TC Led Handlingsregel nr 102 - Process systemsäkerhet Led

I TC Led Handlingsregel nr 102 (HR 102 ver 4) ges en övergripande beskrivning av hur systemsäkerhetsprocessen ska tillämpas inom TC Led ansvarsområde. Handlingsregeln omfattar systemsäkerhet samt integration av humanfaktorer (HFI) och är baserad bland annat på FMV VHL, H SystSäk 2022, gällande delegeringsordningar, FMV Designregel Integration av humanfaktorer och användbarhet i försvarssystem, samt Samordningsavtal FM – FMV.

Handlingsregel 102 är främst tänkt som hjälp vid arbete med systemsäkerhet och HFI inom området Led genom att på en plats samla och beskriva de viktigare kraven gällande hantering av systemsäkerhet och HFI. Kraven återfinns främst i olika andra styrande regelverk, beslut samt riktlinjer och kompletteras här med TC Led styrningar samt förtydliganden.

I enlighet med H SystSäk 2022 presenteras Vägvalsmodellen som den metodik som ska användas vid val av systemsäkerhetsaktiviteter samt vid riskhantering inför Systemsäkerhetsdeklaration. För systemsäkerhetsverksamhet inom TC Led ansvarsområde bedöms Vägval 1 och 7 normalt vara relevanta.

Från denna version av HR 102 omhändertas även området HFI. HFI är en systematisk process för att med framgång kunna integrera försvarssystemets komponenter (människor, processer och teknik) med varandra och därmed optimera systemeffekten för att uppnå önskad förmåga. HFI-arbetet har processmässigt stora likheter med traditionellt systemsäkerhetsarbete, och TC Led har valt att integrera HFI-aspekter i SSD för att på ett effektivt sätt omhänderta de krav FMV har att uppfylla inom HFI-området.

Handlingsregel 102 samlar också viktigare dokumentinstruktioner/mallar som är framtagna för användning inom TC Led ansvarsområde, det vill säga bilagor med anvisningar för framtagande av SSMP, SSD, PHL samt ”Deklaration Mindre ändring systemsäkerhet”.

Handbok Systemsäkerhet (H SystSäk 2022) fastställdes att gälla från och med 2022-09-01. Uppdrag som tecknats mot Försvarsmakten innan detta datum levereras enligt H SystSäk 2011 om inte omförhandling genomförts. Systemsäkerhetsarbeten som påbörjats enligt tidigare version av HR 102 kan under en övergångsperiod använda dessa tidigare principer.

Processer i denna Handlingsregel som rör vidmakthållandeskedet är inriktade för system som FMV har designansvar för eftersom de inte är överlämnade samt system där FM har beställt relevant vidmakthållandeverksamhet från FMV.

**Innehållsförteckning**

[TC Led Handlingsregel nr 102 - Process systemsäkerhet Led 1](#_Toc137648507)

[1 Bakgrund 5](#_Toc137648508)

[1.1 Försvarsmaktens livscykelmodell för tekniska system 5](#_Toc137648509)

[1.2 FMV:s roller i anskaffningsprocessen 5](#_Toc137648510)

[1.3 Krav och beslut 6](#_Toc137648511)

[1.4 TC Led Designansvar 7](#_Toc137648512)

[2 Systemsäkerhet och HFI – övergripande beskrivning 8](#_Toc137648513)

[2.1 Systemsäkerhet och HFI 8](#_Toc137648514)

[2.2 Systemsäkerhetsprocessen 8](#_Toc137648515)

[2.3 HFI-risker 10](#_Toc137648516)

[2.4 Övrig lagstiftning 11](#_Toc137648517)

[3 Framtagning av Systemsäkerhetsunderlag 11](#_Toc137648518)

[3.1 Planering och kravsammanställning 11](#_Toc137648519)

[3.2 Vägvalsmodellen 12](#_Toc137648520)

[3.3 Systemsäkerhets- och HFI-värdering 12](#_Toc137648521)

[3.4 Riskanalys 13](#_Toc137648522)

[3.5 Vägval 1: COTS och CE-märkta produkter 14](#_Toc137648523)

[3.6 Vägval 7: Fullständigt systemsäkerhetsarbete 15](#_Toc137648524)

[3.7 Övriga vägval 18](#_Toc137648525)

[3.8 Systemsäkerhetsdeklaration 19](#_Toc137648526)

[4 Hantering av ändringar 21](#_Toc137648527)

[4.1 Allmänt om ändring 21](#_Toc137648528)

[4.2 Bedömning av systemsäkerhets- och HFI-aspekter 22](#_Toc137648529)

[4.3 Mindre ändring systemsäkerhet 23](#_Toc137648530)

[4.4 Ändring inom ram 23](#_Toc137648531)

[5 Luftfartsprodukter 23](#_Toc137648532)

