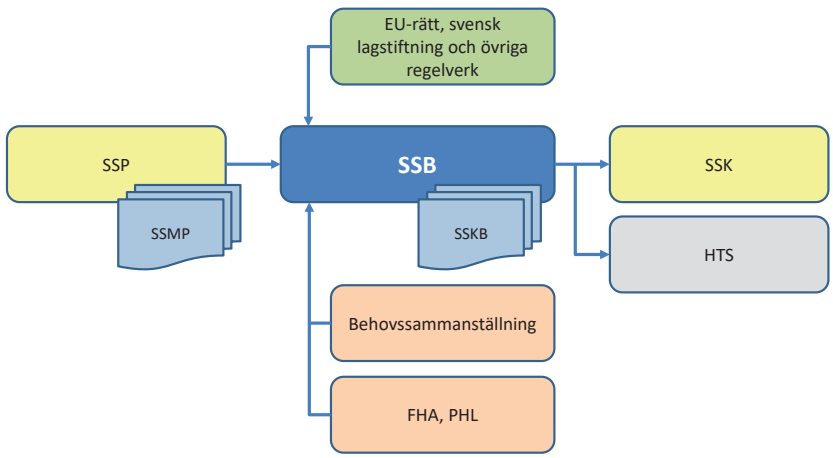
säkerhetskonceptbedömning (SSKB) fokuserar på de mest svårbedömda potentiella olycksriskerna och ger *kravställaren* ett beslutsunderlag.

För oprövad teknik kan fortsatta studier eller utredningar krävas. För hanterbarhet av olycksrisker samt miljöbelastning kan skyddsåtgärder behöva vidtas såsom stora riskområden, begränsningar i användning eller behov av personlig skyddsutrustning (PPE).

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsbedömning* (SSB) utgörs av *Systemsäkerhetsledningsplan* (SSMP), lagstiftning samt underlag från aktiviteten Behovssammanställning. För att identifiera farliga tillstånd och situationer kan inledande riskbedömningar enligt *Funktionell riskanalys* (FHA) och *Riskkällelista* (PHL) tillämpas.

Utdata är *Systemsäkerhetskonceptbedömningen* (SSKB). Den ger indata till *Systemsäkerhetskrav (*SSK) och *Riskhanteringssystem* (HTS).



Bilaga 3, bild 3 *Systemsäkerhetsbedömning (SSB).*

En *Systemsäkerhetsbedömning* (SSB) bör innehålla:

- Vilken teknik som omfattas och dess mognadsgrad
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Beskrivning av vilka riskanalysmetoder som använts

- Vilka olycksrisker som kan inträffa samt dess bedömda konsekvenser
- Sammanfattning av resultatet
  - Värdering (olika alternativ)
  - Rangordnat
  - För- och nackdelar
- Utmönstring av svårhanterliga tekniklösningar
  - Rekommendation om riskreducerande åtgärder
  - Förslag till framtida systemsäkerhetsprovning
- Detaljerad redovisning som ligger till grund för sammanfattningen

S13 – Systemsäkerhetskrav (SSK)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera de systemsäkerhetskrav som ska ingå i olika målsättnings- och kravdokument.

Den engelska benämningen på aktiviteten är *System Safety Requirement* (SSK) och utdata/dokumentation är *System Safety Requirement* (SSK). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetskrav* (SSK).

Systemsäkerhetskraven (SSK) identifieras i EU-rätt, svensk lagstiftning, regelverk, *Designregler* (DR) och utifrån vunna erfarenheter. Identifierade systemsäkerhetskrav utgörs dels av tekniska krav som påverkar konstruktionen, dels av krav på systemsäkerhetsarbete för att visa att det tekniska systemet erbjuder betryggande säkerhet. Som stöd för denna aktivitet tillämpas *Vägvalsmodellen* (VVM).

Kravställarens syfte med denna aktivitet är att identifiera de tekniska systemsäkerhetskraven som ska ingå i *Systemmålsättning* (SMS 2) för aktuellt tekniskt system. Även *kravställarens* krav på *beställarens* systemsäkerhetsarbete ingår. Normalt sett refereras endast till *Systemsäkerhetsledningsplan* (SSMP) i *Systemmålsättningen* (SMS 2). Kompletterande tekniska systemsäkerhetskrav samt utökade krav på *beställarens* systemsäkerhetsarbete kan dock erfordras utifrån aktuellt tekniskt system.

Kravställaren utgår från *Systemsäkerhetsledningsplanen* (SSMP), *Systemsäkerhetsbedömningen* (SSB) samt underlaget från aktiviteten *Behovssammanställning* och

preciserar vid behov kraven för att *beställaren* ska kunna visa att betryggande säkerhet uppnås genom de tillåtna vägvalen i *Vägvalsmodellen* (VVM). Övergripande acceptanskriterier samt eventuella randvillkor och begränsningar anges för respektive vägval. Kompletterande tekniska systemsäkerhetskrav ställs på en principiell nivå utan att begränsa *beställarens* eller i förlängningen *konstruktörens* utformning av det tekniska systemet. Alla tekniska system och produkter ska omfattas av någon *Systemmålsättning* (SMS 2).

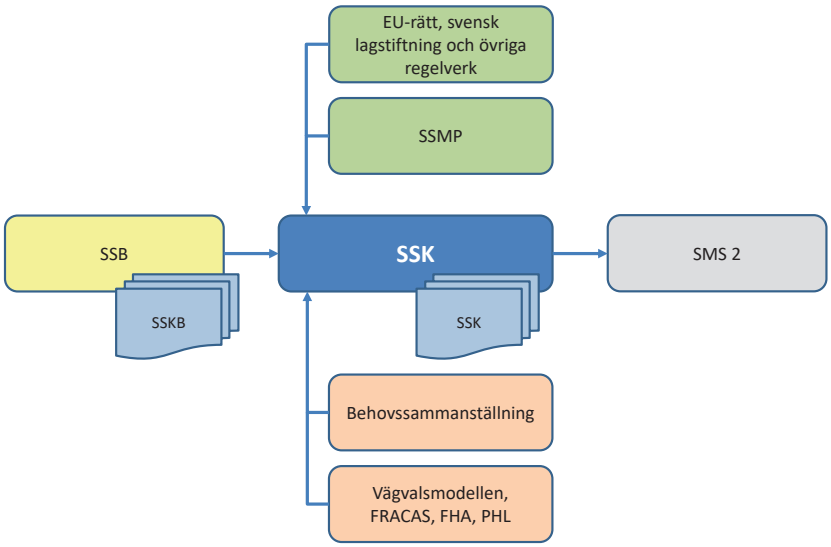
Beställarens syfte med denna aktivitet är att identifiera de tekniska systemsäkerhetskraven som ska ingå i *Förfrågningsunderlaget* (RFP) för aktuellt tekniskt system. Även *beställarens* krav på *konstruktörens* systemsäkerhetsarbete ska ingå i *Förfrågningsunderlaget* (RFP). Systemsäkerhetskraven i aktuell *Systemmålsättning* (SMS 2) omsätts till entydiga och verifierbara krav i *Förfrågningsunderlage*t (RFP). Ytterligare tekniska systemsäkerhetskrav samt utökade krav på *konstruktörens* systemsäkerhetsarbete kan dock erfordras utifrån aktuellt tekniskt system.

Beställaren utgår från aktuell *Systemmålsättning* (SMS 2) och preciserar kraven för betryggande säkerhet genom de tillåtna vägvalen i *Vägvalsmodellen* (VVM). Acceptanskriterier samt eventuellt skärpta randvillkor och begränsningar anges. Kompletterande tekniska systemsäkerhetskrav ställs på en funktionell nivå utan att begränsa *konstruktörens* utformning av det tekniska systemet. Alla tekniska system och produkter som ska anskaffas eller ändras (modifieras) ska omfattas av ett *Förfrågningsunderlag* (RFP).

Indata, utdata och flödesbild

Indata till aktiviteten S*ystemsäkerhetskrav* (SSK) för *kravställare* utgörs av *Systemsäkerhetsbedömning* (SSB), lagstiftning och *Systemsäkerhetsledningsplan* (SSMP) samt underlag från aktiviteten *Behovssammanställning*, exempelvis studier och erfarenheter från de tekniska system och produkter som ska omsättas. Som ytterligare stöd kan *Funktionell riskanalys* (FHA) och *Riskkällelista* (PHL) tillämpas.

Utdata är de *Systemsäkerhetskrav* (SSK) som *kravställaren* ska infoga i *Systemmålsättning* (SMS 2).



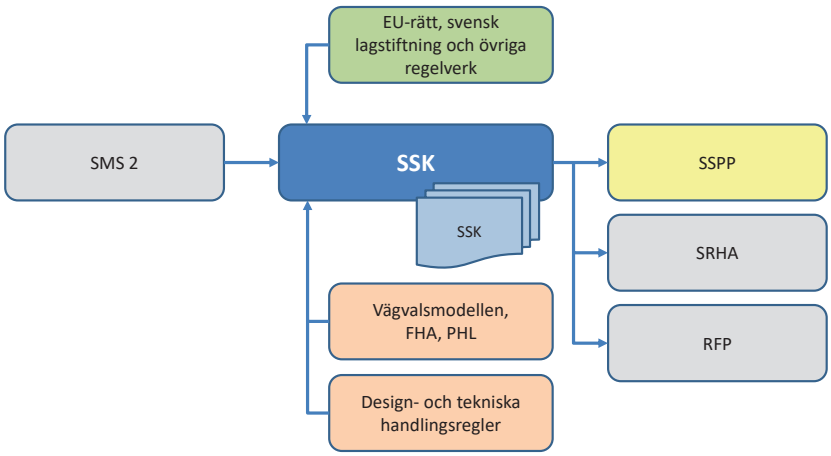
Bilaga 3, bild 4 *Systemsäkerhetskrav (SSK) för kravställare.*

Systemsäkerhetskrav (SSK) till en *Systemmålssättning* (SMS 2) bör utöver ställda krav i *Systemsäkerhetsledningsplanen* (SSMP) omfatta:

- Tekniska krav:
  - Eventuella specifika krav på EU-rätt, svensk lagstiftning samt om särskilda standarder och andra regelverk ska tillämpas
  - Vilka handböcker (designregelsamlingar) *Designregler* (DR) som ska tillämpas
- Verksamhetsåtagande:
  - Preciserade inriktningar och acceptanskriterier för tillåtna vägval enligt *Vägvalsmodellen* (VVM)
  - Eventuellt ytterligare krav på systemsäkerhetsverksamhet som ska genomföras under livscykeln

Indata till aktiviteten *Systemsäkerhetskrav* (SSK) för *beställare* utgörs *av Systemmålsättning* (SMS 2), lagstiftning samt *Designregler* (DR) och *Tekniska handlingsregle*r (THR). Som ytterligare stöd kan *Funktionell riskanaly*s (FHA) och *Riskkällelist*a (PHL) tillämpas.

Utdata är de *Systemsäkerhetskrav* (SSK) som *beställaren* ska infoga i sin egen *Systemsäkerhetsplan* (SSPP) respektive i *Förfrågningsunderlaget* (RFP). *Systemsäkerhetskraven* (SSK) kommer även att vara indata till *kravställarens System Safety Requirement Hazard Analysis* (SRHA).



Bilaga 3, bild 5 *Systemsäkerhetskrav (SSK) för beställare.*

Systemsäkerhetskrav (SSK) till ett *Förfrågningsunderlag* (RFP) bör utöver ställda krav i *Systemmålssättningen* (SMS 2) omfatta:

- Tekniska krav:
  - Vilken EU-rätt, svensk lagstiftning samt vilka domäner/specifika standarder och andra regelverk ska uppfyllas
  - Principiella konstruktionskrav (designregler) på det tänkta tekniska systemet
  - Systemsäkerhetsmål inklusive *Tolerabel risknivå* (TR) uttryckt i riskmatriser
- Verksamhetsåtagande:
  - En organisationsbeskrivning för systemsäkerhetsarbetet och hur denna samverkar med övriga aktörer och andra intressenter
  - Preciserade acceptanskriterier för tillåtna vägval enligt *Vägvalsmodellen* (VVM)
  - Krav på att ta fram en *Systemsäkerhetsplan* (SSPP) som del av kontraktet och som beskriver det systemsäkerhetsarbete som ska genomförs
  - Hur genomfört systemsäkerhetsarbete ska dokumenteras och rapporteras

TASK 102 – System Safety Program Plan (SSPP)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att beskriva det systemsäkerhetsarbete som *beställare* respektive *konstruktör* planerar att genomföra för aktuellt tekniskt system. Aktiviteten kan dels tillämpas för intern verksamhet, dels för systemsäkerhetsarbete som överenskommits i kontrakt.

Den svenska benämningen på aktiviteten är *Systemsäkerhetsprojektplanering* (SSPP) och utdata/dokumentation är en *Systemsäkerhetsplan* (SSPP). Aktiviteten *System Safety Program Plan* (SSPP) inkluderar MIL-STD-882E Task 103, *Hazard Management Plan* (HMP). Aktiviteten inkluderar även Task 108, *Hazardous Material Management Plan* (HMMP) avseende hälso- och miljöaspekter. Den engelska benämningen på utdata/dokumentation är *System Safety Program Plan* (SSPP).

Systemsäkerhetsplanen (SSPP) ska utifrån de gjorda vägvalen i *Vägvalsmodellen* (VVM) redogöra för det planerade systemsäkerhetsarbetet som dels erfordras för att uppfylla kraven, dels beskriva hur resultaten av detta arbete ska dokumenteras.

Beställarens interna systemsäkerhetsarbete för ett visst tekniskt system beskrivs i en *Systemsäkerhetsplan* (SSPP) och är en del av *beställarens* projektplan. *Systemsäkerhetsplanen* (SSPP) beskriver de systemsäkerhetsaktiviteter som man avser att genomföra och hur detta är tänkt att dokumenteras. Vidare beskrivs vilken systemsäkerhetsdokumentation som överlämnas till *kravställaren* i samband med systemöverlämning (SÖL) samt vilka krav på systemsäkerhetsarbete som man avser att ställa på *konstruktören* eller *systemintegratören*.

Konstruktörens systemsäkerhetsarbete för ett visst tekniskt system beskrivs i en *Systemsäkerhetsplan* (SSPP) och är en del av *konstruktörens* projektplan. *Systemsäkerhetsplanens* (SSPP) innehåll och omfattning styrs av kontraktet. *Konstruktören* beskriver de systemsäkerhetsaktiviteter som man avser att genomföra och hur detta är tänkt att dokumenteras. Detta för att *konstruktören* slutligen kunna göra ett ställningstagande att det tekniska systemet erbjuder betryggande säkerhet.

En preliminär *Systemsäkerhetsplan (*SSPP) kan i ett skede före kontrakt utvärdera en potentiell *konstruktörs* förståelse för och prioritering av det systemsäkerhetsarbete som erfordras vid utveckling eller modifiering av tekniska system.

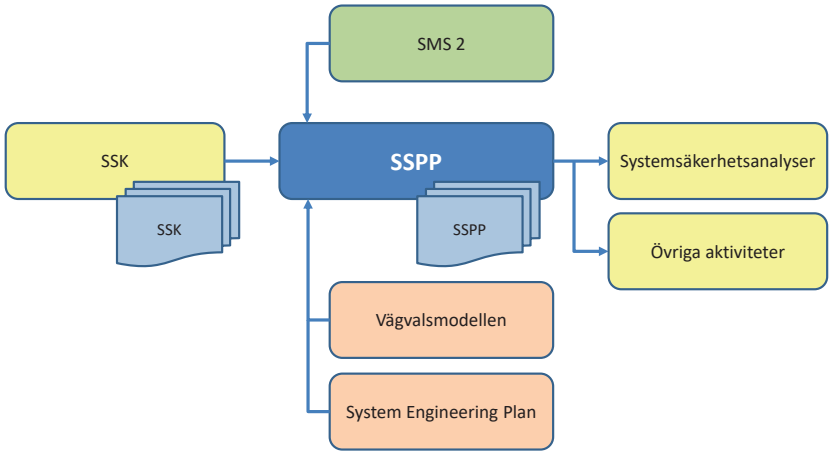
Konstruktören kan lägga till ytterligare systemsäkerhetsaktiviteter än de som *beställaren* har krävt. Vidare beskrivs vilken systemsäkerhetsdokumentation som överlämnas till *beställaren* i samband med leverans och vilka krav på systemsäkerhetsarbete som man avser att ställa på underleverantörer. *Systemsäkerhetsplanen* (SSPP) utgör ofta en integrerad del av System Engineering-processen med dess tekniska granskningar såsom *Preliminary Design Review* (PDR) och *Critical Design Review* (CDR) och bör därför samordnas med dessa.

Systemintegratörens systemsäkerhetsarbete för ett visst system-av-system regleras av *beställarens Systemsäkerhetsplan* (SSPP). *Beställaren* beskriver de systemsäkerhetsaktiviteter som *systemintegratören* minst behöver genomföra och hur detta är tänkt att dokumenteras. Detta för att *beställaren* slutligen kunna göra ett ställningstagande för att samfunktionen mellan tekniska system och produkter till ett system-av-system erbjuder betryggande säkerhet.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsplanering* (SSPP) för *beställaren* utgörs av *Systemsäkerhetskrav* (SSK) och *Systemmålsättning* (SMS 2). Som stöd för denna aktivitet kan *Vägvalsmodellen* (VVM) tillämpas.

Utdata är den *Systemsäkerhetsplan* (SSPP) som *beställaren* ska arbeta efter respektive identifiera krav ur som kan överföras till *Förfrågningsunderlaget* (RFP). *Systemsäkerhetsplanen* (SSPP) kommer även att beskriva vilka systemsäkerhetsanalyser och övriga aktiviteter *beställaren* ska genomföra, vilka återfinns i sektionerna 200 – 500.



Bilaga 3, bild 6 *Systemsäkerhetsplan (SSPP) för beställare.*

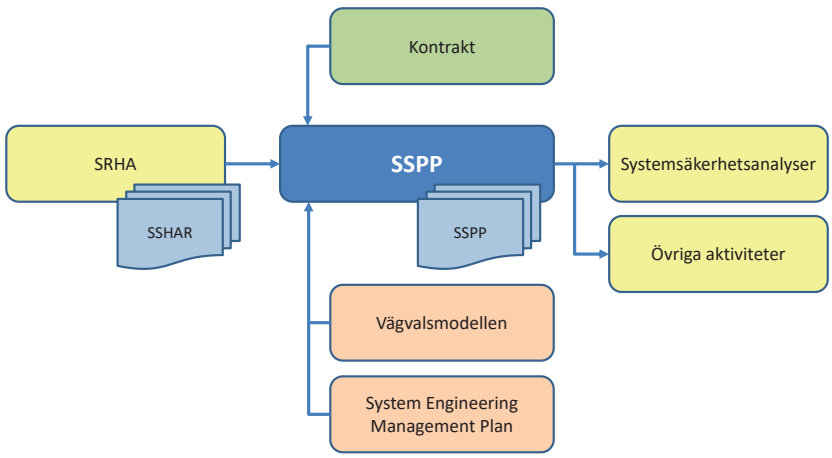
En *Systemsäkerhetsplan (*SSPP) för *beställaren* bör omfatta:

- Syfte, omfattning samt beskrivning av det tekniska systemet och dess användning
- En organisationsbeskrivning för systemsäkerhetsarbetet och hur denna (internt och externt) samverkar med Försvarsmakten, övriga aktörer och andra intressenter inklusive samverkan med andra närliggande kompetensområden *(se bild 2.7)*
- Vilken EU-rätt och svensk lagstiftning samt vilka standarder och andra regelverk som ska tillämpas samt hur *Systemsäkerhetskrav* (SSK) genomförs
- Systemsäkerhetskrav inklusive *Tolerabel risknivå* (TR) uttryckt i riskmatriser
- Inriktningar och acceptanskriterier för vägvalen enligt *Vägvalsmodellen* (VVM)
- Hantering av tillhandahållen materiel (GFE) och andra integrationsprodukter
- En processbeskrivning med koppling till *System Engineering*-processen över det systemsäkerhetsarbete som ska genomföras samt hur detta ska dokumenteras och rapporteras
- Genomförande av systemsäkerhetsgenomgångar dels i *Arbetsgrupp för systemsäkerhet* (SSWG), dels i *Systemsäkerhetsgruppen* (IPT/WG)
- En beskrivning av de systemsäkerhetsanalyser som ska genomföras, hur de dokumenteras samt hur erfarenhetsdata omhändertas
- Hur verifiering och validering av ställda systemsäkerhetskrav genomförs

- En processbeskrivning för stängning av systemsäkerhetsarbete för olycksrisker samt rutiner för hantering av restriktioner
- Hur systemsäkerhetsvärderingen utarbetas
- Hur framtagning av *Systemsäkerhetsdeklaration* (SSD), *Systemsäkerhetsrapport* (SAR), *Risklogg* (RL) samt övrig systemsäkerhetsdokumentation sker
- Hur framtagning av teknisk information utifrån systemsäkerhetsarbetet sker
- Hur genomförande av utbildning sker
- Hur omhändertagande av felrapportering sker
- Hur revision av *beställarens Systemsäkerhetsplanen* (SSPP) sker

Indata till aktiviteten *Systemsäkerhetsplan* (SSPP) för *konstruktören* utgörs av *Systemsäkerhetskravanalysen* (SRHA) och kontraktet med *beställaren*. Som stöd för denna aktivitet kan *Vägvalsmodellen* (VVM) tillämpas.

Utdata är den *Systemsäkerhetsplan* (SSPP) som *konstruktören* ska arbeta efter. *Systemsäkerhetsplanen* (SSPP) beskriver vilka systemsäkerhetsanalyser och övriga aktiviteter *konstruktören* ska genomföra, vilka återfinns i sektionerna 200 – 500.



Bilaga 3, bild 7 *Systemsäkerhetsplan (SSPP) för konstruktör.*

En *Systemsäkerhetsplan* (SSPP) för *konstruktören* bör omfatta:

- Syfte, omfattning samt beskrivning av det tekniska systemet och dess användning
- En organisationsbeskrivning för systemsäkerhetsarbetet och hur denna (internt och externt) samverkar med övriga aktörer och andra intressenter inklusive samverkan med andra närliggande kompetensområden *(se Bild 2.7)*
- Vilken EU-rätt och svensk lagstiftning samt vilka standarder och andra regelverk som ska tillämpas samt hur *Systemsäkerhetskravanalysen* (SRHA) genomförs
- Systemsäkerhetskrav inklusive *Tolerabel risknivå* (TR) uttryckt i riskmatriser
- Inriktningar och acceptanskriterier för vägvalen enligt *Vägvalsmodellen* (VVM)
- Hantering av tillhandahållen materiel (GFE) och andra integrationsprodukter
- En processbeskrivning med koppling till S*ystem Engineering*-processen över det systemsäkerhetsarbete som ska genomföras samt hur detta ska dokumenteras och rapporteras
- Genomförande av systemsäkerhetsgenomgångar i *Systemsäkerhetsgruppen* (IPT/WG)
- En beskrivning av de systemsäkerhetsanalyser som ska genomföras, hur de dokumenteras samt hur erfarenhetsdata omhändertas
- Hur verifiering och validering av ställda systemsäkerhetskrav genomförs
- En processbeskrivning för stängning av systemsäkerhetsarbete för olycksrisker samt rutiner för hantering av restriktioner
- Hur systemsäkerhetsvärderingen utarbetas
- Hur framtagning av *Systemsäkerhetsutlåtande* (SCA), *Systemsäkerhetsrapport* (SAR), *Risklogg* (RL) samt övrig systemsäkerhetsdokumentation sker
- Hur framtagning av teknisk information utifrån systemsäkerhetsarbetet sker
- Hur genomförande av utbildning sker
- Hur omhändertagande av felrapportering sker
- Hur revision av *Systemsäkerhetsplanen* (SSPP) sker

TASK 103 – Hazard Management Plan (HMP)

Denna aktivitet ingår i TASK 102 - System Safety Program Plan (SSPP).

TASK 104 – Support of Government Reviews/Audits (SGRA)

Denna aktivitet regleras dels av Handbok Vapen- och Ammunitionssäkerhet (H VAS) avseende FMV:s Rådgivningsgrupper för Vapen- och ammunitionssäkerhet, dels genom medverkan i Försvarsmaktens Undersökningskommission (FMUK), dels i respektive beställares Systemsäkerhetsplaner (SSPP) för övriga myndighetsgranskningar.

S14 – Arbetsgrupp för systemsäkerhet (SSWG)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att inom systemsäkerhetsområdet vara en rådgivande funktion till *kravställaren*. *Arbetsgruppen för systemsäkerhet* (SSWG) kan dels följa upp tekniska system och produkter under vidmakthållandeskedet, dels bereda inkomna ärenden med koppling till systemsäkerhet. Försvarsmakten inrättar *Arbetsgrupper för systemsäkerhet* (SSWG).

Den engelska benämningen på aktiviteten är *System Safety Working Group* (SSWG) och utdata/dokumentation är protokoll eller mötesanteckningar.

Ordförande i *Arbetsgruppen för systemsäkerhet* (SSWG) upprätthåller en arbetsbeskrivning baserat på kraven i *Systemsäkerhetsledningsplanen* (SSMP). Ordföranden leder det operativa arbetet med att föreslå bemanning till arbetsgruppen, kalla till möten och att protokoll eller mötesanteckningar förs. *Beställaren* kan adjungeras till arbetsgruppen. *Arbetsgruppen för systemsäkerhet* (SSWG) bör ha enstaka fasta mötestidpunkter, men i övrigt sammanträda då behov föreligger.

Arbetsgruppen för systemsäkerhet (SSWG) uppdaterar *Risklogg* (RL) baserat på information från myndigheter eller tillverkare, information om olyckor, tillbud eller avvikelserapporter samt *Systemsäkerhetsmeddelanden* (SSM) eller andra brukarerfarenheter. Arbetsgruppen föreslår säkerhetshöjande åtgärder såsom ändringar (modifieringar) eller informationskampanjer.

Om ett *Systemsäkerhetsmeddelande* (SSM) endast innebär att information för att förtydliga, upplysa eller påminna användaren om förhållanden med koppling till avsedd användning, förändrat användningssätt inklusive normglidning

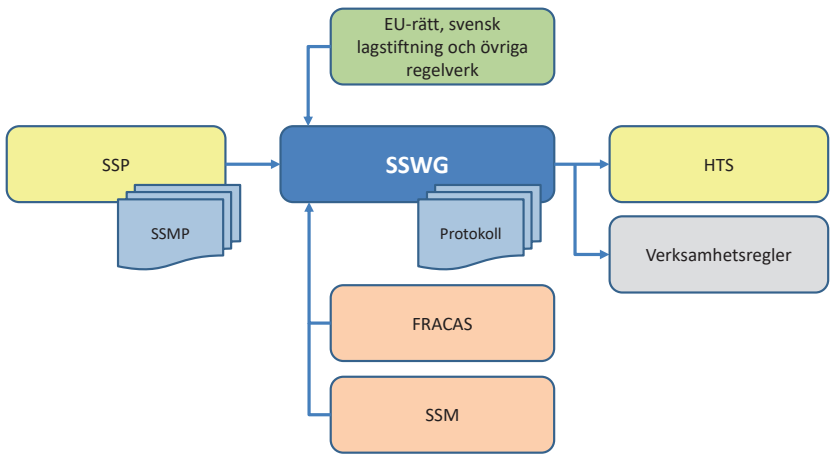
eller att verksamhetsregler behöver skärpas, kan ärendet stängas av ordförande i *Arbetsgrupp för systemsäkerhet* (SSWG), utan att nya systemsäkerhetsbeslut utfärdas.

Om ett *Systemsäkerhetsmeddelande* (SSM) återtas av utfärdaren och om säkerhetsbristen inte längre anses vara aktuell dokumenteras detta. Ärendet stängs av ordförande i *Arbetsgrupp för systemsäkerhet* (SSWG).

Indata, utdata och flödesbild

Indata till aktiviteten A*rbetsgrupp för systemsäkerhet* (SSWG) utgörs av *Systemsäkerhetsledningsplanen* (SSMP), lagstiftning samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS), S*ystemsäkerhetsmeddelanden* (SSM) och övriga brukarerfarenheter.

Utdata är protokoll eller mötesanteckningar. Dessa ger indata till *Riskhanteringssystemet* (HTS) samt ger underlag för revidering av verksamhetsregler.



Bilaga 3, bild 8 *Arbetsgrupp för systemsäkerhet (SSWG).*

TASK 105 – Integrated Product Team/Working Group Support (IPT/WG)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att vara ett mötesforum mellan *beställare* och *konstruktör,* dels för att följa upp utvecklingsarbetet av det tekniska systemet, dels följa upp att *konstruktören* följer *Systemsäkerhetsplanen* (SSPP). *Kravställaren* kan adjungeras till mötesforumet.

Den svenska benämningen är *Systemsäkerhetsgrupp* (IPT/WG) och utdata/dokumentation från systemsäkerhetsgenomgångar är protokoll eller mötesanteckningar.

I standarden MIL-STD-882E definieras två olika systemsäkerhetsrelaterade grupper, *Integrated Product Team* (IPT) respektive *Working Group* (WG). En *Working Group* (WG) har som främsta uppgift att behandla systemsäkerhetsaspekter. En *Integrated Product Team* (IPT) kan hantera ytterligare aspekter vid sidan om de som är systemsäkerhetsrelaterade. Grupperna kan tillsättas för ett enskilt projekt och dess uppgifter och befogenheter styrs av den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Parterna i S*ystemsäkerhetsgruppen* (IPT/WG) kan genomföra förberedande systemsäkerhetsgranskningar av det tekniska systemet inför projektets tekniska granskningar såsom *Preliminary Design Review* (PDR) och *Critical Design Review* (CDR).

Systemsäkerhetsgruppen (IPT/WG) hanterar följande systemsäkerhetsrelaterade delar:

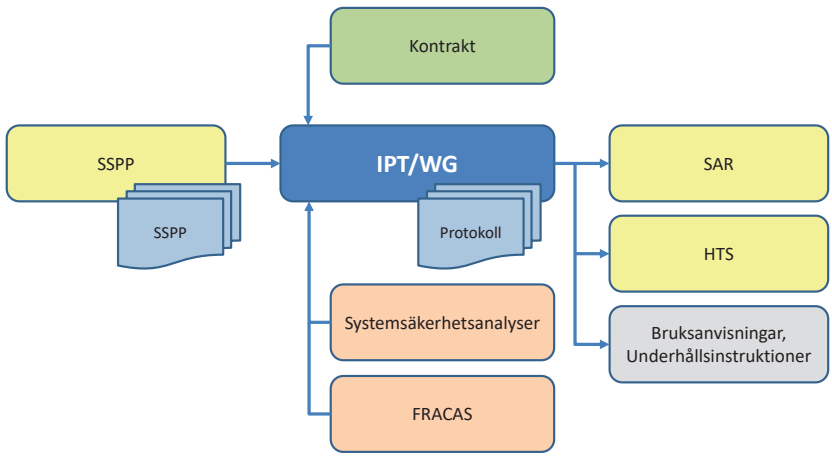
- Att inom ramen för kontraktet överenskomma *Systemsäkerhetsplan* (SSPP) inklusive uppdateringar
- Uppföljning av att systemsäkerhetsarbetet sker i enlighet med överenskommen *Systemsäkerhetsplan* (SSPP) samt om behov av revidering föreligger
- Genomgång av systemsäkerhetsrelaterade krav och kravverifiering
- Genomgång av *Riskloggen* (RL) över identifierade olycksrisker samt dess status avseende riskreduceringsarbetet
- Genomgång av övrig systemsäkerhetsdokumentation såsom *Systemsäkerhetsrapport* (SAR), listor och systemsäkerhetsvärdering

– Hantering av eventuella problem med åtgärder för riskreducering, vilka kan behöva beslutas av projektet

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsgruppen* (IPT/WG) utgörs av *Systemsäkerhetsplanen* (SSPP) och kontraktet samt resultat från systemsäkerhetsanalyser och data från *konstruktörens Felrapporteringssystem* (FRACAS).

Utdata är protokoll eller mötesanteckningar. Informationen från dessa infogas i *Systemsäkerhetsrapporten* (SAR) och *Riskloggen* (RL). Vidare kan informationen påverka innehållet i bruksanvisningar och underhållsinstruktioner.



Bilaga 3, bild 9 *Systemsäkerhetsgrupp (IPT/WG).*

TASK 106 – Hazard Tracking System (HTS)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att skapa en riskhanteringsprocess och genomföra löpande riskuppföljning samt ha sammanställd information och samlad lägesbild över alla identifierade olycksrisker för ett visst tekniskt system.

Den svenska benämningen är *Riskhanteringssystem* (HTS) och utdata/dokumentation är en *Risklogg* (RL). Den engelska benämningen på utdata/dokumentation är *Risk Log* (RL).

Information om genomförd och planerad olycksriskhantering samt status för de identifierade olycksriskerna sammanställs i en *Risklogg* (RL). I *Systemsäkerhetsrapporten* (SAR), eller i de underliggande systemsäkerhetsanalysrapporterna, finns de utförliga beskrivningarna av olycksriskerna samt resultatet av de genomförda systemsäkerhetsanalyserna. *Riskloggen* (RL) är ett komplement till *Systemsäkerhetsrapporten* (SAR) och innehåller också aktuell status kring det pågående riskreduceringsarbetet.

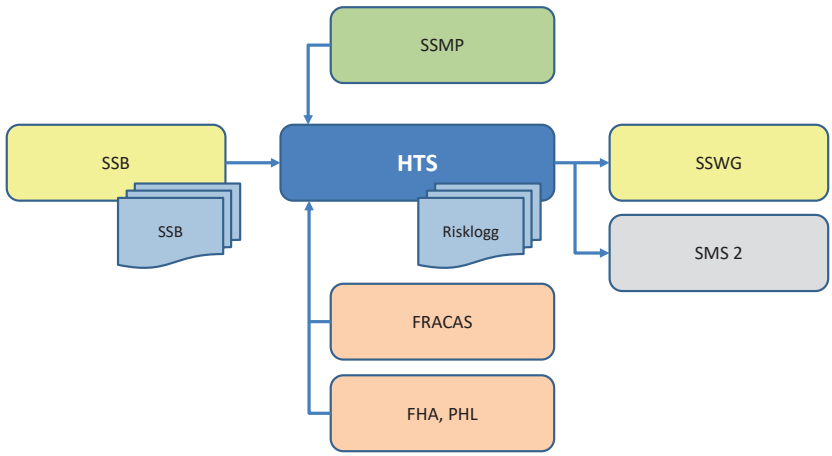
Kravställare, beställare och *konstruktör* kan ha sitt eget *Riskhanteringssystem* (HTS) och för löpande *Riskloggen* (RL) för olika tekniska system. I kontrakt mellan *beställare* och *konstruktör* finns de krav som gäller för *Riskhanteringssystem* (HTS) med tillhörande *Risklogg* (RL). Det kan vara en fördel om *Riskloggen* (RL) har samma uppställning och disposition oavsett vilken aktör som för tillfället ansvarar för dess innehåll. På så sätt kan *Riskloggen* (RL) upprätthållas för det tekniska systemet under hela dess livslängd.

Kravställaren listar de vanligast förekommande olycksriskerna i en *Risklogg* (RL) som *beställaren* behöver olycksriskhantera. *Beställaren* kan komplettera *Riskloggen* (RL) med ytterligare olycksrisker och denna bifogas *Förfrågningsunderlaget* (RFP). *Konstruktören* tillför därefter alla identifierade olycksrisker för det aktuella tekniska systemet. Vid leverans tar *beställaren* emot *konstruktörens Risklogg* (RL) för fortsatt olycksriskhantering. Efter genomförd olycksriskhantering överlämnas denna till *kravställaren* för avslutande olycksriskhantering. *Kravställaren* kan därmed tillse att *Arbetsgrupp för systemsäkerhet* (SSWG) får tillgång till *Riskloggen* (RL) i det fortsatta systemsäkerhetsarbetet under vidmakthållande- och avvecklingsskedet.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskhanteringssystem* (HTS) för *kravställaren* utgörs av *Systemsäkerhetsbedömning* (SSB) och *Systemsäkerhetsledningsplanen* (SSMP) samt data ur *Felrapporteringssystem* (FRACAS) och resultat från olika systemsäkerhetsanalyser.

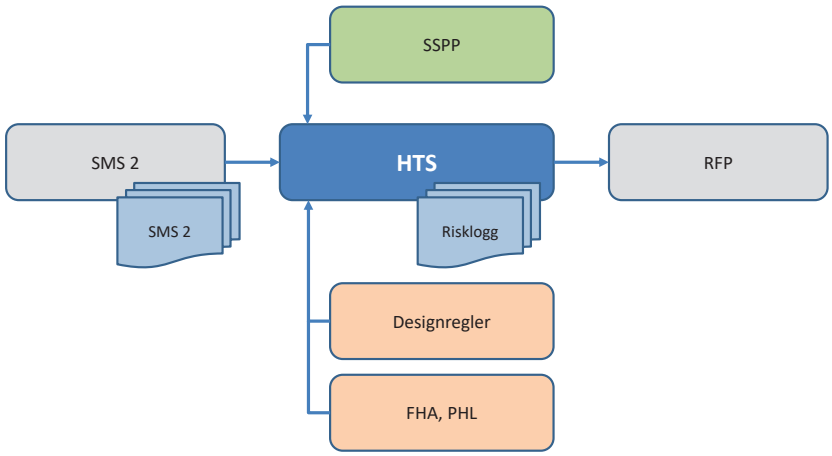
Utdata är *Riskloggen* (RL). Den ger indata till *Arbetsgrupp för systemsäkerhet* (SSWG) och *Systemmålsättning* (SMS 2).



Bilaga 3, bild 10 *Riskhanteringssystem (HTS) för kravställare.*

Indata till aktiviteten *Riskhanteringssystem* (HTS) för *beställaren* utgörs av *Systemmålsättning* (SMS 2) och *beställarens Systemsäkerhetsplan* (SSPP) samt *Designregler* (DR) och resultat från *Funktionell riskanalys* (FHA) och *Riskkällelista* (PHL).

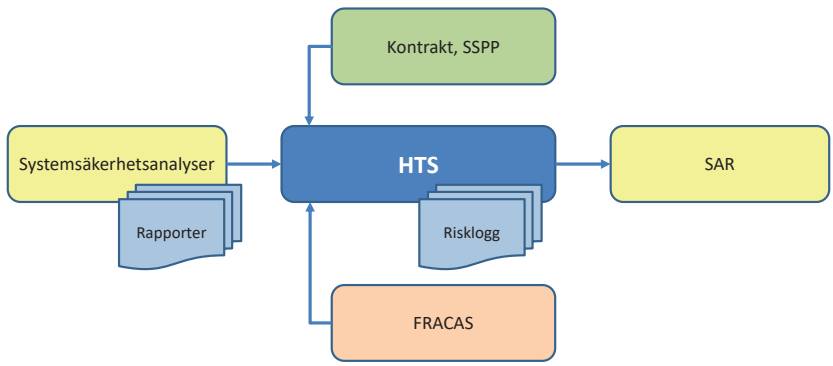
Utdata är *Riskloggen* (RL). Den ger indata till *Förfrågningsunderlaget* (RFP).



Bilaga 3, bild 11 *Riskhanteringssystem (HTS) för beställare.*

Indata till aktiviteten *Riskhanteringssystem* (HTS) för *konstruktören* utgörs av olika systemsäkerhetsanalyser och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt data ur *Felrapporteringssystem* (FRACAS).

Utdata är *Riskloggen* (RL). Den ger indata till *Systemsäkerhetsrapporten* (SAR).



Bilaga 3, bild 12 *Riskhanteringssystem (HTS) för konstruktör.*

Riskloggen (RL) bör innehålla följande information:

- Vilket tekniskt system eller produkt som avses
- Riskidentifiering (risknummer och olycksrisk samt vid behov standardscenarion, vådahändelser, farliga tillstånd mm)
- Vilka vägval som tillämpats
- Riskvärdering före riskreducerande åtgärder
- Riskreducerande åtgärder med angivande av verifierings- och valideringsmetod
- Riskvärdering efter riskreducerande åtgärder
- Riskreducering efter tillämpning av exponerings- och styrbarhetsfaktorer
- Diarienummer på protokoll eller mötesanteckning för fattade beslut
- Acceptansbeslut (åtgärder införda respektive verifierade)
- Status på riskreduceringsarbetet för enskilda olycksrisker
- Olycksrisker som avförts efter riskreducerande åtgärder
- Anmärkningar

TASK 107 – Hazard Management Progress Report (HMPR)

Denna aktivitet ingår i Integrated Product Team / Working Group (IPT/WG).

TASK 108 – Hazardous Materials Management Plan (HMMP)

Denna aktivitet ingår i TASK 102 - System Safety Program Plan (SSPP).

Aktiviteter – SEKTION 200 – Analyser

TASK 208 – Functional Hazard Analysis (FHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är dels att klassificera systemfunktioner ur kritikalitetssynpunkt för kravställning, dels identifiera och värdera funktionellt relaterade olycksrisker för enskilda tekniska system och produkter eller för system-av-system.

Den svenska benämningen är *Funktionell riskanalys* (FHA) och utdata/dokumentation är en *Funktionell riskanalys* (FHA). Den engelska benämningen på utdata/dokumentation är *Functional Hazard Analysis* (FHA).

Den *Funktionella riskanalysen* (FHA) kan dels baseras på framtagen systemarkitektur, dels på erfarenhetsdata ur *Felrapporteringssystem* (FRACAS). De identifierade systemfunktionerna analyseras avseende indata, utdata och interaktioner med andra delsystem, i syfte att fördela de potentiella felfunktionerna till de berörda delsystemen samt som underlag för klassificering av säkerhetskritiska funktioner enligt *Säkerhetskritiska funktioner* (SCF). För kravställning identifieras principiella konstruktionsinriktade åtgärder för att eliminera eller reducera olycksriskerna för det tekniska systemet. För de funktionellt relaterade olycksriskerna som infogas i *Riskloggen* (RL) bedöms i första hand konsekvenserna av dessa felfunktioner.

Vid utarbetandet av en säkerhetsarkitektur kan kritiska systemfunktioner fördelas mellan eller inom tekniska system. Kritiska systemfunktioner kan delas upp mellan funktionella eller fysiska komponenter såsom maskinvara, elektronik eller programvara, men kan även påverka användargränssnitt utifrån användbarhet. Den *Funktionella riskanalysen* (FHA) identifierar säkerhetskritiska programvaror för vidare hantering enligt Handbok för Programvara i säkerhetskritiska tillämpningar (H ProgSäk).

Kravställaren identifierar funktionella olycksrisker med dess dimensionerande konsekvenser och för in dessa i *Riskloggen* (RL). Resultatet är indata till *Systemsäkerhetsbedömningen* (SSB).

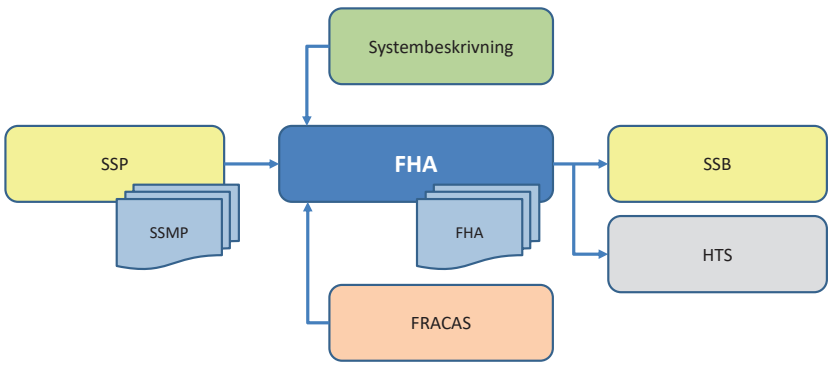
Beställarens identifierar funktionella olycksrisker med dess dimensionerande konsekvenser och för in dessa i *Riskloggen* (RL). Resultatet är indata till *Systemsäkerhetskrav* (SSK).

Konstruktören använder resultatet av den *Funktionella riskanalysen* (FHA) dels för att identifiera tekniska systemsäkerhetskrav som del av *Systemsäkerhetskravanalysen* (SRHA), dels som indata till de fördjupade systemsäkerhetsanalyserna.

Indata, utdata och flödesbild

Indata till aktiviteten *Funktionell riskanalys* (FHA) för *kravställaren* utgörs av *Systemsäkerhetsledningsplanen* (SSMP) och systembeskrivningen samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

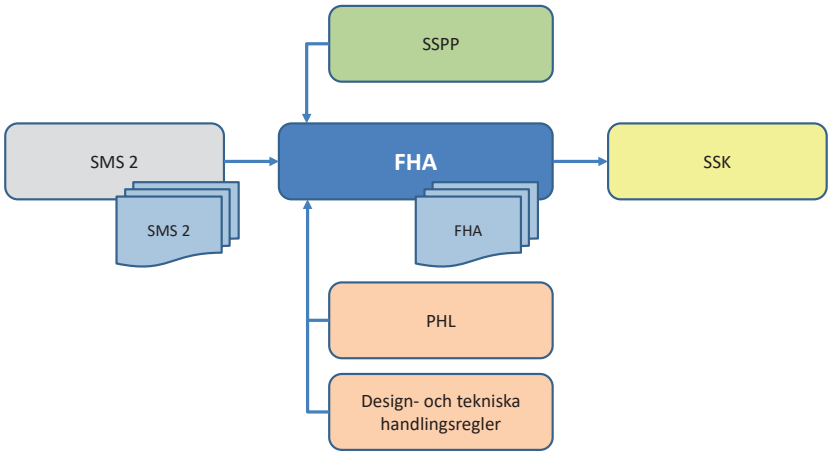
Utdata är *Funktionell riskanalys* (FHA). Den är indata till *Systemsäkerhetsbedömning* (SSB) och *Risklogg* (RL).



Bilaga 3, bild 13 *Funktionell riskanalys (FHA) för kravställare.*

Indata till aktiviteten *Funktionell riskanalys* (FHA) för *beställaren* utgörs av *Systemmålsättning* (SMS 2) och *beställarens Systemsäkerhetsplan* (SSPP) samt *Riskkällelista* (PHL), *Designregler* (DR) och *Tekniska handlingsregler* (THR).

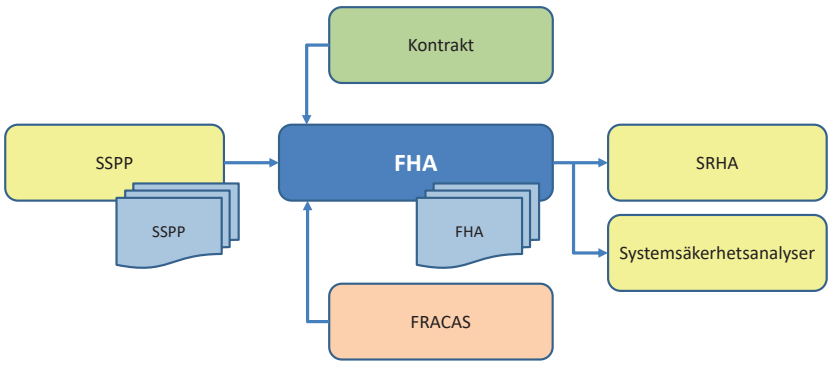
Utdata är *Funktionell riskanalys* (FHA). Den är indata till *Systemsäkerhetskrav* (SSK).



Bilaga 3, bild 14 *Funktionell riskanalys (FHA) för beställare.*

Indata till aktiviteten *Funktionell riskanalys* (FHA) för *konstruktören* utgörs av den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) och systembeskrivningen i kontrakt samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

Utdata är *Funktionell riskanalys* (FHA). Den är indata till *Systemsäkerhetskrav-analysen* (SRHA) samt till övriga systemsäkerhetsanalyser.



Bilaga 3, bild 15 *Funktionell riskanalys (FHA) för konstruktör.*

En *Funktionell riskanalys* (FHA) bör innehålla:

- En övergripande systembeskrivning avseende delsystemen inklusive möjliga programvaror samt dess huvudsakliga interaktioner, exempelvis i blockschema
- En lista över systemfunktioner respektive systemsäkerhetskritiska funktioner
- En beskrivning av vilka säkerhetskritiska funktioner som kan realiseras genom programvara inklusive förslag till kritikalitetsnivå
- Indata till *Risklogg* (RL) i form av olycksrisker med konsekvensklassning
- En lista över identifierade systemsäkerhetskrav

TASK 201 – Preliminary Hazard List (PHL)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera riskkällor och/eller riskfyllda situationer, vilka kan vara fysikaliska eller funktionella egenskaper, som finns i eller är sammankopplade med det tekniska systemet eller produkten.

Den svenska benämningen är *Riskkällelista* (PHL) och utdata/dokumentation är en *Riskkällelista (*PHL). Den engelska benämningen på utdata/dokumentation är *Preliminary Hazard List* (PHL).

Riskkällelista (PHL) kan användas som indata dels vid kravställning, dels till de fördjupade systemsäkerhetsanalyserna, dels till *Riskhanteringssystemet* (HTS).

Riskkällelista (PHL) är en lista över de riskkällor och/eller riskfyllda situationer som för närvarande finns i eller är sammankopplade med det tekniska systemet, vilket innebär att innehållet i listan kan behöva uppdateras intill dess att konfigurationen är fastställd.

Kravställaren identifierar dimensionerande riskkällor och/eller riskfyllda situationer som kan motverkas genom att ställa systemsäkerhetskrav i *Systemmålsättning* (SMS 2). Detta innebär i princip att vissa konstruktionslösningar inte tillåts, medan andra medges.

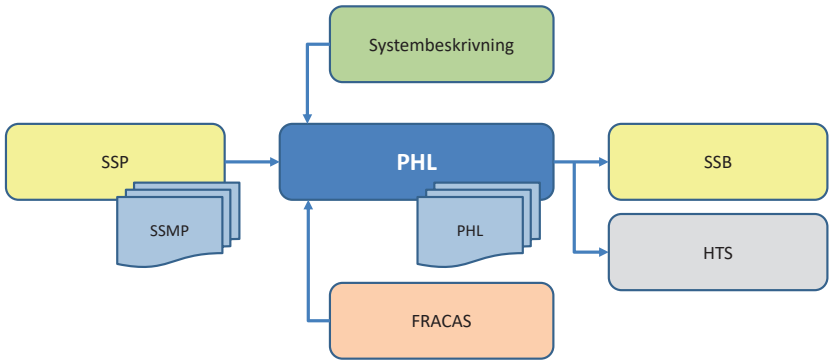
Beställaren identifierar möjliga riskkällor och/eller riskfyllda situationer som kan motverkas genom att ställa systemsäkerhetskrav i *Förfrågningsunderlaget* (RFP). Detta innebär i princip att krav på vissa principiella konstruktionslösningar ställs. Exempelvis att det ska finnas (minst) två av varandra oberoende säkringar eller skyddsanordningar.

Konstruktören identifierar samtliga riskkällor och/eller riskfyllda situationer som finns i eller är sammankopplade med det tekniska systemet eller produkten. Resultatet används dels i *Systemsäkerhetskravanalysen* (SRHA), dels som indata till de fördjupade systemsäkerhetsanalyserna.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskkällelista* (PHL) för *kravställaren* utgörs av *Systemsäkerhetsledningsplanen* (SSMP) och systembeskrivningen samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

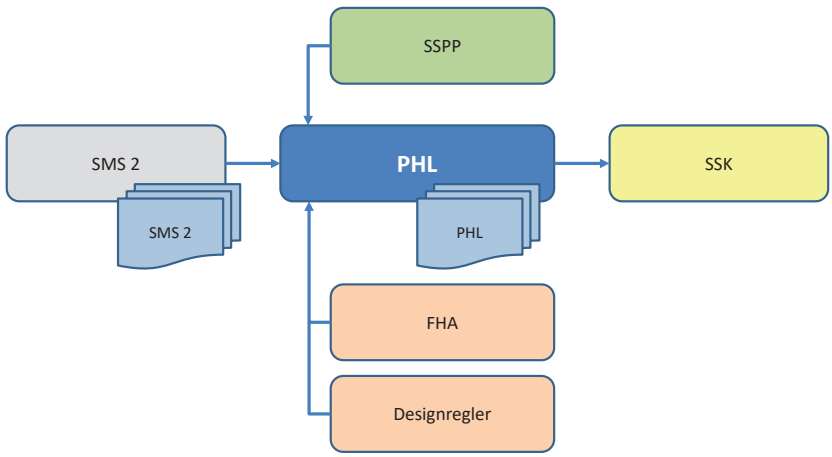
Utdata är *Riskkällelista* (PHL). Den är indata till *Systemsäkerhetsbedömningen* (SSB) och *Riskhanteringssystemet* (HTS).



Bilaga 3, bild 16 *Riskkällelista (PHL) för kravställare.*

Indata till aktiviteten *Riskkällelista* (PHL) för *beställaren* utgörs av *Systemmålsättning* (SMS 2) och *beställarens Systemsäkerhetsplan* (SSPP) samt den *Funktionella riskanalysen* (FHA) och erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

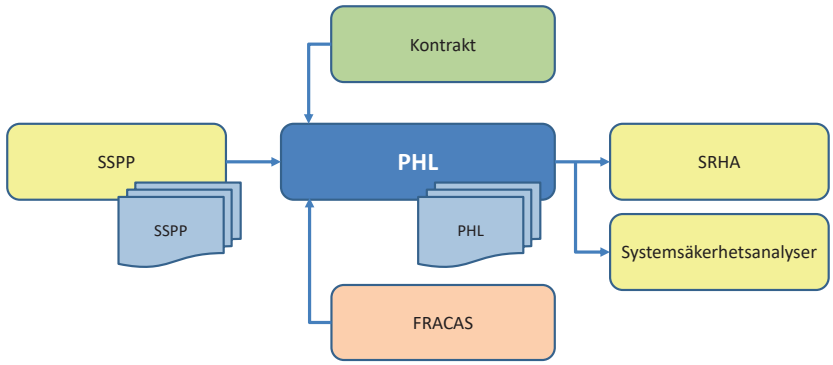
Utdata är *Riskkällelista* (PHL). Den är indata till *Systemsäkerhetskrav* (SSK).



Bilaga 3, bild 17 *Riskkällelista (PHL) för beställare.*

Indata till aktiviteten *Riskkällelista* (PHL) för *konstruktören* utgörs av den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) och kontrakt samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

Utdata är *Riskkällelista* (PHL). Den är indata till *Systemsäkerhetskravanalysen* (SRHA) och övriga systemsäkerhetsanalyser.



Bilaga 3, bild 18 *Riskkällelista (PHL) för konstruktör.*

En *Riskkällelista* (PHL) kan innehålla olika mycket information beroende på aktörens syfte med listan.

En *Riskkällelista* (PHL) bör innehålla:

- Referens till en beskrivning av konceptet eller det tekniska systemet
- En lista över komponenter med dess riskkällor och/eller riskfyllda situationer samt vid behov:
  - Vådahändelser och/eller olycksrisker med skattade konsekvenser om olyckan inträffar
  - Enkel prioritering mellan riskkällorna och de riskfyllda situationerna inför de fördjupade systemsäkerhetsanalyserna.

TASK 202 – Preliminary Hazard Analysis (PHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera vådahändelser och olycksrisker, relaterade till konstruktion eller funktion, som finns i eller är sammankopplade med det tekniska systemet eller produkten, utifrån de identifierade riskkällorna i *Riskkällelista* (PHL). Aktiviteten omfattar även en första analys och värdering av de identifierade olycksriskerna samt ger möjlighet att föreslå tänkbara riskreducerande åtgärder.

Den svenska benämningen är *Riskkälleanalys* (PHA) och utdata/dokumentation är en *Riskkälleanalys* (PHA). Den engelska benämningen på utdata/dokumentation är *Preliminary Hazard Analysi*s (PHA).

Riskkälleanalysen (PHA) tar vid där *Riskkällelistan* (PHL) avslutades.

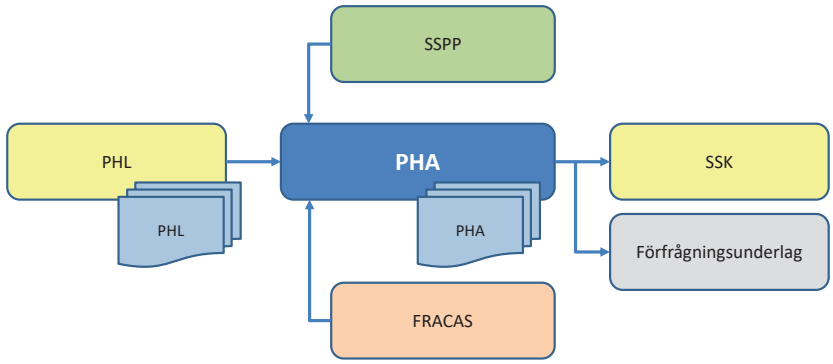
Riskkälleanalysen (PHA) är en inledande analys och värdering av olycksrisker där detaljeringen sker i de fördjupade systemsäkerhetsanalyserna. *Riskkälleanalysen* (PHA) behöver analysera användning, underhåll, förrådshållning (transport) samt avveckling. Vidare behöver gränsytor och samverkan med andra tekniska system och produkter beaktas. Resultatet kan även användas vid formulering av systemsäkerhetskrav.

Riskkälleanalysen (PHA) kan även användas för att identifiera och beteckna delsystem och komponenter ur kritikalitetssynpunkt. De betecknade delsystemen eller komponenterna utreds vidare i aktiviteten S*äkerhetskritiska funktioner* (SCF).

Indata, utdata och flödesbild

Indata till aktiviteten *Riskkälleanalys* (PHA) för *beställaren* utgörs av *Riskkällelista (*PHL) och *beställarens Systemsäkerhetsplan* (SSPP) samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

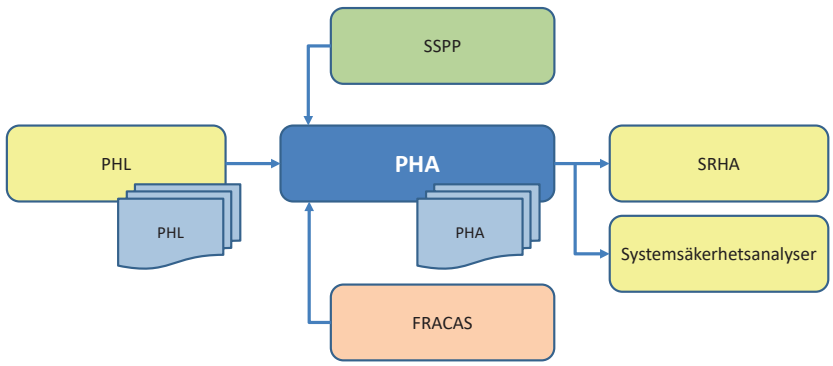
Utdata är *Riskkälleanalys* (PHA). Den är indata till *Systemsäkerhetskrav* (SSK) och *Förfrågningsunderlag* (RFP).



Bilaga 3, bild 19 *Riskkälleanalys (PHA) för beställaren.*

Indata till aktiviteten *Riskkälleanalys* (PHA) för *konstruktören* utgörs av *Riskkällelist*a (PHL) och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

Utdata är *Riskkälleanalys* (PHA). Den är indata till *Systemsäkerhetskravanalysen* samt övriga fördjupade systemsäkerhetsanalyser.



Bilaga 3, bild 20 *Riskkälleanalys (PHA) för konstruktören.*

En *Riskkälleanalys* (PHA) utgår från *Riskkällelistan* (PHL) och den kan dessutom kompletteras med beskrivande text om respektive olycksrisk.

En *Riskkälleanalys* (PHA) bör innehålla:

- Referens till en beskrivning av konceptet eller det tekniska systemet
- Identifierade vådahändelser och olycksrisker samt en första inledande bedömning av sannolikheter och skadeklasser, inklusive hälso- och miljöpåverkan
- En lista över identifierade säkerhetskritiska delsystem och komponenter
- Förslag till riskreducerande åtgärder för att motverka identifierade vådahändelser och olycksrisker
- En beskrivning av respektive olycksrisk

S21 – Säkerhetskritiska funktioner (SCF)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera systemsäkerhetskritiska funktioner, delsystem eller komponenter som finns i eller är sammankopplade med det tekniska systemet eller produkten. Resultatet av aktiviteten visar vilka egenskaper hos delsystem eller komponenter som under utveckling och tillverkning kräver särskilda åtgärder eller kvalitetskontroller. Motsvarande gäller även för programvaror som ingår i det tekniska systemet.

Den engelska benämningen är S*afety Critical Functions* (SCF) och utdata/dokumentation är en *Safety Critical Functions* (SCF). Den svenska benämningen på utdata/dokumentation är *Säkerhetskritiska funktioner* (SCF).

I styrdokumentation för utveckling och tillverkning av tekniska system eller produkter behöver *konstruktören* upprätta, dokumentera och vidmakthålla beskrivningar av utvecklings- och tillverkningsprocesser samt arbetsinstruktioner för de produktionsoperationer som krävs för de egenskaper som kan betecknas som kritiska ur systemsäkerhetssynpunkt. Genom att ange kritikalitetsklassning i utvecklings- och produktbeskrivande dokument skapas förutsättningar för att använda anpassad metodik, styra resurserna vid utveckling och tillverkning samt genomföra särskilda kvalitetskontroller alternativt verifiering av programvara.

Säkerhetskritiska och säkerhetsrelaterade delsystem och komponenter kan ha särskilda egenskaper såsom specifika funktioner, mått, vissa toleranser, hårdhet eller ytfinhet. I de fallen brister finns i sådana egenskaper kan vådahändelser eller olyckor inträffa. Det gäller exempelvis om komponenter saknas i en installation.

För delsystem som innehåller programvara anges krav på kritikalitetsnivå i de fallen där brister bedöms kunna förorsaka vådahändelser eller olyckor.

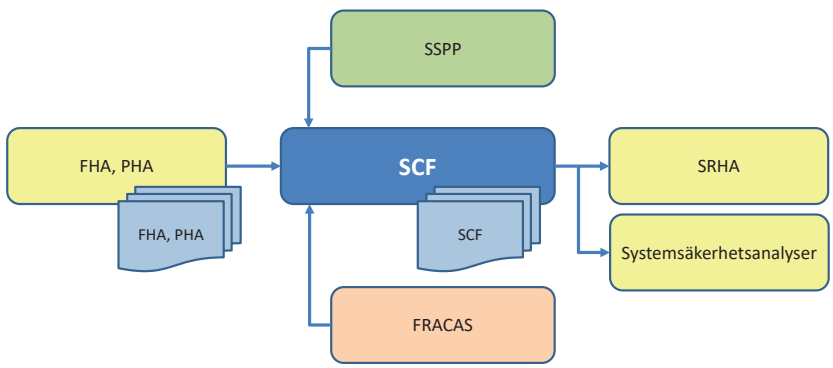
De säkerhetskritiska delsystemen/komponenterna med dess egenskaper är de som direkt påverkar systemsäkerheten hos det tekniska systemet, exempelvis medger enkelfel. De säkerhetsrelaterade delsystemen/komponenterna med dess egenskaper är de som indirekt påverkar systemsäkerheten hos det tekniska systemet, exempelvis där det krävs dubbelfel eller fel av högre ordning.

Om det i delsystem eller komponenter finns brister i dess egenskaper och om dessa egenskaper bedöms ha en signifikant inverkan på vådahändelsen behöver komponenterna markeras på ritningar eller i annat konstruktionsunderlag. För maskinvara eller maskininriktade komponenter betecknas de kritiska egenskaper (*Critcal Item List* (CIL)) exempelvis enligt SS 2222 *Teknisk dokumentation - Klassificering av fordringar i produktionsunderlage*t. För programvara med tillhörande elektronik kan kritikalitetsklassificeringen utföras enligt metodiken i Handbok för Programvara i säkerhetskritiska tillämpningar (H ProgSäk).

Indata, utdata och flödesbild

Indata till aktiviteten *Säkerhetskritiska funktioner* (SCF) utgörs av *Funktionell riskanalys* (FHA), *Riskkälleanalys* (PHA) och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS).

Utdata är *Säkerhetskritiska funktioner* (SCF), vilken dels kan vara en lista över kritiska egenskaper/delar (*Critical Item List* (CIL)), dels en lista över kritikalitets- eller tillförlitlighetsnivåer (*Safety Integrity Level* (SIL)), vilka används för vidare kravställning.



Bilaga 3, bild 21 Säkerhetskritiska funktioner (SCF).

Säkerhetskritiska funktioner (SCF) bör innehålla:

- Referenser till standarder för kritikalitetsklassificering som tillämpats för
  - Maskinvara
  - Programvara

TASK 203 – System Requirements Hazard Analysis (SRHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att *konstruktören* ska identifiera de systemsäkerhetskrav som är tillämpliga för det tekniska systemet utifrån EU-rätt, svensk lagstiftning, standarder, *beställarens* krav i kontraktet samt företagsinterna systemsäkerhetskrav.

Den svenska benämningen är *Systemsäkerhetskravanaly*s (SRHA) och utdata/dokumentation är en *Systemsäkerhetskravanalysrapport* (SRHAR). Den engelska benämningen på utdata/dokumentation är *System Requirements Hazard Analysis* (SRHA).

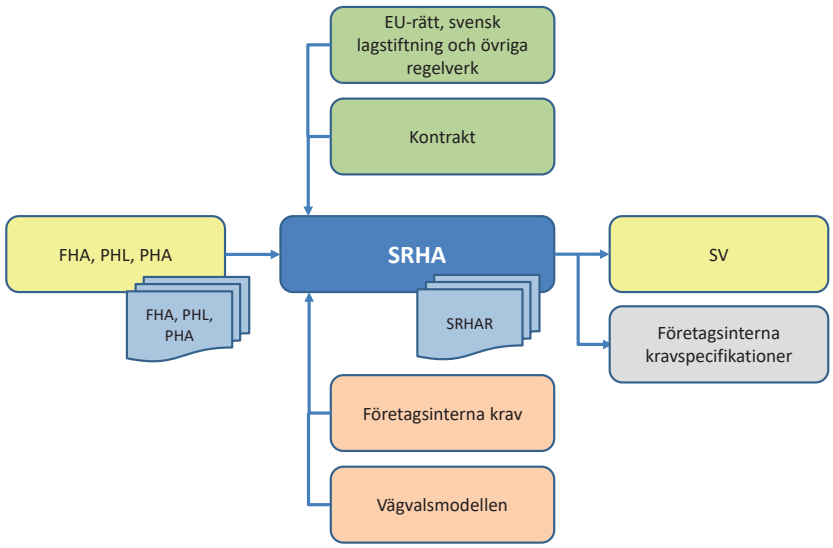
Konstruktören utarbetar systemsäkerhetskrav i syfte att identifiera riskreducerande åtgärder för att motverka de olycksrisker som identifierades i *Funktionell riskanalys* (FHA), *Riskkällelista* (PHL) och *Riskkälleanaly*s (PHA).

Identifierade systemsäkerhetskrav i *Systemsäkerhetskravanalysrapporten* (SRHAR) utgörs dels av tekniska krav som påverkar konstruktionen, dels av krav på systemsäkerhetsarbete för att visa att det tekniska systemet erbjuder betryggande säkerhet. Alla krav överförs och fördelas till *konstruktörens* olika kravspecifikationer. Varje krav behöver vara verifierbart för att senare tas om hand i aktiviteten *Systemsäkerhetsverifiering* (SV). Som stöd för denna aktivitet tillämpas *Vägvalsmodellen* (VVM).

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetskravanalys* (SRHA) utgörs av *Funktionell riskanalys* (FHA), *Riskkällelista* (PHL) och *Riskkälleanalys* (PHA) samt lagstiftning och kontrakt. Även företagsinterna krav på konstruktion eller utvecklingsarbetet beaktas.

Utdata är *Systemsäkerhetskravanalysrapport* (SRHAR). Den är indata till *Systemsäkerhetsverifieringen* (SV) och till *konstruktörens* interna kravspecifikationer.



Bilaga 3, bild 22 Systemsäkerhetskravanalys (SRHA).

En *Systemsäkerhetskravanalysrapport* (SRHAR) bör innehålla:

- Vilket tekniskt system som avses
- Kravnummer (löpnummer)
- Källhänvisning (titel/dokument)
  - EU-rätt, svensk lagstiftning, standarder, teknisk specifikation, handböcker (designregelsamlingar) samt systemsäkerhetsanalyser
- Kravtext (exempelvis krav ur teknisk specifikation och handböcker (designregelsamlingar))
- Eventuella undantag från lagstiftning för militär materiel
- Verifieringskriterium
- Markering att kravet är uppfyllt

TASK 204 – Subsystem Hazard Analysis (SSHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att främst påverka konstruktion och funktion av delsystem och komponenter som ingår i ett tekniskt system för att uppnå betryggande säkerhet under användning. Som stöd för denna aktivitet tillämpas *Vägvalsmodellen* (VVM).

Den svenska benämningen är *Riskanalys för delsystem* (SSHA) och utdata/dokumentation är en *Riskanalysrapport för delsystem* (SSHAR). Den engelska benämningen på utdata/dokumentation är *Subsystem Hazard Analysis* (SSHA).

Resultatet av *Riskanalys för delsystem* (SSHA) fokuserar huvudsakligen på konstruktion och funktion, med eventuella programvaror, så att betryggande säkerhet erbjuds under användning, underhåll, förrådshållning (transport) samt avveckling.

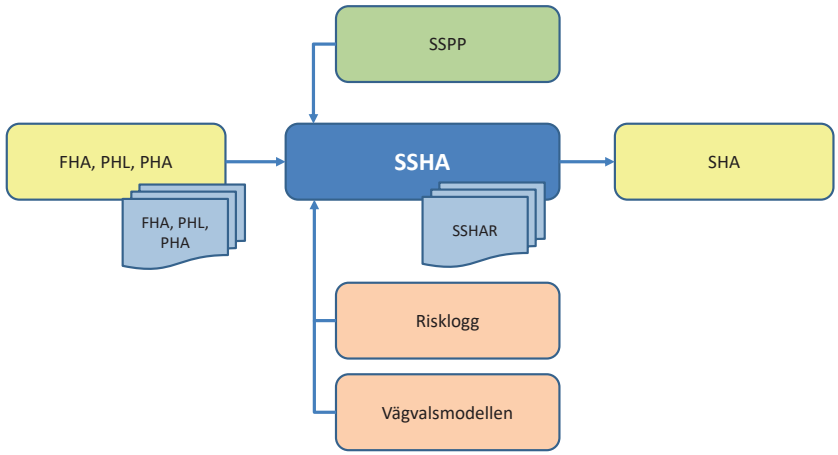
För de olycksrisker som dels identifierades i *Funktionell riskanalys* (FHA), *Riskkällelista* (PHL) och *Riskkälleanalys* (PHA), dels eventuellt tillkommande olycksrisker under *Riskanalys för delsystem* (SSHA), så ska dessa analyseras, värderas och klassificeras samt vid behov ska riskreducerande åtgärder införas. Som stöd för denna aktivitet används *Risklogg* (RL).

I *Riskloggen* (RL) kan både olycksrisker, delsystemet och systemsäkerhetskritiska komponenter listas. Genom att tillämpa *Vägvalsmodellen* (VVM) kan dels olycksrisker, dels delsystemet, dels systemsäkerhetskritiska komponenter omhändertas genom olika vägval. Se kapitel 11. Endast de olycksrisker som inte har kunnat omhändertas i vägval (VV1–VV6) ska hanteras i vägval (VV7) och bedömas mot *Tolerabel risknivå* (TR) uttryckt i riskmatris.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskanalys för delsystem* (SSHA) utgörs av *Funktionell riskanalys* (FHA), *Riskkällelista* (PHL) och *Riskkälleanalys* (PHA) samt den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Utdata är *Riskanalysrapport för delsystem* (SSHAR). Den är indata till *Riskanalys för system* (SHA).



Bilaga 3, bild 23 *Riskanalys för delsystem (SSHA).*

En *Riskanalysrapport för delsystem* (SSHAR) bör innehålla:

- En övergripande systembeskrivning samt detaljerad fysisk och funktionell beskrivning av delsystemen
- Vilka krav på systemnivån som har brutits ner till respektive delsystem
- Beskrivning av vilka riskanalysmetoder som använts
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Sammanfattning av resultatet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till framtida systemsäkerhetsprovning
- Detaljerad redovisning som ligger till grund för sammanfattningen
- Data som överförs till *Risklogg* (RL)

TASK 205 – System Hazard Analysis (SHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att främst påverka konstruktion och funktion av tekniska system och produkter för att uppnå betryggande säkerhet under användning. Tekniska system och produkter kan i sin tur ingå ett system-av-system. Som stöd för denna aktivitet tillämpas V*ägvalsmodellen* (VVM).

Den svenska benämningen är *Riskanalys för system* (SHA) och utdata/dokumentation är en *Riskanalysrapport för system* (SHAR). Den engelska benämningen på utdata/dokumentation är *System Hazard Analysis* (SSHA).

Resultatet av *Riskanalys för system* (SHA) fokuserar huvudsakligen på konstruktion och funktion, med eventuella programvaror, inom och mellan olika delsystem och produkter så att betryggande säkerhet erbjuds under användning, underhåll, förrådshållning (transport) samt avveckling. Olika delsystem och produkter kan ha godkänts eller uppfyllt krav mot olika regelverk eller standarder. Detta behöver beaktas i systemsäkerhetsarbetet för det tekniska systemet.

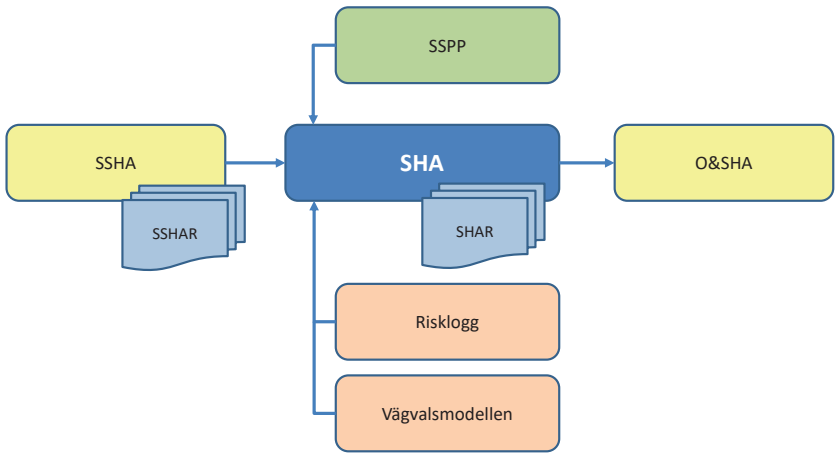
För de olycksrisker som dels identifierades i *Funktionell riskanalys* (FHA), *Riskkällelista* (PHL), *Riskkälleanalys* (PHA) och *Riskanalys för delsystem* (SSHA), dels eventuellt tillkommande olycksrisker under *Riskanalys för system* (SHA), så ska dessa analyseras, värderas och klassificeras samt vid behov ska riskreducerande åtgärder införas. Som stöd för denna aktivitet används *Risklogg* (RL).

I *Riskloggen* (RL) kan både olycksrisker, det tekniska systemet, delsystem och systemsäkerhetskritiska komponenter listas. Genom att tillämpa *Vägvalsmodellen* (VVM) kan dels olycksrisker, dels det tekniska systemet, dels delsystem och systemsäkerhetskritiska komponenter omhändertas genom olika vägval. Se kapitel 11. Endast de olycksrisker som inte har kunnat omhändertas i vägval (VV1–VV6) ska hanteras i vägval (VV7) och bedömas mot *Tolerabel risknivå* (TR) uttryckt i riskmatris.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskanalys för system* (SHA) utgörs av *Riskanalys för delsystem* (SSHA) samt den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Utdata är *Riskanalysrapport för system* (SHAR). Den är indata till *Riskanalys för hantering* (O&SHA).



Bilaga 3, bild 24 Riskanalys för system (SHA).

En *Riskanalysrapport för system* (SHAR) bör innehålla:

- En detaljerad fysisk och funktionell systembeskrivning samt övergripande beskrivningar av delsystemen
- Vilka krav på systemnivån finns
- Beskrivning av vilka riskanalysmetoder som använts
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Sammanfattning av resultatet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till framtida systemsäkerhetsprovning
- Detaljerad redovisning som ligger till grund för sammanfattningen
- Data som överförs till *Risklogg* (RL).

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

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att främst påverka hanteringen av tekniska system och produkter med en fastställd konfiguration för att uppnå betryggande säkerhet.

Den svenska benämningen är *Riskanalys för hantering* (O&SHA) och utdata/dokumentation är en *Riskanalysrapport för hantering* (O&SHAR). Den engelska benämningen på utdata/dokumentation är *Operating and Support Hazard Analysis* (O&SHA).

Resultatet av *Riskanalys för hantering* (O&SHA) fokuserar huvudsakligen på hanteringen av tekniska system och produkter så att betryggande säkerhet erbjuds under användning, underhåll samt förrådshållning (transport). Således behöver scenarion som beskriver olika användningsmiljöer och användningssätt definieras samt om annan materiel eller kemiska produkter behöver användas, exempelvis ett visst verktyg eller rengöringsmedel vid underhåll.

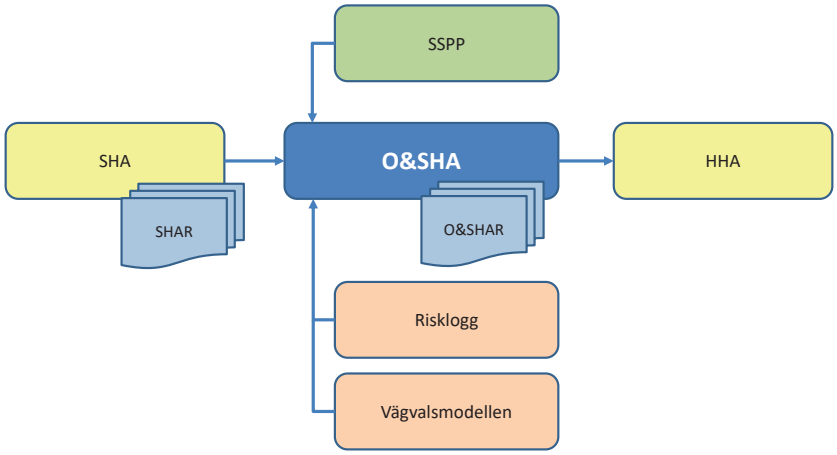
För de olycksrisker som dels identifierades i *Riskanalys för system* (SHA), dels eventuellt tillkommande olycksrisker under *Riskanalys för hantering* (O&SHA), så ska dessa analyseras, värderas och klassificeras samt vid behov ska verksamhetsregler ändras eller restriktioner införas. För vissa olycksrisker kan förslag lämnas på ändring (modifiering) av det tekniska systemet. Som stöd för denna aktivitet används *Risklogg* (RL).

I *Riskloggen* (RL) kan både olycksrisker och arbetsmiljörisker listas. Genom att tillämpa *Vägvalsmodellen* (VVM) kan dels olycksrisker, dels arbetsmiljörisker omhändertas genom olika vägval. Se kapitel 11. Endast de olycksrisker som inte har kunnat omhändertas i vägval (VV1–VV6) ska hanteras i vägval (VV7) och bedömas mot *Tolerabel risknivå* (TR) uttryckt i riskmatris.

Indata, utdata, och flödesbild

Indata till aktiviteten *Riskanalys för hantering* (O&SHA) utgörs av *Riskanalys för system* (SHA) samt den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Utdata är *Riskanalys för hantering* (O&SHA). Den ger indata till den *Hälsorelaterade riskanalysen* (HHA).



Bilaga 3, bild 25 *Riskanalys för hantering (O&SHA).*

En *Riskanalysrapport för hantering* (O&SHAR) bör innehålla:

- En detaljerad fysisk och funktionell systembeskrivning samt övergripande beskrivningar av delsystemen
- En beskrivning av användningsscenariorna
- Vilka krav på systemnivån finns
- Beskrivning av vilka riskanalysmetoder som använts
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Sammanfattning av resultatet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till framtida utbildning
- Detaljerad redovisning som ligger till grund för sammanfattningen
  - Beskrivning av förslag till ändringar av det tekniska systemet eller delsystemen
  - Rekommendationer om instruktioner, varselmärkningar, nödutrustning och personlig skyddsutrustning (PPE)
  - Rekommendationer för transport- och förvaringsregler
- Data som överförs till *Risklogg* (RL)

TASK 209 – System-of-Systems Hazard Analysis (SoSHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att säkerställa samfunktion mellan två eller flera tekniska system och produkter, med avsikt att möjliggöra nya förmågor eller funktioner, så att betryggande säkerhet uppnås under användning. För ingående tekniska system och produkter finns systemsäkerhetsbeslut utfärdade. Aktiviteten genomförs genomförs främst av *systemintegratören*.

Den svenska benämningen är *Riskanalys för system-av-syste*m (SoSHA) och utdata/dokumentation är en *Riskanalysrapport för system-av-system* (SoSHAR). Den engelska benämningen på utdata/dokumentation är *System-of-Systems Hazard Analysis* (SoSHA).

Resultatet av *Riskanalys för system-av-system* (SoSHA) fokuserar huvudsakligen på att få en säker samfunktion mellan olika tekniska system och produkter, utan att de fastställda konfigurationerna ändras. Vid behov kan olika anslutningsdon för sammankoppling eller adaptrar för gränsytor tillåtas. Detta så att betryggande säkerhet erbjuds under användning. I de fallen tekniska system eller produkter behöver modifieras så sker detta av en *konstruktör*.

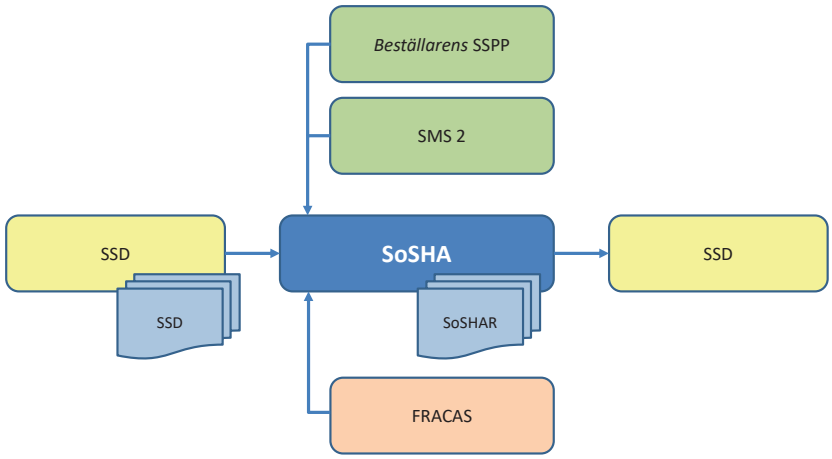
För de olycksrisker som identifieras för system-av-system så ska dessa analyseras, värderas och klassificeras samt vid behov ska riskreducerande åtgärder införas. Som stöd för denna aktivitet används *Funktionell riskanalys* (FHA), *Riskkällelista* (PHL), fördjupade systemsäkerhetsanalyser samt *Risklogg* (RL).

Riskanalys för system-av-system (SoSHA) behöver även utreda om andra olycksrisker på de ingående tekniska systemen eller produkterna påverkas och därmed behöver omvärderas, vilket även kan leda till att nya systemsäkerhetsbeslut behöver utfärdas.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskanalys för system-av-system* (SoSHA) utgörs av *Systemsäkerhetsdeklarationer* (SSD), *Systemmålsättning* (SMS 2) och *beställarens Systemsäkerhetsplan* (SSPP) samt erfarenheter ur *Felrapporteringssystem* (FRACAS).

Utdata är *Riskanalysrapport för system-av-system* (SoSHAR). Den ger indata till *Systemsäkerhetsdeklaration* (SSD) för system-av-system.



Bilaga 3, bild 26 *Riskanalys för system-av-system (SoSHA).*

En *Riskanalysrapport för system-av-system* (SoSHAR) bör innehålla:

- En beskrivning över vilka nya förmågor eller funktioner som åstadkommes vid samverkan mellan tekniska system och produkter
- En detaljerad fysisk och funktionell systembeskrivning över system-av-system eller funktionskedja samt övergripande beskrivningar av de ingående tekniska systemen
- Vilka anslutningsdon för sammankoppling eller adaptrar för gränsytor som krävs för samfunktionen
- Vilka krav som finns på system-av-system eller funktionskedjan
- En beskrivning av vilka riskanalysmetoder som använts
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Vilka unika olycksrisker som identifierats för system-av-system eller funktionskedja
- Sammanfattning av resultatet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till framtida systemsäkerhetsprovning
- Detaljerad redovisning som ligger till grund för sammanfattningen
- Data som överförs till *Risklogg* (RL)

TASK 207 – Health Hazard Analysis (HHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera hälsorelaterade olycks- och arbetsmiljörisker med tekniska system och produkter genom att bland annat utvärdera buller, emissioner och hälsofarliga ämnen som ger någon grad av omedelbar skada eller ohälsa. Denna aktivitet bör samordnas med den *Miljörelaterade risk–analysen* (EHA).

Den svenska benämningen är *Hälsorelaterad riskanalys* (HHA) och utdata/dokumentation är en *Hälsorelaterad riskanalysrapport* (HHAR). Den engelska benämningen på utdata/dokumentation är *Health Hazard Analysis* (HHA).

Resultatet av den *Hälsorelaterade riskanalysen* (HHA) ger även information till den som har arbetsgivar- och delegerat arbetsmiljöansvar i den organisation där det tekniska systemet ska användas. Långsiktig hälsopåverkan, exempelvis där ackumulerad dos över tid ger skador, samt psykosociala aspekter omhändertas i det systematiska arbetsmiljöarbetet.

Granskning och utvärdering bör ske mot EU-rätt, svensk lagstiftning och olika myndigheters föreskrifter, exempelvis utgivna av Arbetsmiljöverket, Kemikalieinspektionen eller Strålsäkerhetsmyndigheten.

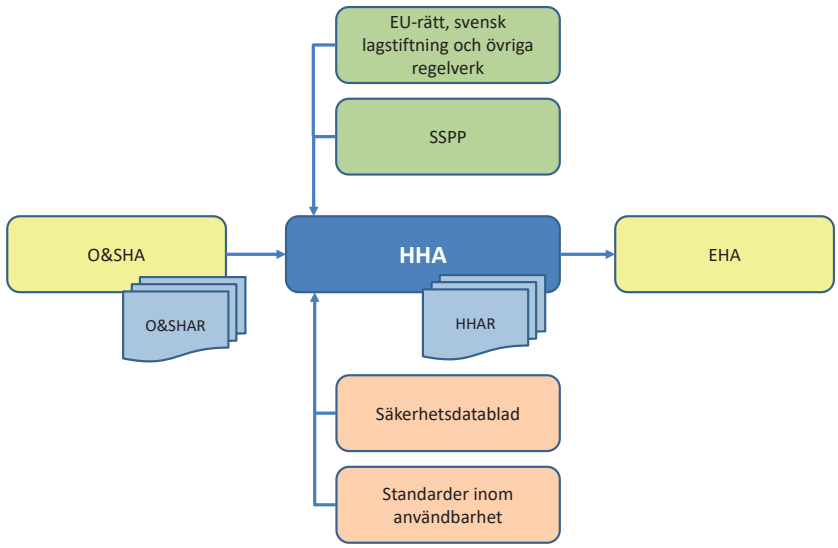
Den *Hälsorelaterad riskanalyse*n (HHA) identifierar farliga tillstånd och situationer för vilka användarna kan exponeras av buller, emissioner, hälsofarliga ämnen och kemiska produkter under det tekniska systemets alla användningssituationer. I analysen ingår även att analysera biologiska risker såsom mikro- och makrobiologiska organismer, ergonomiska risker såsom tunga lyft och felaktiga arbetsställningar samt risker med joniserad och icke-joniserad strålning såsom radioaktiva ämnen och radarstrålning. Vidare analyseras farliga ämnen som kan bildas vid abnorma miljöer, exempelvis vid brand.

I den *Hälsorelaterade riskanalysrapporten* (HHAR) kan riskreducerande åtgärder föreslås dels på det tekniska systemet avseende konstruktion eller val av kemiska produkter, dels att tillföra personlig skyddsutrustning (PPE), dels för den verksamhet som förväntas att genomföras. Vidare kan möjligheten till omhändertagande av exponerade personer beaktas, exempelvis under insats.

Indata, utdata och flödesbild

Indata till aktiviteten *Hälsorelaterad riskanalys* (HHA) utgörs av *Riskanalys för hantering* (O&SHA), lagstiftning, den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt säkerhetsdatablad och standarder inom användbarhet.

Utdata är *Hälsorelaterad riskanalysrapport* (HHAR). Den ger indata till den *Miljörelaterade riskanalysen* (EHA).



Bilaga 3, bild 27 *Hälsorelaterad riskanalys (HHA).*

En *Hälsorelaterad riskanalysrapport* (HHAR) bör innehålla:

- Vilket tekniskt system som avses
- Vilka möjligheter, krav och begränsningar som lagstiftningen ger
- Vilka andra begränsningar som beaktats, exempelvis krav i kontrakt
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Sammanfattning av resultatet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till fördjupade användbarhetsanalyser
- Detaljerad redovisning som ligger till grund för sammanfattningen
- Data som överförs till *Risklogg* (RL)

TASK 210 – Environmental Hazard Analysis (EHA)

Denna aktivitet är ersatt av S22 – Miljörelaterad riskanalys (EHA).

S22 – Miljörelaterad riskanalys (EHA)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera miljörelaterade olycksrisker och övrig miljöpåverkan med tekniska system och produkter genom att bland annat utvärdera buller, emissioner och miljöfarliga ämnen som ger någon grad av omedelbar skada eller miljöpåverkan på både flora och fauna. Denna aktivitet bör samordnas med den *Hälsorelaterade riskanalysen* (HHA).

Den engelska benämningen är *Environmental Hazard Analysis* (EHA) och utdata/dokumentation är en *Environmental Hazard Analysis* (EHA). Den svenska benämningen på utdata/dokumentation är *Miljörelaterad riskanalysrapport* (EHAR).

Resultatet av den *Miljörelaterade riskanalysen* (EHA) ger även information till den som har arbetsgivar- och delegerat arbetsmiljöansvar i den organisation där det tekniska systemet ska användas. Långsiktig miljöpåverkan, exempelvis där emissioner över tid bidrar till den globala uppvärmningen, eller miljöpåverkan som rör en specifik geografisk plats omhändertas i Försvarsmaktens hållbarhetsarbete.

Granskning och utvärdering bör ske mot EU-rätt, svensk lagstiftning och olika myndigheters föreskrifter, exempelvis utgivna av Naturvårdsverket eller Kemikalieinspektionen.

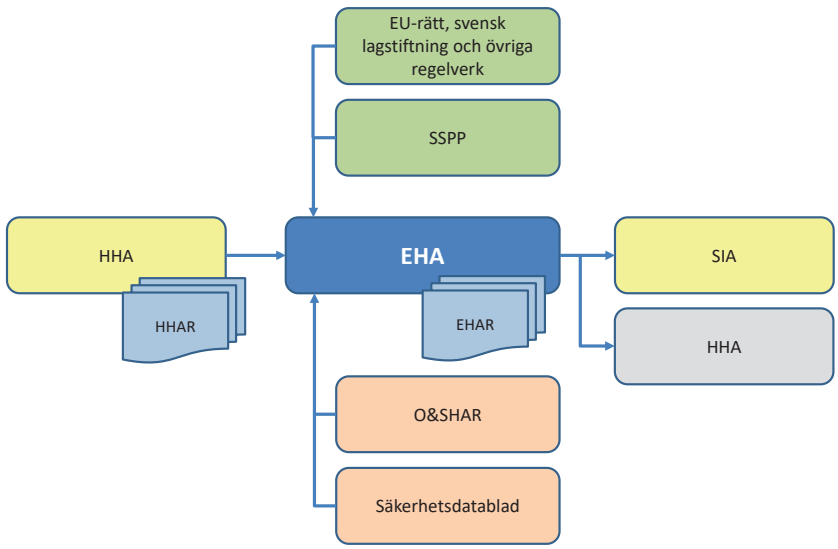
Den *Miljörelaterade riskanalysen* (EHA) identifierar farliga tillstånd och situationer för vilken flora och fauna kan exponeras av buller, emissioner, hälsofarliga ämnen och kemiska produkter under det tekniska systemets alla användningssituationer. Vidare analyseras farliga ämnen som kan bildas vid abnorma miljöer, exempelvis vid brand.

I den *Miljörelaterade riskanalysrapporten* (EHAR) kan riskreducerande åtgärder föreslås dels på det tekniska systemet avseende konstruktion eller val av kemiska produkter, dels att tillföra skyddsutrustning exempelvis en matta för att samla upp spill, dels för den verksamhet som förväntas att genomföras. Vidare kan möjligheten till sanering av exponerad flora beaktas, exempelvis under insats.

Indata, utdata och flödesschema

Indata till aktiviteten *Miljörelaterad riskanalys* (EHA) utgörs av *Hälsorelaterad riskanalys* (HHA), lagstiftning och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt *Riskanalysrapporten för hantering* (O&SHAR) och säkerhetsdatablad.

Utdata är *Miljörelaterade riskanalysrapporten* (EHAR). Den ger indata till *Säkerhetsföreskriftsanalys* (SIA) och *Hälsorelaterad riskanalys* (HHA).



Bilaga 3, bild 28 *Miljörelaterad riskanalys (EHA).*

En *Miljörelaterad riskanalysrapport* (EHAR) bör innehålla:

- Vilket tekniskt system som avses
- Vilka möjligheter, krav och begränsningar som lagstiftningen ger
- Vilka andra begränsningar som beaktats, exempelvis krav i kontrakt
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Sammanfattning av resultatet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till fördjupade miljöanalyser
- Detaljerad redovisning som ligger till grund för sammanfattningen
- Data som överförs till *Risklogg* (RL)

S23 – Säkerhetsföreskriftanalys (SIA)

Syfte och aktivitetsbeskrivning

Syftet med aktiviteten *Säkerhetsföreskriftsanalys* (SIA) är att redovisa de säkerhetsinstruktioner, varningar och varselmärkningar som behövs för att tekniska system och produkter ska erbjuda betryggande säkerhet vid användning, underhåll och förrådshållning (transport).

Den engelska benämningen är *Safety Instruction Analysis* (SIA) och utdata/dokumentation är *Safety Instruction* (SI). Den svenska benämningen på utdata/dokumentation är *Säkerhetsföreskrifter* (SI).

Konstruktören utarbetar *Säkerhetsföreskrifter* (SI) efter det att riskreducerande åtgärder såsom konstruktions- och skyddsåtgärder inte längre är möjliga. *Säkerhetsföreskrifter* (SI) påverkar dels vilka säkerhetsinstruktioner som krävs för säker hantering, dels vilka användningsbegränsningar och varningar som behöver infogas i bruksanvisningar och underhållsinstruktioner, dels vilka varselmärkningar som ska anbringas på tekniska system och produkter.

Krav på varselmärkningar och dess utförande finns ofta reglerat i olika föreskrifter. Varselmärkningar kan vara i form av skyltar, dekaler och andra märkningar såsom efterlysande plattor för nödutrymning.

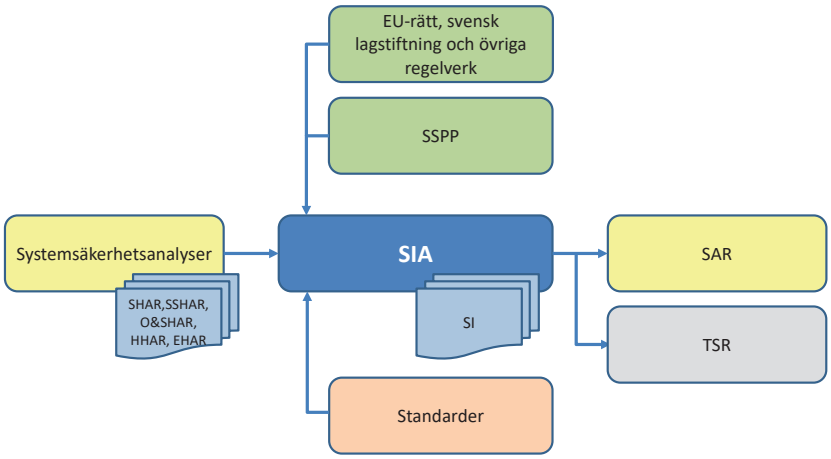
Bruksanvisningar och underhållsinstruktioner innehåller främst beskrivningar över hur man ska göra. I vissa fall behöver dessa beskrivningar kompletteras med varningstexter. Varningstexter bör innehålla följa:

- Vad är faran och hur kan man skydda sig, dvs varför ska instruktionen följas?
- Vad kan hända om en olycka inträffar?
- Vad blir konsekvensen om olyckan inträffar?

Indata, utdata och flödesbild

Indata till aktiviteten *Säkerhetsföreskriftsanalys* (SIA) utgörs av de genomförda systemsäkerhetsanalyser, lagstiftning och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt standarder.

Utdata är *Säkerhetsföreskrifter* (SI). Den ger indata till *Systemsäkerhetsrapport* (SAR) och *Handhavande och utbildning* (TSR).



Bilaga 3, bild 29 *Säkerhetsföreskriftanalys (SIA).*

Säkerhetsföreskrifter (SI) bör omfatta:

- Användningsbegränsningar
- Risk- och restriktionsområden
- Tillåten omgivningsmiljö vid användning (temperatur, luftfuktighet, elektromagnetiska fält mm)
- Tillåten förrådshållningsmiljö och samförvaringsbegränsningar (livslängd i obruten och bruten förpackning mm)
- Tillåtna transportsätt (landsväg, sjötransport, flygtransport, järnvägstransport)
- Tillåtna förpackningskrav, staplings- och samtransportbegränsningar (transportsäkringar, accelerationer, tryck- och temperaturväxlingar mm)

S24 – Riskanalys inför avveckling av system (RADS)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att identifiera olycksrisker som kan uppstå under den fysiska avvecklingen av tekniska system och produkter.

Den engelska benämningen är *Risk Assessment Prior to Disposal of Systems* (RADS) och utdata/dokumentation är en *Risk Assessment Prior to Disposal of Systems Report* (RADSR). Den svenska benämningen på utdata/dokumentation är *Riskanalysrapport inför avveckling av system* (RADSR).

Riskanalysen (RADS) genomförs dels under utveckling av tekniska system och produkter, dels inför den faktiska avvecklingen. Beroende på avvecklingsmetod såsom överlåtelse, försäljning eller destruktion kan *Riskanalysen* (RADS) få skilda fokus. *Riskanalysen* (RADS) omfattar olycksrisker som kan skada både person och/eller yttre miljö.

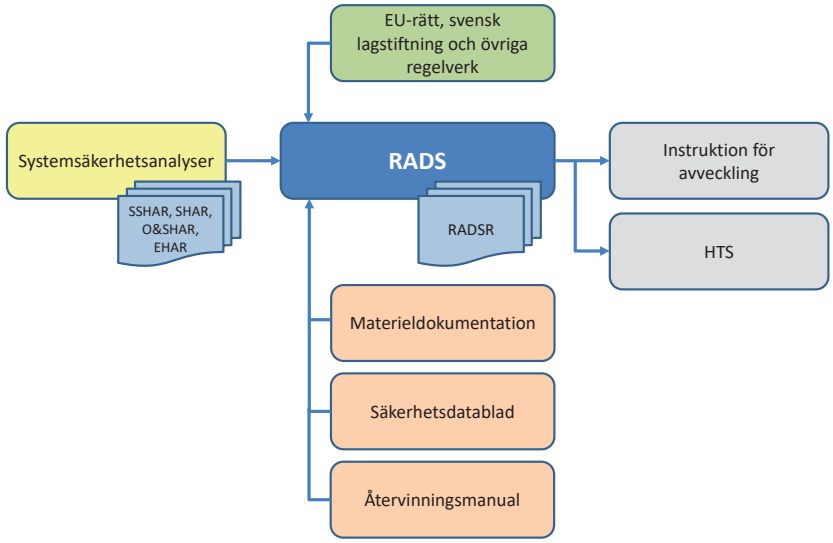
Riskanalysrapporten (RADSR) som tas fram under utvecklingsskedet fokuserar främst på konstruktionen samt på olycksrisker som kan inträffa vid borttagning och isärtagning av delsystem och produkter. Detta innebär exempelvis att val av material och kemiska produkter, ytbehandlingar och sammanfogningar av olika material beaktas ur ett destruktionsperspektiv. För olycksrisker som kan orsakas av lagrad energi, exempelvis i form av trycksatta kärl, spända fjädrar, reaktiva ämnen och energi i elektriska komponenter, ska säkra metoder för att eliminera eller reducera dessa olycksrisker anges.

Riskanalysrapporten (RADSR) som uppdateras eller tas fram under avvecklingsskedet analyserar krav i lagstiftningen inklusive tillämpligt producentansvar. För borttagning av delsystem och komponenter utgår man ifrån materieldokumentationen med inriktning på avhjälpande underhåll och identifierar sådana moment som tidigare inte har analyseras ut ett systemsäkerhetsperspektiv.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskanalys* (RADS) utgörs av de genomförda systemsäkerhetsanalyserna och lagstiftning samt materieldokumentationen med inriktning på avhjälpande underhåll, säkerhetsdatablad samt återvinningsmanual.

Utdata är *Riskanalysrapport* (RADSR). Den ger indata till en instruktion för avveckling och till *Riskhanteringssystemet* (HTS).



Bilaga 3, bild 30 *Riskanalys inför avveckling av system (RADS).*

En *Riskanalysrapport* (RADSR) bör innehålla:

- En fysisk systembeskrivning med de ingående delsystemen och annan eventuell utrustning såsom reservmateriel eller verktygssatser
- Vilka möjligheter, krav och begränsningar som lagstiftningen ger
- Vilka andra begränsningar som beaktats, exempelvis slutanvändarintyg
- Beskrivning av föreslagna avvecklingssätt såsom överlåtelse, försäljning, destruktion samt eventuella musei- eller uppvisningsföremål
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- Sammanfattning av resultatet
  - Föreslagna avvecklingssätt av det tekniska systemet
  - Kravuppfyllnad
  - Rekommendation om riskreducerande åtgärder
  - Förslag till fördjupade systemsäkerhetsanalyser, exempelvis inför överlåtelse, försäljning eller för eventuella musei- eller uppvisningsföremål
- Detaljerad redovisning som ligger till grund för sammanfattningen
- Data som överförs till *Risklogg* (RL)

Aktiviteter – SEKTION 300 – Utvärdering

TASK 301 – Safety Assessment Report (SAR)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att sammanfatta genomfört systemsäkerhetsarbete och redovisa dess slutsatser, ge information om kravuppfyllnad mot lagstiftning och kontrakt samt ge en detaljerad beskrivning av respektive olycksrisk med eventuell kompletterande information. Om *Systemsäkerhetsrapporten* (SAR) kompletteras med utökad information om ingående material så uppfyller den även Task 302, *Hazard Management Assessment Report* (HMAR).

Den svenska benämningen är *Systemsäkerhetsrapport* (SAR) och utdata/dokumentation är en *Systemsäkerhetsrapport* (SAR). Den engelska benämningen på utdata/dokumentation är *Safety Assessment Report* (SAR).

Systemsäkerhetsrapporten (SAR) kan antingen innehålla all information, alternativt utgöra en sammanfattning med referenser till underliggande systemsäkerhetsanalysrapporter eller annan riskdokumentation. För tekniska system och produkter som exempelvis godkänts genom vägval (VV1 och/eller VV3) kan motsvarande information redovisas direkt i systemsäkerhetsbeslutet.

Kravställarens sammanfattning över genomfört systemsäkerhetsarbete samt kravuppfyllnad mot lagstiftning, *Systemsäkerhetsledningsplan* (SSMP) och *Systemmålsättning* (SMS 2) behöver inte alltid dokumenteras i en särskild *Systemsäkerhetsrapport* (SAR) utan kan ingå direkt i *Systemsäkerhetsgodkännande*t (SSG).

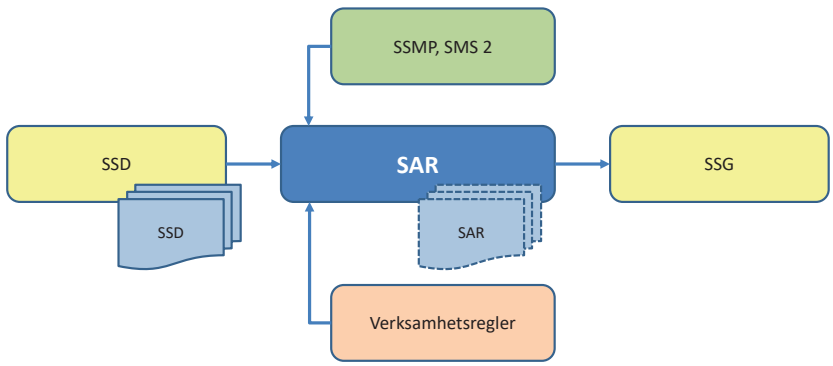
Beställarens sammanfattning över genomfört systemsäkerhetsarbete samt kravuppfyllnad mot lagstiftning och *Systemmålsättning* (SMS 2), vilken baseras på *konstruktörens Systemsäkerhetsutlåtande* (SCA), behöver inte alltid dokumenteras i en särskild *Systemsäkerhetsrapport* (SAR) utan kan ingå direkt i *Systemsäkerhetsdeklarationen* (SSD).

Konstruktörens Systemsäkerhetsrapport (SAR) baseras på checklistan nedan.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsrapport* (SAR) för *kravställaren* utgörs av *beställarens Systemsäkerhetsdeklaration* (SSD), *Systemsäkerhetsledningsplan* (SSMP) och *Systemmålsättning* (SMS 2) samt verksamhetsregler.

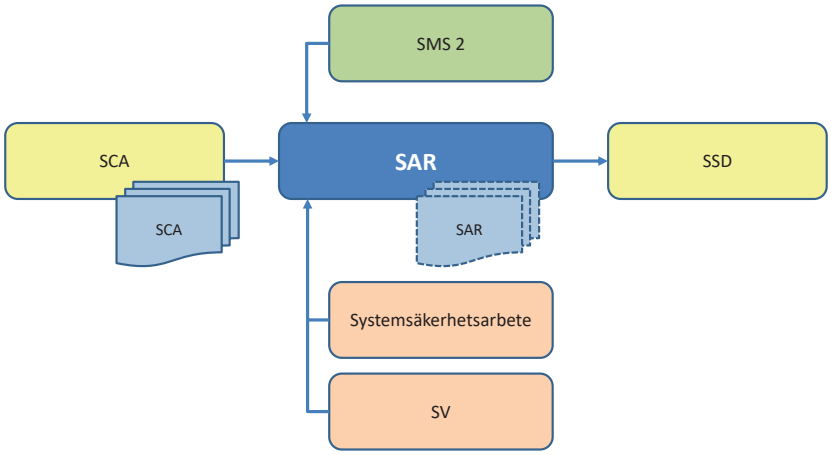
Utdata är *Systemsäkerhetsrapport* (SAR). Den är indata till *Systemsäkerhetsgodkännandet* (SSG).



Bilaga 3, bild 31 *Systemsäkerhetsrapport (SAR) för kravställaren.*

Indata till aktiviteten *Systemsäkerhetsrapport* (SAR) för *beställaren* utgörs av *konstruktörens Systemsäkerhetsutlåtande* (SCA) och *Systemmålsättning* (SMS 2) samt eget systemsäkerhetsarbete och *Systemsäkerhetsverifiering* (SV).

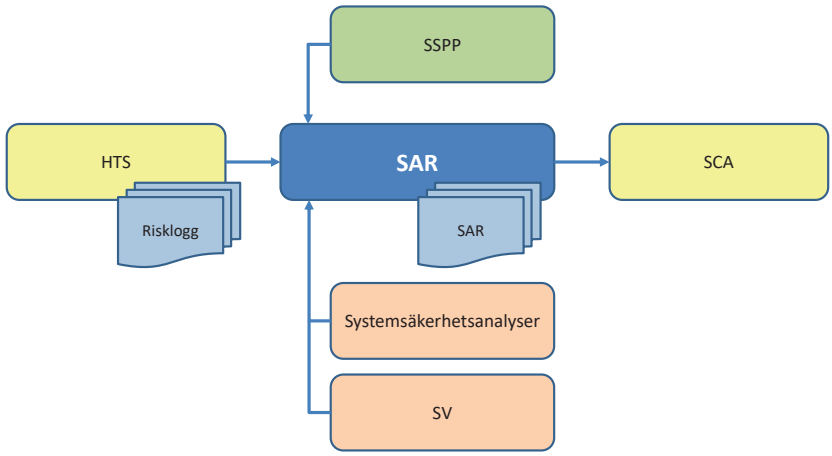
Utdata är *Systemsäkerhetsrapport* (SAR). Den är indata till *Systemsäkerhetsdeklarationen* (SSD).



Bilaga 3, bild 32 *Systemsäkerhetsrapport (SAR) för beställaren.*

Indata till aktiviteten *Systemsäkerhetsrapport* (SAR) för *konstruktören* utgörs av *Riskhanteringssystemet* (HTS) och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt de genomförda systemsäkerhetsanalyserna och resultat från *Systemsäkerhetsverifiering* (SV).

Utdata är *Systemsäkerhetsrapporten* (SAR). Den är indata till *Systemsäkerhetsutlåtandet* (SCA).



Bilaga 3, bild 33 *Systemsäkerhetsrapport (SAR) för konstruktören.*

En *Systemsäkerhetsrapport* (SAR) bör innehålla:

- En systembeskrivning med ingående delsystem, utbildningssystem och annan eventuell utrustning såsom reservmateriel eller verktygssatser
- En precisering av tekniskt systems tillåtna konfigurationer, tillåtna ändringsbara parameterintervall samt gränsytor
- Referenser till bruksanvisningar och underhållsinstruktioner samt tekniska data
- En beskrivning av avsedd användningsmiljö och operationsbetingelser
- Vilka data och förutsättningar som använts samt vilka antaganden som gjorts
- En redovisning av krav i lagstiftning, kontrakt och *Systemsäkerhetsplan* (SSPP)
- De myndighetsbeslut som finns för att kunna ta det tekniska systemet i bruk
- Redovisning av tillämpade civila och militära standarder
- En redovisning över vilka vägval (VV) som gjorts, motiv för vägvalen samt acceptanskriterier för när dessa ansetts vara relevanta och tillräckliga
- Att olycksrisker som hanterats med vägval (VV7) ryms inom *Tolerabel risknivå* (TR)
- En sammanfattning över dimensionerande olycksrisker samt referens till *Risklogg* (RL)
- Referenser till andra systemsäkerhetsrapporter och riskdokumentation som använts
- Referenser till systemsäkerhetsprovningar och ett ställningstagande utifrån resultaten
- Kvarstående olycksrisker med restriktioner och kriterier för hävande av restriktioner
- En systemsäkerhetsvärdering som grund för ställningstagandet
- Bilagor, exempelvis säkerhetsdatablad

TASK 302– Hazard Management Assessment Report (HMAR)

Denna aktivitet regleras helt av aktiviteten Safety Assessment Report (SAR).

TASK 303 – Test and Evaluation Participation (TEP)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att redovisa ett ställningstagande avseende det tekniska systemets eller delsystemens systemsäkerhet inför den provning som ska ske mot standarder, kontrakt eller andra krav och som genomförs inom den egna organisationen.

Den svenska benämningen är *Riskanalys inför provning* (TEP) och utdata/dokumentation är ett *Systemsäkerhetsintyg* (SSI). Den engelska benämningen på utdata/dokumentation är *System Safety Certificate* (SSI).

Riskanalys inför provning (TEP) utgår ifrån det tekniska systemets eller delsystemens aktuella konfigurationer. Vidare analyseras den provningsverksamhet som anges i de standarder, alternativt i de provprogram eller provplaner, som ska genomföras. Utifrån det tekniska systemets utvecklingsstatus identifieras olycksrisker och förslag ges till riskreducerande åtgärder inför provningen. Som stöd för denna aktivitet kan *Riskkälleanalys* (PHA), *Säkerhetsföreskriftanalys* (SIA) samt vid behov de fördjupade systemsäkerhetsanalyserna tillämpas.

Systemsäkerhetsintyget (SSI) är ett ställningstagande från *beställaren, systemintegratören* eller *konstruktören* till den egna provningsorganisationen, som bekräftar att lagstiftning, regelverk och bestämmelser uppfylls. *Systemsäkerhetsintyget* (SSI) utgör en sammanfattning av hittills utfört systemsäkerhetsarbete samt att eventuella avvikelser eller osäkerheter kring provningen är hanterade genom riskreducerande åtgärder samt att det tekniska systemet eller delsystemen erbjuder betryggande säkerhet, givet att förslagen till *Säkerhetsföreskrifter* (SI) följs.

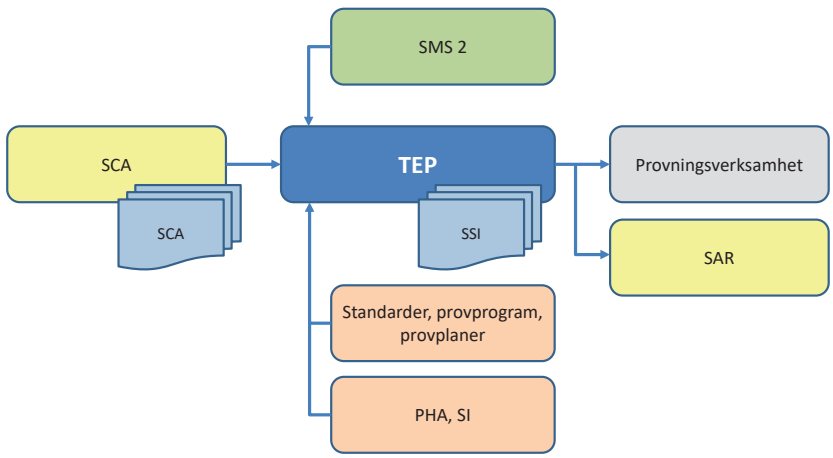
Systemsäkerhetsintyget (SSI) kan i princip ha samma struktur och innehåll som ett motsvarande systemsäkerhetsbeslut, exempelvis *Systemsäkerhetsutlåtande* (SCA) eller *Systemsäkerhetsdeklaration* (SSD). *Systemsäkerhetsintyget* (SSI) undertecknas av behörig person utanför den del av organisationen som ska genomföra provningen.

Systemsäkerhetsintyg (SSI) utfärdas inte för organisations- och metodförsök som genomförs i Försvarsmaktens regi.

Indata, utdata och flödesbild

Indata till aktiviteten *Riskanalys inför provning* (TEP) för *beställare* och *systemintegratör* utgörs av *Systemsäkerhetsutlåtande* (SCA) och *Systemmålsättning* (SMS 2) samt standarder, provprogram eller provplaner.

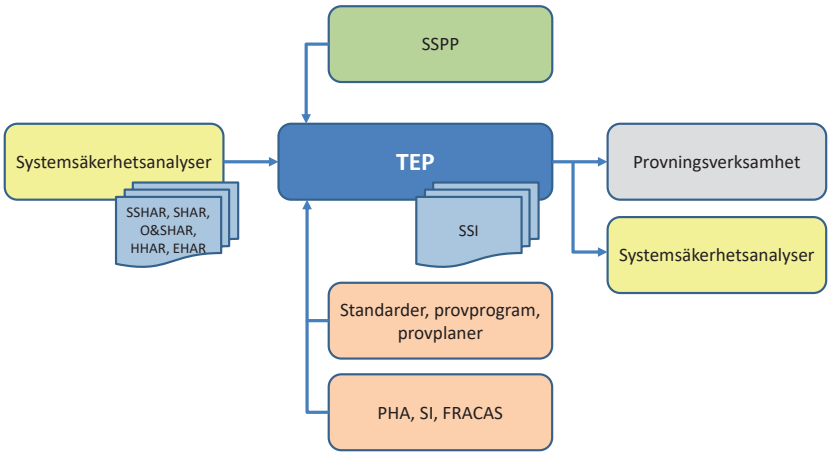
Utdata är ett *Systemsäkerhetsintyg* (SSI). Den ger indata till provningsverksamheten samt till *Systemsäkerhetsrapporten* (SAR).



Bilaga 3, bild 34 *Riskanalys inför provning (TEP) för beställare och systemintegratör.*

Indata till aktiviteten *Riskanalys inför provning* (TEP) för *konstruktör* utgörs av systemsäkerhetsanalyser och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt standarder, provprogram, provplaner och erfarenhetsdata ut *Felrapporteringssystem* (FRACAS).

Utdata är ett *Systemsäkerhetsintyg* (SSI). Den ger indata till provningsverksamheten samt till *Systemsäkerhetsanalyser*.



Bilaga 3, bild 35 *Riskanalys inför provning (TEP) för konstruktör.*

Om en *Systemsäkerhetsrapport* (SAR) finns som innehåller nedanstående information, kan hänvisning ske till detta dokument. Ett *Systemsäkerhetsintyg* (SSI) bör innehålla:

- En precisering av tekniskt systems eller delsystemens utförande, tillåtna konfigurationer, tillåtna ändringsbara parameterintervall samt gränsytor
- Vilka bruksanvisningar och *Säkerhetsföreskrifter* (SI) som finns
- En beskrivning av avsedd provningsmiljö
- Referens till provprogram eller provplan
- Att lagstiftningen är uppfylld vid tidpunkten för provningen
- Vilka systemsäkerhetsanalyser som genomförts för att identifiera, analysera, värdera olycksrisker samt förslag till riskreducerande åtgärder för provningen
- Vilka miljö- och hälsofarliga ämnen/material som finns i det tekniska systemet och som personer eller yttre miljö kan exponeras för vid provningen. För kemiska produkter ska säkerhetsdatablad finnas
- Rekommenderad utbildning för provpersonalen

S31 – Felrapporteringssystem (FRACAS)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är att återföra tillbuds- och olycksrelaterad information för att förhindra att en liknande olycka under motsvarande förutsättningar kan inträffa på nytt. Aktiviteten kan dels tillämpas för tillbuds- och olycksrapportering

i intern verksamhet, dels genom överenskommelse i kontrakt i syfte att förändra konstruktionen innan det tekniska systemet har tagits i bruk.

Den engelska benämningen är *Failure Reporting, Analysis and Corrective Action System* (FRACAS) och utdata/dokumentation är *Åtgärdsrapporter*.

Felrapporteringssystem (FRACAS) bör finnas från första provningen eller hanteringen till dess att det tekniska systemet är avvecklat. Data ur *Felrapporteringssystemet* (FRACAS) och dess sammanställda information kan användas både för det aktuella tekniska systemet och för likartade tekniska system som exempelvis använder samma delsystem eller komponenter.

Data ur *Felrapporteringssystemet* (FRACAS) utgör en del av underlaget till de olika systemsäkerhetsanalyserna. Erfarenhetsrelaterad information kan dels användas för att analysera reell påverkan av eventuella modifieringar, dels för att värdera effekten av föreslagna riskreducerande åtgärder i det tekniska systemet eller i dess användning.

Data ur *kravställarens Felrapporteringssystem* (FRACAS) analyseras lämpligen av *Arbetsgrupp för systemsäkerhet* (SSWG) under vidmakthållande- och avvecklingsskedet, vilka även har att föreslå korrigerande åtgärder eller påverka innehållet i framtida *Systemmålsättningar* (SMS).

Data ur *konstruktörens Felrapporteringssystem* (FRACAS) analyseras lämpligen av *Systemsäkerhetsgruppen* (IPT/WG) under det tekniska systemets utvecklingsskede, vilka även har att föreslå riskreducerande åtgärder.

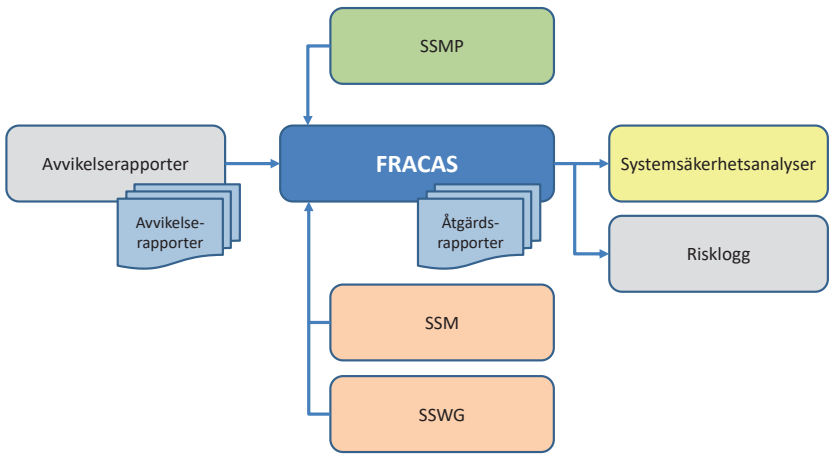
Felrapporteringssystemet (FRACAS) förser olika intressenter med data eller sammanställd information oavsett i vilket livscykelskede det tekniska systemet befinner sig i. Ansvarig instans för *Felrapporteringssystemet* (FRACAS) behöver ha möjlighet att klassificera inkomna avvikelserapporter ur allvarlighetssynpunkt avseende systemsäkerhet.

Orsaken till olyckor och tillbud är oftast inte en enskild felorsak utan en händelsekedja med ett antal olyckliga omständigheter bestående av både felorsaker och naturliga tillstånd. Syntesen av en mängd olika data tillsammans med vissa förutsättningar kan förhindra framtida olyckor.

Indata, utdata och flödesbild

Indata till aktiviteten *Felrapporteringssystem* (FRACAS) för *kravställare* utgörs av avvikelserapporter från Försvarsmaktens användning, underhåll och förrådshållning (transport) samt *Systemsäkerhetsledningsplan* (SSMP). Även *Systemsäkerhetsmeddelanden* (SSM) kan finnas. *Arbetsgrupp för systemsäkerhet* (SSWG) kan utarbeta *åtgärdsrapporter*.

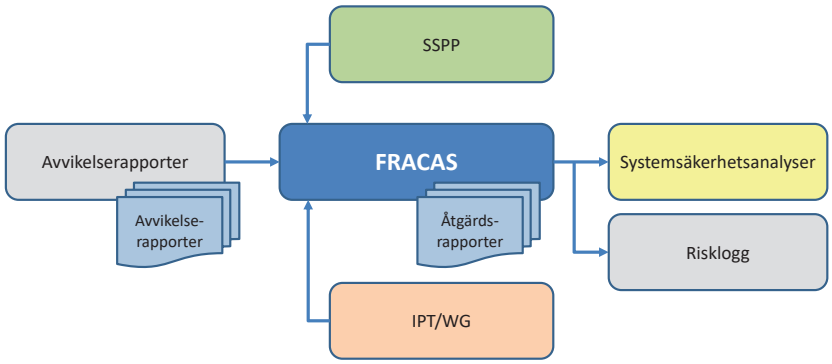
Utdata är *Åtgärdsrapporter*. Dessa kan utgöra indata till fördjupade systemsäkerhetsanalyser och *Risklogg* (RL).



Bilaga 3, bild 36 *Felrapporteringssystem (FRACAS) för kravställare.*

Indata till aktiviteten *Felrapporteringssystem* (FRACAS) för *konstruktör* utgörs av avvikelserapporter från *konstruktörens* användning, provning, underhåll, förrådshållning (transport) och annan hantering samt den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Utdata är *Åtgärdsrapporter* som utgör indata till *konstruktörens* olika fördjupade systemsäkerhetsanalyser och *Risklogg* (RL).



Bilaga 3, bild 37 *Felrapporteringssystem (FRACAS) för konstruktör.*

Felrapporteringssystem (FRACAS) bör innehålla:

- Rapportör med kontaktuppgifter
- Det tekniska systemet identitet och materieldokumentationens status
- Vilka *Säkerhetsföreskrifter* (SI) fanns
- Beskrivning av händelseförlopp och konsekvens av det inträffade
  - Plats och datum för händelsen
  - Den verksamhet som utövades då händelsen inträffade, exempelvis under användning, förflyttning, strid, vård, underhåll eller förrådshållning (transport)
  - Eventuella skador på person, egendom eller yttre miljö, även på tredje person eller dennes egendom
  - Vilka skador som potentiellt skulle kunnat inträffa
  - Övrigt
- Återkoppling till rapportör

TASK 304 – Safety Review (SR)

Syftet med denna aktivitet är att ur systemsäkerhetssynpunkt utvärdera föreslagna ändringar (modifieringar) på fastställda konfigurationer av tekniska system och produkter. Det kan dels avse ändringar i kravdokument, dels föreslagna modifieringar på maskin-, elektronik och/eller programvara. Aktiviteten bör samordnas med det tekniska systemets konfigurationsplan.

Aktiviteter – SEKTION 400 – Verifiering

TASK 401 – Safety Verification (SV)

Syfte och aktivitetsbeskrivning

Syftet med denna aktivitet är dels att visa att systemsäkerhetskraven är uppfyllda genom verifiering, dels att visa att det tekniska systemet motsvarar efterfrågat behov genom validering.

Den svenska benämningen är *Systemsäkerhetsverifiering* (SV) och utdata/dokumentation är *Systemsäkerhetsverifieringsrapport* (SVR). Den engelska benämningen för utdata/dokumentation är *Safety Verification* (SV).

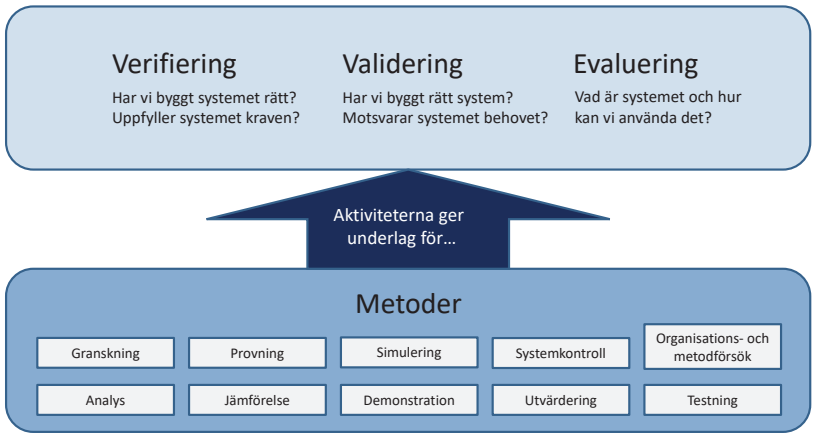
Det finns ett flertal olika metoder som kan ge underlag för analys om respektive krav är uppfyllt. Resultatet av verifieringen och valideringen kan användas som stöd och för att styrka beläggen i systemsäkerhetsvärderingen.

Metoder för *Systemsäkerhetsverifiering* (SV) bör vara en integrerad del av verifieringen av det tekniska systemet och ingå i den samlade planeringen för samtliga verifieringsaktiviteter.

Att införa mekaniska fel eller injicera fel i programvaran kan användas för att demonstrera att säkerhetssystem inklusive feldetektering, fungerar som det är tänkt och att den samlade robustheten av riskreducerande åtgärder kan anses vara tillräcklig. Detta innebär också att gränsytor måste anpassas så att felinjicering är möjlig på det tekniska systemet.

Vid konstruktionsändringar måste förnyad verifiering av systemsäkerhetskraven ske.

Evaluering faller utanför verifiering och validering och tillämpas för att undersöka hur det tekniska systemet är möjligt att använda innan den slutliga konfigurationen fastställs.

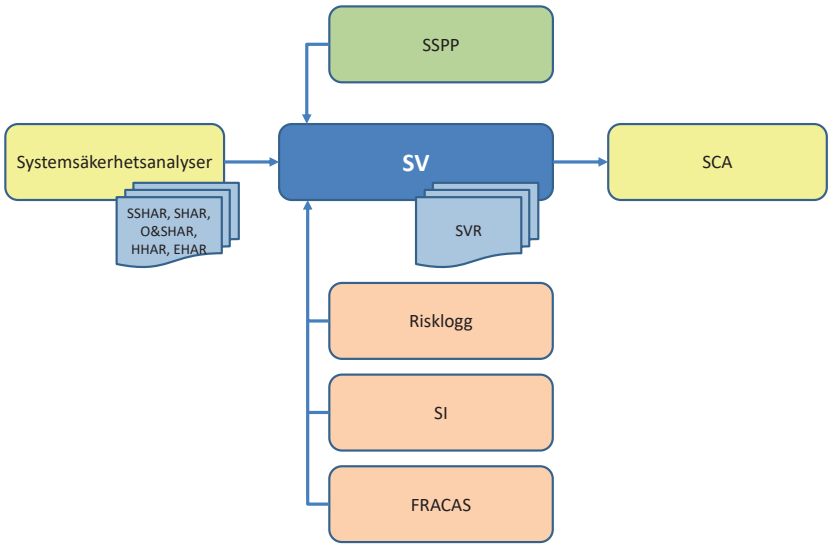


Bilaga 3, bild 38 Metoder för verifiering och validering.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsverifiering* (SV) utgörs av genomförda systemsäkerhetsanalyser och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP) samt erfarenhetsdata ur *Felrapporteringssystem* (FRACAS) och *Säkerhetsföreskrifter* (SI).

Utdata är *Systemsäkerhetsverifieringsrapport* (SVR). Den utgör ett underlag för *Systemsäkerhetsutlåtande* (SCA).



Bilaga 3, bild 39 Systemsäkerhetsverifiering (SV).

En *Systemsäkerhetsverifieringsrapport* (SVR) bör innehålla:

- Det tekniska systemets konfiguration och status
- Avsikten med verifieringen och vilka specifika systemsäkerhetskrav som omfattas
- Referens till använda standarder eller beskrivning av andra metoder för verifieringen
- En sammanfattning och slutsatser från erhållna provningsresultat
- Motiv för vilka olycksrisker som med stöd av resultat från genomförd provning, kan visa på kravuppfyllnad eller bidra till att demonstrera det tekniska systemets systemsäkerhet

TASK 402 – Explosives Hazard Classification Data

Denna aktivitet regleras helt av Handbok Vapen- och Ammunitionssäkerhet (H VAS).

TASK 403 – Explosive Odnance Disposal Data

Denna aktivitet regleras helt av Handbok Vapen- och Ammunitionssäkerhet (H VAS).

Aktiviteter – SEKTION 500 – Beslut

S51 – Systemsäkerhetsutlåtande (SCA)

Syfte och aktivitetsbeskrivning

Syftet med aktiviteten *Systemsäkerhetsutlåtande* (SCA) är att *konstruktören* redovisar dennes ställningstagande avseende det tekniska systemets systemsäkerhet inför leverans.

Den engelska benämningen är *Safety Compliance Assessmen*t (SCA) och utdata/dokumentation är *Safety Compliance Assessment* (SCA). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetsutlåtande* (SCA).

Systemsäkerhetsutlåtandet (SCA) utgör en sammanfattning över *konstruktörens* genomförda systemsäkerhetsarbete för ett visst tekniskt system, vilket baseras på den kontraktsbundna *Systemsäkerhetsplanen* (SSPP). *Systemsäkerhetsutlåtandet* (SCA) redovisar att gällande lagstiftning vid leveranstidpunkten är uppfylld, att *beställarens* systemsäkerhetskrav är uppfyllda samt att det tekniska systemet erbjuder betryggande säkerhet.

Systemsäkerhetsutlåtandet (SCA) innehåller *konstruktörens* ställningstagande som förutsätter att bruksanvisningar, underhållsinstruktioner och *Säkerhetsföreskrifter* (SI) följs när det tekniska systemet tas i bruk. *Konstruktörens* ställningstagande baseras på genomförd systemsäkerhetsvärdering.

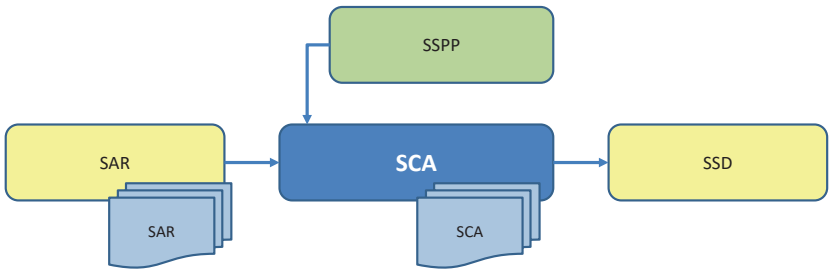
Som underlag för systemsäkerhetsvärderingen, med dess argument och belägg, ligger alla de systemsäkerhetsaktiviteter som genomförts under det tekniska systemets utveckling. Resultatet av dessa aktiviteter har dokumenterats efterhand som de genomförts. Det sammanställda underlaget för *Systemsäkerhetsutlåtandet* (SCA) dokumenteras oftast i en *Systemsäkerhetsrapport* (SAR) tillsammans med en *Risklogg* (RL). I *Systemsäkerhetsutlåtande* (SCA) hänvisas till dessa dokument samt till annan riskdokumentation.

Systemsäkerhetsutlåtandet (SCA) undertecknas av firmatecknare hos *konstruktören* eller någon av denne delegerad, vilket regleras i den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsutlåtande* (SCA) utgörs av *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL) och den kontraktsbundna *Systemsäkerhetsplanen* (SSPP).

Utdata är *Systemsäkerhetsutlåtande* (SCA). Den är indata till *Systemsäkerhetsdeklarationen* (SSD).



Bilaga 3, bild 40 Systemsäkerhetsutlåtande (SCA).

Om en *Systemsäkerhetsrapport* (SAR) finns som innehåller nedanstående information, kan hänvisning ske till detta dokument. *Systemsäkerhetsutlåtande* (SCA) bör omfatta följande:

- En precisering av tekniskt systems utförande, tillåtna konfigurationer, ändringsbara parameterintervall, gränsytor samt tillhörande tekniska data
- Vilka bruksanvisningar, underhållsinstruktioner och *Säkerhetsföreskrifter* (SI) som finns
- En beskrivning av avsedd användningsmiljö och operationsbetingelser
- Att lagstiftningen är uppfylld vid tidpunkten för leverans
- Att intyg eller godkännanden såsom DoC, CoC eller CA finns
- Att fysiska märkningar såsom CE- och rattmärkning finns
- Att eventuella undantag för militär materiel finns dokumenterade
- Vilka myndighetsbeslut som finns för att få ta det tekniska systemet i bruk
- Vilka civila och militära systemsäkerhetsrelaterade standarder som tillämpats
- Vilka vägval som gjorts samt motivering varför dessa ansetts relevanta och tillräckliga
- Vilka systemsäkerhetskrav med dess kriterier som uppfyllts samt hur kraven har verifierats

- Vilka systemsäkerhetsanalyser och systemsäkerhetsprovningar som genomförts för att identifiera, analysera, värdera, klassificera och åtgärda olycksrisker och deras orsaker
- Att *Risklogg* (RL) med varje identifierad olycksrisk som kan förekomma under såväl förväntad användning som under abnorma betingelser, tillsammans med riskreducerande åtgärder, rekommendationer och *Säkerhetsföreskrifter* (SI) finns
- Vilka olycksrisker som är hanterade
- Vilka olycksrisker som är kvarstående med restriktioner
- Vilka miljö- och hälsofarliga ämnen/material som finns i det tekniska systemet och som personer eller yttre miljö kan exponeras för vid användning, underhåll, förrådshållning (transport) eller avveckling. För kemiska produkter ska säkerhetsdatablad finnas
- Rekommenderad utbildning för användare
- Referenser till protokoll eller mötesanteckningar från *Systemsäkerhetsgruppen* (IPT/WG)

S52 – Systemsäkerhetsdeklaration (SSD)

Syfte och aktivitetsbeskrivning

Syftet med aktiviteten *Systemsäkerhetsdeklaration* (SSD) är att *beställaren* redovisar dennes ställningstagande avseende det tekniska systemets systemsäkerhet inför överlämning.

Den engelska benämningen är *System Safety Declaration* (SSD) och utdata/dokumentation är *System Safety Declaration* (SSD). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetsdeklaration* (SSD).

Systemsäkerhetsdeklarationen (SSD) utgör en sammanfattning över genomfört systemsäkerhetsarbete hos både *beställaren* och *konstruktören* för ett visst tekniskt system, vilket baseras på kraven i *Systemmålsättnin*g (SMS 2) omsatt till *beställarens Systemsäkerhetsplan* (SSPP). *Systemsäkerhetsdeklarationen* (SSD) redovisar att gällande lagstiftning vid leveranstidpunkten är uppfylld, att *kravställarens* systemsäkerhetskrav är uppfyllda samt att det tekniska systemet erbjuder betryggande säkerhet.

Systemsäkerhetsdeklarationen (SSD) innehåller *beställarens* ställningstagande, som förutsätter att materielpublikationer och *Säkerhetsföreskrifter* (SI) följs när det tekniska systemet tas i bruk. *Beställarens* ställningstagande baseras på genomförd systemsäkerhetsvärdering med *konstruktörens Systemsäkerhetsutlåtande* (SCA) som grund.

Som underlag för *beställarens* systemsäkerhetsvärdering, med dess argument och belägg, ligger alla de systemsäkerhetsaktiviteter som genomförts av både *konstruktören* och *beställaren* under det tekniska systemets utveckling. Resultatet av dessa aktiviteter har dokumenterats efterhand som de genomförts. Det sammanställda underlaget för *Systemsäkerhetsdeklaration* (SSD) dokumenteras oftast i en *Systemsäkerhetsrapport* (SAR) tillsammans med en *Risklogg* (RL). I *Systemsäkerhetsdeklaration* (SSD) hänvisas till dessa dokument samt till annan riskdokumentation.

Systemsäkerhetsdeklaration (SSD) kan även innehålla restriktioner, vilka är temporära inskränkningar i det tekniska systemets tillåtna användning, för att tillfälligt hantera en viss kvarstående olycksrisk och därigenom innehålla ställda krav på systemsäkerhet.

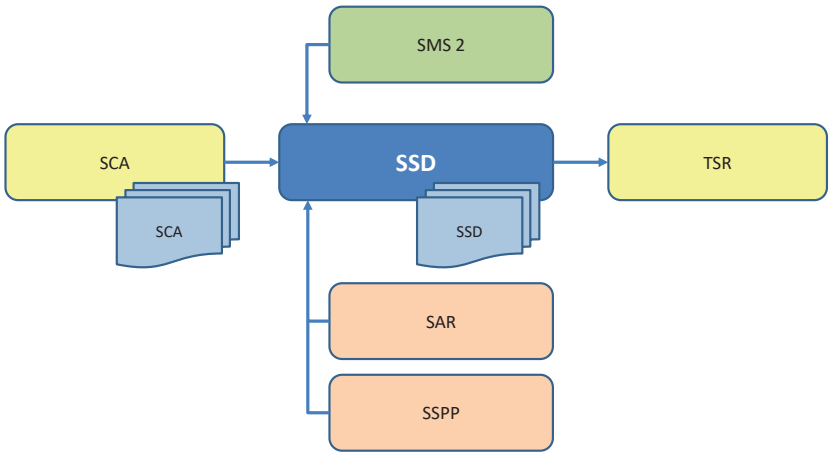
För ammunition ska protokoll från FMV:s Rådgivningsgrupper bifogas och genomförda åtgärder vara kommenterade. Om ett visst enskilt råd inte har följts ska även detta anges och motiveras.

Systemsäkerhetsdeklaration (SSD) undertecknas av behörig person hos *beställaren*.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsdeklaration* (SSD) utgörs av *konstruktörens Systemsäkerhetsutlåtande* (SCA) och *Systemmålsättning* (SMS 2) samt *beställarens Systemsäkerhetsplan* (SSPP) och *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL).

Utdata är *Systemsäkerhetsdeklaration* (SSD). Den är indata till *Handhavande och utbildning* (TSR).



Bilaga 3, bild 41 Systemsäkerhetsdeklaration (SSD).

Om en *Systemsäkerhetsrapport* (SAR) finns som innehåller nedanstående information, kan hänvisning ske till detta dokument. *Systemsäkerhetsdeklarationen* (SSD) bör omfatta följande:

- Precisering av tekniskt systems utförande, tillåtna konfigurationer, ändringsbara parameterintervall samt gränsytor
- Vilka materielpublikationer, tekniska data och *Säkerhetsföreskrifter* (SI) som finns
- Beskrivning av avsedd användningsmiljö och operationsbetingelser
- Att lagstiftningen är uppfylld vid tidpunkten för överlämning
- Att intyg eller godkännanden såsom DoC, CoC eller CA finns
- Att fysiska märkningar såsom CE- och rattmärkning finns
- Att eventuella undantag för militär materiel finns dokumenterade
- Vilka myndighetsbeslut som finns för att få ta det tekniska systemet i bruk
- Vilka civila och militära systemsäkerhetsrelaterade standarder som tillämpats
- Vilka vägval som gjorts samt motivering varför dessa ansetts relevanta och tillräckliga
- Vilka systemsäkerhetskrav med dess kriterier som uppfyllts samt hur kraven har verifierats

- Vilka systemsäkerhetsanalyser och systemsäkerhetsprovningar som genomförts för att identifiera, analysera, värdera, klassificera och åtgärda olycksrisker och deras orsaker
- Att *Risklogg* (RL) med varje identifierad olycksrisk som kan förekomma under såväl förväntad användning som under abnorma betingelser, tillsammans med riskreducerande åtgärder, rekommendationer och *Säkerhetsföreskrifter* (SI) finns
- Vilka olycksrisker som är hanterade
- Vilka olycksrisker som är kvarstående med restriktioner och vilka kriterier som gäller för att kunna häva restriktionerna
- Redovisning av de miljö- och hälsofarliga ämnen/material som finns i det tekniska systemet och som personer eller yttre miljö kan exponeras för vid användning, underhåll, förrådshållning (transport) eller avveckling. För kemiska produkter ska säkerhetsdatablad finnas
- Rekommenderad utbildning för användare
- Svar på eventuell hemställan om undantag för olycksrisk som är *Ej tolerabel* (ET)
- Om det tekniska systemet innehåller vapen, ammunition eller explosiv vara ska:
  - Protokoll från FMV:s Rådgivningsgrupper finns och att råden är kommenterade och motiverade
  - Förteckning över godkänd ammunition som får användas i vapensystemet finnas, alternativt att ammunitionen är godkänd mot vissa vapensystem

S53 – Handhavande och utbildning (TSR)

Syfte och aktivitetsbeskrivning

Syftet med aktiviteten *Handhavande och utbildning* (TSR) är att *kravställaren* fastställer materieldokumentation, färdigställer utbildningar samt ger ut de verksamhetsregler som erfordras för säker hantering av det tekniska systemet. Med hantering avses användning, underhåll, förrådshållning (transport) och avveckling.

Den engelska benämningen är *Training Safety Regulations* (TSR) och utdata/dokumentation är *Training Safety Regulations* (TSR). Den svenska benämningen på utdata/dokumentation är *Handhavande och utbildning* (TSR).

Fastställande av materieldokumentation och verksamhetsregler är en förutsättning för att kunna utfärda *Systemsäkerhetsgodkännande* (SSG). Färdigställande av utbildningar bör ske innan *Beslut om användning, central nivå* (BOAC) fattas. Underlag framgår bland annat av *Säkerhetsföreskrifterna* (SI).

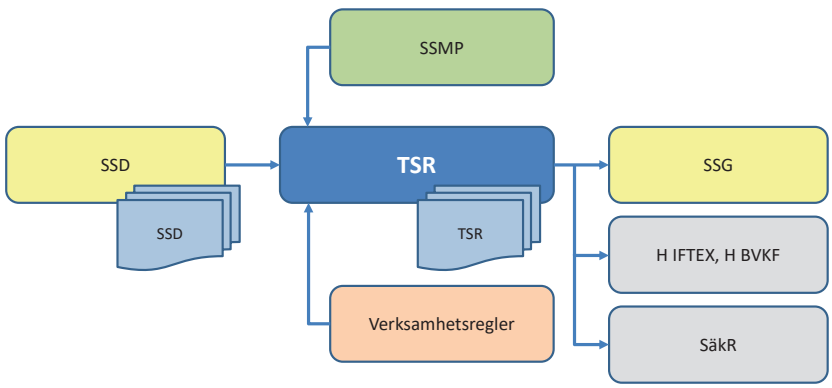
Särskilda instruktioner kan finnas för transport och förvaring av explosiver (IFTEX), brand- och räddningsinstruktioner (BRI) samt för användning, exempelvis Säkerhetsreglementet (SäkR).

Föreskrifter för transport och förvaring av tekniska system eller produkter som innehåller explosivämne fastställs av Myndigheten för samhällsskydd och beredskap (MSB), inklusive klassificeringskod enligt *United Nations Recommendations on the Transport of Dangerous Goods* (FN:s system). Koden består av en FN-klass och ett FN-nummer och tillämpas i olika transportregelverk, exempelvis ADR-S. För ytterligare detaljer, se H IFTEX.

Indata, utdata och flödesbild

Indata till aktiviteten *Handhavande och utbildning* (TSR) utgörs av *Systemsäkerhetsdeklaration (*SSD) och *Systemsäkerhetsledningsplanen* (SSMP) samt verksamhetsregler.

Utdata är *Handhavande och utbildning* (TSR). Den ger underlag till reglementen och kompletterande handböcker, exempelvis *Försvarsmaktens Handbok Förvaring och transport av ammunition och övriga explosiva varor* (H IFTEX), *Försvarsmaktens Handbok för åtgärder mot brand- och explosionsfara vattenförorening samt kemisk hälsopåverkan från brandfarliga varor* (H BVKF) samt *Säkerhetsreglementet* (SäkR).



Bilaga 3, bild 42 *Handhavande och utbildning (TSR).*

S54 – Systemsäkerhetsgodkännande (SSG)

Syfte och aktivitetsbeskrivning

Syftet med aktiviteten *Systemsäkerhetsgodkännande* (SSG) är att *kravställaren* dels redovisar dennes ställningstagande avseende det tekniska systemets systemsäkerhet, dels att riskreducerande åtgärder för verksamheten har vidtagits inför att det tekniska systemet tas i bruk.

Den engelska benämningen är *System Safety Approval* (SSG) och utdata/dokumentation är *System Safety Approval* (SSG). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetsgodkännande* (SSG).

Systemsäkerhetsgodkännandet (SSG) utgör en sammanfattning över genomfört systemsäkerhetsarbete hos både *beställaren*, *konstruktören* och *kravställaren* för ett visst tekniskt system, vilket baseras på kraven i *Systemsäkerhetsledningsplanen* (SSMP) och S*ystemmålsättning* (SMS 2). S*ystemsäkerhetsgodkännandet* (SSG) redovisar att gällande lagstiftning vid tidpunkten för mottagen materiel är uppfylld, att *kravställarens* egna systemsäkerhetskrav är uppfyllda samt att det tekniska systemet erbjuder betryggande säkerhet för den verksamhet som ska bedrivas.

Systemsäkerhetsgodkännandet (SSG) innehåller *kravställarens* eget ställningstagande, som förutsätter att materieldokumentation och verksamhetsregler följs när det tekniska systemet tas i bruk. *Kravställarens* eget ställningstagande baseras på genomförd systemsäkerhetsvärdering med *beställarens Systemsäkerhetsdeklaration* (SSD) som grund. S*ystemsäkerhetsgodkännandet* (SSG) är giltigt för tillåtna konfigurationer, inklusive de ändringsbara parameterintervallen, av det tekniska systemet. Om ändring (modifiering) sker kan ett nytt *Systemsäkerhetsgodkännande (*SSG) behöva utfärdas.

Som underlag för *kravställarens* egen systemsäkerhetsvärdering, med dess argument och belägg, ligger alla de systemsäkerhetsaktiviteter som genomförts av både *konstruktören* och *beställaren* under det tekniska systemets utveckling. Det sammanställda underlaget för *Systemsäkerhetsgodkännandet* (SSG) dokumenteras oftast i en *Systemsäkerhetsrapport* (SAR) tillsammans med en *Risklogg* (RL). I S*ystemsäkerhetsgodkännandet* (SSG) hänvisas till dessa dokument och eventuellt till annan riskdokumentation.

Systemsäkerhetsgodkännandet (SSG) kan även innehålla restriktioner, vilka är temporära inskränkningar i det tekniska systemets tillåtna användning, för att

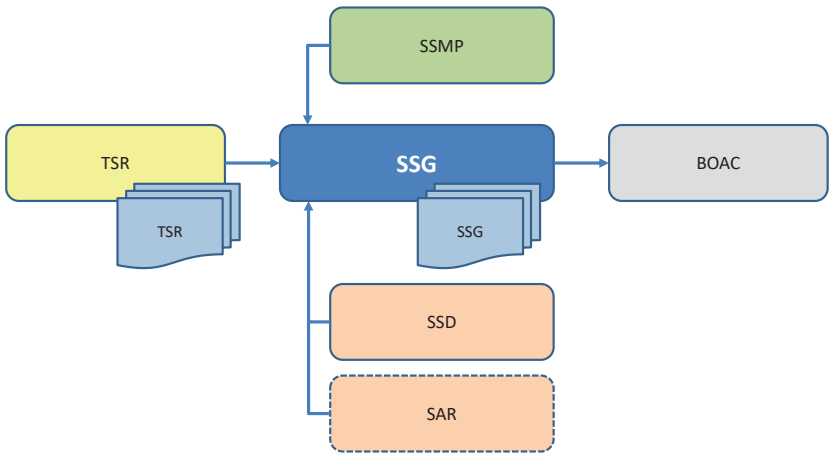
tillfälligt hantera en viss kvarstående olycksrisk och därigenom innehålla ställda krav på systemsäkerhet.

Systemsäkerhetsgodkännandet (SSG) undertecknas av behörig person hos *kravställaren*. För omfattning och innehåll i *Systemsäkerhetsgodkännandet* (SSG), se avsnitt 17.5.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsgodkännande* (SSG) utgörs av *Handhavande och utbildning* (TSR) och *Systemsäkerhetsledningsplanen* (SSMP) samt *beställarens Systemsäkerhetsdeklaration* (SSD) och vid behov *kravställarens* egen *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL).

Utdata är *Systemsäkerhetsgodkännande* (SSG). Den ger indata till *Beslut om användning, central nivå* (BOAC).



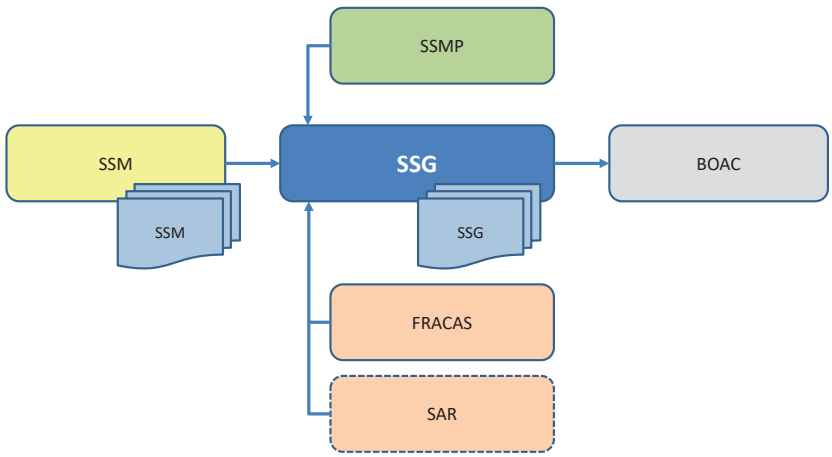
Bilaga 3, bild 43 *Systemsäkerhetsgodkännande (SSG) baserat på Systemsäkerhetsdeklaration (SSD).*

I de fallen *kravställaren* mottar *Systemsäkerhetsmeddelanden* (SSM) kan dessa kräva ändringar (modifieringar) av tekniska system och att nya systemsäkerhetsbeslut från *beställare* och *konstruktör* behöver utfärdas.

Indata till aktiviteten *Systemsäkerhetsgodkännande* (SSG) utgörs av *Systemsäkerhetsmeddelanden* (SSM) och *Systemsäkerhetsledningsplan* (SSMP) samt data ur

Felrapporteringssystem (FRACAS) och vid behov *kravställarens* egen *Systemsäkerhetsrapport* (SAR) med *Risklogg* (RL).

Utdata är *Systemsäkerhetsgodkännande* (SSG). Den ger indata till *Beslut om användning, central nivå* (BOAC).



Bilaga 3, bild 44 *Systemsäkerhetsgodkännade(SSG) baserat på Systemsäkerhetsmeddelanden (SSM).*

S55 – Systemsäkerhetsmeddelande (SSM)

Syfte och aktivitetsbeskrivning

Syftet med aktiviteten *Systemsäkerhetsmeddelande* (SSM) är att den aktör som vill informera om en säkerhetsbrist i ett tekniskt system eller produkt, eller om brister och felaktigheter i dess användning, underhåll eller hantering, kan göra detta utan att återta ett utfärdat systemsäkerhetsbeslut.

Den engelska benämningen är *System Safety Announcement* (SSM) och utdata/dokumentation är *System Safety Announcement* (SSM). Den svenska benämningen på utdata/dokumentation är *Systemsäkerhetsmeddelande* (SSM).

Genom att utfärda ett *Systemsäkerhetsmeddelande* (SSM) till *kravställaren* kan aktuell aktör skaffa sig rådrum för att genomföra initial beredning och föreslå åtgärder såsom ändring (modifiering), ändring i övrig dokumentation eller införande av restriktion. Ett *Systemsäkerhetsmeddelande* (SSM) gäller till dess att säkerhetsbristen är hanterad.

Om flera olika händelser eller observationer finns för samma tekniska system eller produkt rekommenderas att ett *Systemsäkerhetsmeddelande* (SSM) utfärdas per observation. Detta förenklar administrationen vid beslut om att säkerhetsbristen är hanterad.

Om ett S*ystemsäkerhetsmeddelande* (SSM) innebär att information för att förtydliga, upplysa eller påminna användaren om förhållanden med koppling till avsedd användning eller underhåll, viss hantering, förändrat användningssätt inklusive normglidning eller att verksamhetsregler behöver skärpas, kan ärendet stängas av ordförande i *Arbetsgrupp för systemsäkerhet* (SSWG), utan att nya systemsäkerhetsbeslut utfärdas.

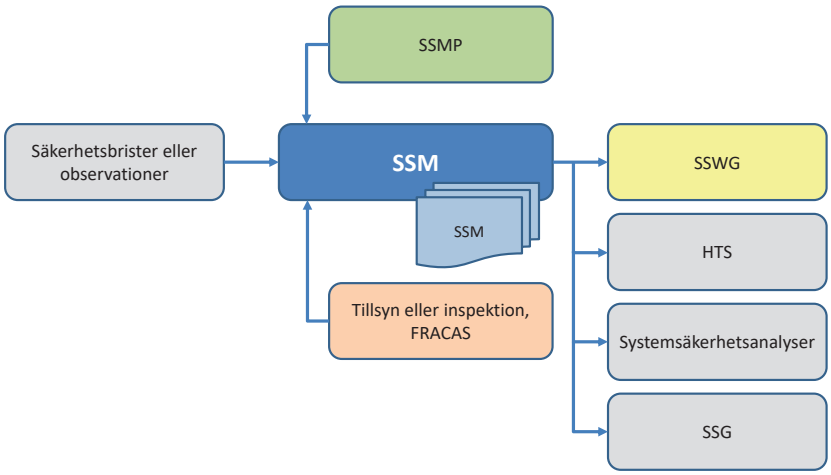
Om ett *Systemsäkerhetsmeddelande* (SSM) innebär att en ändring (modifiering) behöver genomföras för att åtgärda säkerhetsbristen behöver nya systemsäkerhetsbeslut utfärdas.

Ett *Systemsäkerhetsmeddelande* (SSM) kan återtas av utfärdaren om säkerhetsbristen inte längre anses vara aktuell. Ett sådant återtagande dokumenteras av ordförande i *Arbetsgrupp för systemsäkerhe*t (SSWG) i protokoll eller mötesanteckningar.

Indata, utdata och flödesbild

Indata till aktiviteten *Systemsäkerhetsmeddelande* (SSM) utgörs av *beställarens* eller *konstruktörens* kännedom om säkerhetsbrister eller av observationer och *Systemsäkerhetsledningsplan* (SSMP). Indata kan även utgöras av rapporter från tillsyn eller inspektioner eller data ur *Felrapporteringssystem* (FRACAS).

Utdata är *Systemsäkerhetsmeddelande* (SSM). Den ger indata till *Arbetsgrupp för systemsäkerhet* (SSWG) för beredning av ärendet.



Bilaga 3, bild 45 Systemsäkerhetsmeddelande (SSM).

Ett *Systemsäkerhetsmeddelande* (SSM) bör minst omfatta följande:

- Identifiering av tekniskt system eller produkt
- Analys av det inträffade eller det observerade
- Riskbedömning
- Förslag till rekommendationer (exempelvis användningsförbud)

Redaktionell information

Revideringen av Handbok Systemsäkerhet har genomförts i syfte att effektivisera och modernisera systemsäkerhetsverksamheten vid Försvarsmakten och FMV. Den föregående versionen av handboken har använts dels i materielprojekt vid Försvarsmakten, FMV, industri och konsultföretag både nationellt och internationellt, dels vid FMV Systemsäkerhetskurs. Det har då framkommit ett sammantaget stort behov av att omarbeta handbokens innehåll. Vidare har en ny version av MIL-STD-882 givits ut.

SÄKINSP gav FMV i uppdrag att lämna förslag till en ny Handbok Systemsäkerhet i uppdraget ”Samordning Systemsäkerhet 2017–2019” med fortsättning i uppdraget ”Samordning Systemsäkerhet 2020–2022”.

Det huvudsakliga redaktörsarbetet har utförts av FMV.

Arbetsgrupp vid FMV:

Lars Lange, Projektledare
Mikael Lindbergh, Vice projektledare
Bo Höjdefors
Johan Niemi
Peter Djervbrant

Områdesexperter:

Martin Dalaryd
Jan Jacobson
Pär-Anders Wallentin

HKV PROD konstituerade en Försvarsmaktsgemensam styrgrupp i september 2018, med C RPE MTRL Joakim Sellén som ordförande, för att styra arbetsgruppen vid FMV. Styrgruppen har genomfört 15 möten.

Förankring av handbokens utformning och sakinnehåll har genomförts av FMV tillsammans med en referensgrupp om cirka 45 personer vilka representerade Försvarsmakten, FMV, industri och konsultföretag. Relevant innehåll i föregående handbok, Handbok Systemsäkerhet 2011, har omhändertagits i denna utgåva.

Det första referensgruppsmötet genomfördes den 22 november 2018 (ca 40 deltagare) med syfte att erhålla synpunkter och erfarenheter från tillämpningen av Handbok Systemsäkerhet 2011 samt för att säkerställa handbokens bredd, djup och kvalitet så att den nya utgåvan skulle bli väl förankrad hos samtliga aktörer.

Det andra referensgruppsmötet genomfördes den 21 november 2019 (ca 35 deltagare) där deltagarna fick ett första utkast av handboken presenterat med förslag på disposition samt metodiken för livscykel-, olycksrisk- och vägvalsmodellen. Referensgruppen fick därefter möjlighet att studera innehållet och återkomma med synpunkter under första kvartalet 2020.

Arbetsgruppen bearbetade inkomna synpunkter och tog fram ett bredare och mer innehållsrikt förslag till ny handbok, vilken sedan skickades ut på formell remiss inom FM och FMV under andra kvartalet 2021. Arbetsgruppen omhändertog synpunkterna samt hade en löpande avstämning med representanter ur referensgruppen samt med FLYGI och SÄKINSP.

En slutremiss inom Försvarsmakten och FMV genomfördes under första kvartalet 2022. Remissen föranledde endast mindre justeringar och förtydliganden.

C RPE MTRL tillika styrgruppens ordförande, Joakim Sellén, tillsammans med representanter från HKV PROD och FMV, föredrog Handbok Systemsäkerhet 2022 för C RPE, Jonas Lotsne, den 20 maj 2022.

Försvarsmaktens publikationssamordnare har tillstyrkt fastställande den 22 juni 2022.

Bildförteckning

I denna publikation förekommer inga bilder med verkshöjd.

Källförteckning

I denna version av handboken har följande källor använts.

Källor utanför Försvarsmakten

- EU-förordning 1907/2006, Registration, evaluation, authorization and restriction of chemicals (REACH)
- EU-förordning 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter
- EU-förordning 1272/2008, Classification, labelling and packaging of substances and mixtures (CLP)
- EU-direktiv 2006/42/EC om maskiner
- EU-direktiv 2013/35/EU om elektromagnetisk kompatibilitet (EMCD)
- EU-direktiv 2014/90/EU om marin utrustning (MED)
- EU-direktiv 2021/555/EU om kontroll av förvärv och innehav av vapen (kodifiering)
- Lågspänningsdirektivet (LVD; direktiv om elektrisk utrustning) 2014/35/EU
- Radioutrustningsdirektivet (RED) 2014/53/EU
- Miljöbalk (SFS 1998:808)
- Arbetsmiljölag (SFS 1977:1160)
- Elsäkerhetslag (SFS 2016:732)
- Fartygssäkerhetslag (SFS 2003:364)
- Fordonsförordning (SFS 2009:211)
- Fordonslag (SFS 2002:574)
- Lag (SFS 2010:1011) om brandfarliga och explosiva varor (LBE)
- Lag (SFS 2016:768) om marin utrustning
- Luftfartslag (SFS 2010:500)
- Produktansvarslag (SFS 1992:18)
- Produktsäkerhetslag (SFS 2004:451)
- Förordning (SFS 2003:440) om säkerheten på örlogsfartyg
- Förordning (SFS 2007:936) om folkrättslig granskning av vapenprojekt
- Förordning (SFS 2014:1039) om marknadskontroll av varor och närliggande tillsyn

- Förordning (SFS 2016:770) om marin utrustning
- Luftfartsförordning (SFS 2010:770)
- Militärtrafikförordning (SFS 2009:212)
- AFS 2006:4, Arbetsmiljöverkets föreskrifter om användning av arbetsutrustning
- AFS 2008:3, Arbetsmiljöverkets föreskrifter och allmänna råd om maskiner
- AFS 2020:1, Arbetsmiljöverkets föreskrifter om arbetsplatsens utformning
- PTSFS 2016:5, Post- och telestyrelsens föreskrifter om krav mm på radioutrustning
- TSFS 2011:91, Transportstyrelsens föreskrifter och allmänna råd om arbetsmiljö på örlogsfartyg
- TSFS 2016:22, Transportstyrelsens föreskrifter och allmänna råd om bilar och släpvagnar som dras av bilar och som tas i bruk den 1 juli 2010 eller senare
- TSFS 2016:81, Transportstyrelsens föreskrifter om marin utrustning
- TSFS 2019:19, Transportstyrelsens föreskrifter och allmänna råd om drift av godkänd flygplats
- DEF STAN 00-055 Requirements for Safety of Programmable Elements (PE), Software etc in Defence Systems (UK)
- DEF STAN 00-056:Part 1 Safety Management Requirements for Defence Systems, Issue 7, 2017 (UK)
- DEF STAN 00-251:Part 3 Human Factors Integration for Defence Systems: Human Factors System Requirements, 2016 (UK)
- DO-178C/ED-12C Software Considerations in Airborne Systems and Equipment Certification, 2012
- DO-254/ED-80 Design Assurance Guidance for Airborne Electronic Hardware, (Functions that are allocated to hardware), 2016
- FSD 9251 Integration av humanfaktorer i försvarssystem, 2018
- GEIA-STD-0010A Standard Best Practice for System Safety Program Development and Execution, 2015
- IEC 60601 Elektrisk utrustning för medicinskt bruk (serie)
- IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems (serie)
- IEC 80601 / ISO 80601 Elektrisk utrustning för medicinskt bruk – Särskilda krav (serie)

- ISO/IEC/IEEE 15288 Systems and software engineering – System life cycle processes
- MIL-STD-882E Department of Defense Standard Practise System Safety, 2012
- MIL-STD-1472H Department of Defense Design Criteria Standard, Human Engineering, 2020
- MIL-STD-46855A Department of Defence Standard Practice: Human Engineering Requirements for Military Systems, Equipment and Facilities, 2011
- SAE ARP 4754A Guidelines for Development of Civil Aircraft and Systems, 2010
- SAE ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, 1996
- SS-EN 60945 Marin navigerings- och radiokommunikationsutrustning - Allmänna fordringar - Provningsmetoder och erforderliga provningsresultat
- SS-EN 61508 Säkerhetsfordringar på elektriska, elektroniska och programmerbara elektroniska säkerhetskritiska systems funktion (serie)
- SS-EN IEC 60204-1 Maskinsäkerhet – Maskiners elutrustning – Del 1: Allmänna fordringar
- SS-EN ISO 12100:2010 Maskinsäkerhet – Allmänna konstruktionsprinciper – Riskbedömning och riskreducering
- SS-EN ISO 13850:2015 Maskinsäkerhet – Nödstoppsutrustning – Konstruktionsprinciper
- SS-EN ISO 14971:2020 Medicintekniska produkter – Tillämpning av ett system för riskhantering för medicintekniska produkter
- SS 2222 Teknisk dokumentation – Klassificering av fordringar i produktionsunderlaget.
- STANAG 2310 Technical Performance Specification Providing for the Interchangeability of 7.62 mm x 51 Ammunition, 2020
- STANAG 4297/AOP-15 Guidance on the Assessment of the Safety and Suitability for Service of Non-Nuclear Munitions for Nato Armed Forces, 2001
- STANAG 4518, edition 1 Safe disposal of munitions, design principles and requirements and safety assessment, 2001

- BAAINBw, System Safety Demonstration Manual (01/04/2014), Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (Tyskland)
- FMV Handbok EMMA (Handbok Elektromagnetisk miljö användarhandbok)
- FMV Handbok för Fordonssäkerhet (H FordonSäk)
- FMV Handbok för Programvara i säkerhetskritiska tillämpningar (H ProgSäk)
- FMV Handbok för Säkra fältmässiga arbetsplatser (H SFAPL)
- FMV Handbok Säkra elektriska produkter och system (H SEPS)
- FMV Handbok Vapen- och Ammunitionssäkerhet (H VAS)
- Räddningsverket Handbok för riskanalys, Utgivningsår 2003, Beställningsnummer: U 30-626/02, ISBN 91-7253-178-9
- SEES Handbok Miljötålighetsteknik (Swedish Environmental Engineering, Society, Environmental Engineering Handbook)

Källor inom Försvarsmakten

- Försvarsmaktens beslutsmodell tekniska system (FM BMTS), FM2017-22065:1
- Samordningsöverenskommelse SAMO (FM–FMV) FM2019-4243:4, 19FMV5660-1:1

Regelstyrning som påverkat innehållet i denna handbok

FFS	FFS 2019:10, Försvarsmaktens föreskrifter om militär luftfart
Handbok	Målsättningsarbete förband 2011, gällande från och med 2011-01-01
Handbok	Målsättningsarbete Tekniska system 2015, gällande från och med 2015-04-01
Handbok	Styrande dokument och handböcker 2021, gällande från och med 2021-11-01
Handbok	Förnödenhetsavveckling 1997, gällande från och med 1997-10-01

Handbok	Förvaring och transport av ammunition och övriga explosiva varor del 1 2011, gällande från och med 2011-01-01
Handbok	Åtgärder mot brand- och explosionsfara, vattenförorening samt kemisk hälsopåverkan från brandfarliga varor 2014, gällande från och med 2014-09-01

ANTECKNINGAR

ANTECKNINGAR

ANTECKNINGAR

Försvarsmakten ska uppfylla krav på arbetsmiljö och säkerhet för Försvarsmaktens personal samt säkerhet för tredje person, egendom och yttre miljö. Materielen ska uppfylla lagstiftningen och samtidigt inneha kravställda prestanda.

Försvarsmaktens systemsäkerhetsverksamhet syftar till att olycksrisker i förbandsverksamheten hålls så låga som möjligt. Härvid ställs systemsäkerhetskrav på materiel som anskaffas eller modifieras.

Handboken beskriver Försvarsmaktens process från målsättning till avveckling samt redogör för andra aktörers systemsäkerhetsarbete.

FÖRSVARSMAKTEN

107 85 Stockholm
www.forsvarsmakten.se

H SYSTSÄK 2022
M7739-352022
Versionsnr: 3.0 Ä0