[6 Flygsäkerhetspåverkande risker i övriga system 24](#_Toc137648533)

[7 System av system 24](#_Toc137648534)

[8 Återtagande av materiel från Försvarsmakten 25](#_Toc137648535)

[9 Språk 25](#_Toc137648536)

[10 Beslut 26](#_Toc137648537)

**Terminologi**

Följande terminologilista är gemensam för huvuddokument och bilagor.

|  |  |
| --- | --- |
| **Beteckning** | **Betydelse** |
| Användbarhet | Den utsträckning till vilken en specifik användare kan använda en produkt för att uppnåspecifika mål, med ändamålsenlighet, effektivitet och tillfredsställelse i ett givetanvändningssammanhang (källa FMV H HFI samt ISO 9241-11:1998). |
| AFS | Arbetsmiljöverkets författningssamling |
| BOAC, BOAL | Försvarsmaktens Beslut om användning på central resp. lokal nivå. |
| CI | Chefsingenjör inom FMV |
| COTS | ”Commercial off the Shelf”; hyllvara, färdig produkt. I systemsäkerhetsprocessen beteckning på en klassning av civilt godkända och certifierade system (se kap. 3.5). |
| Delegeringsordning | Gällande delegeringsordning vid FMV, fastställd i t.ex. ”Besluts- och samrådsmatris inom TC Led ansvarsområde”. |
| DoC | Declaration of Conformity; Försäkran om överensstämmelse, t.ex. gentemot specificerat EG-regelverk (CE-märkning m.m.) |
| FM | Försvarsmakten |
| HFI | Human Factors Integration; integrering av humanfaktorer. En systematisk process för att med framgång integrera systemets komponenter (människor, processer och teknik) för att uppnå önskad förmåga (källa FSD 9251). För HFI-risk, se kap. 2.3. |
| HFI-krav | Krav avseende humanfaktorer och användbarhet kopplade till att materiel, utrustning och tekniska system ska passa all personal, samt för att uppnå specifika mål, med ändamålsenlighet, effektivitet och tillfredsställelse i ett givet användningssammanhang. Kan indelas i användarkrav, processkrav och tekniska krav. Se FMV H HFI samt FSD 9251. |
| HFI-mål | Mål avseende humanfaktorer och användbarhet som ställts på en eller flera produkter och system. HFI-mål kan uttryckas i form av en riskmatris med tillåtna risknivåer. HFI-mål ingår i denna handlingsregel i begreppet ”säkerhetsmål”. |
| Luftfartsprodukt | För definition av luftfartsprodukt, se RML-G. För definition av ”luftfartsprodukt inom TC Led ansvarsområde”, se gällande utgåva av TC Led Handlingsregel nr 5. Kortfattat: Teknisk utrustning/system inom TC Led ansvarsområde, som omfattas av TC Led flygsäkerhetsprocess och ingår i en flygsäkerhetspåverkande funktionskedja. |
| MOTS | ”Military off the Shelf”. Kommersiellt men inte allmänt tillgängliga färdiga produkter såsom hårdvara eller programvara, för militär användning. |
| OSG | Oberoende systemgranskningsfunktion vid VerkO LedM gällande system- och flygsäkerhet, under ansvar av Systemgranskningsledare inom området. |
| Produkt | Sådan vara som ”säljs över disk”/är kommersiellt tillgänglig och säkerhetsmässigt är konstruerad för att uppfylla produktsäkerhets- och produktansvarslagarna samt tillämpliga EU-direktiv (se H SystSäk). I systemsäkerhetsprocessen beteckning på en vara före eventuell klassning som COTS eller Trivial materiel. |
| PRL | Produktledare vid produktdomän inom TC Led ansvarsområde. |
| RAIDO | Risks, Assessments, Issues, Dependencies, and Opportunities - Risker, antaganden, problem, beroenden och möjligheter inom Human Factors Integration-området. |
| Restriktion | Tillfällig inskränkning i det tänkta nyttjandet (definition enligt H SystSäk). Restriktioner finns för kvarstående olycksrisker där riskreducerande åtgärder ännu inte är införda. |
| RFP | Request For Proposal; förfrågningsunderlag från beställare. |
| Riskkälla | Något som kan leda till skada på person, egendom eller yttre miljö. Översättning av engelskans ”hazard” (se H SystSäk). |
| SAMO | Samordningsavtal mellan Försvarsmakten (FM) och Försvarets materielverk (FMV), för övergripande samordning av relationer och rutiner mellan FM och FMV. |
| SMS | Systemmålsättning. SMS 1 beskriver en systemlösning och tas fram i kravställarens konceptskede inför beslut om upphandling. SMS 2 utarbetas inför beslut om produktion och inkluderar systemsäkerhetskrav.Ska inte förväxlas med Safety Management System. |
| SSG | Systemsäkerhetsgodkännande (FM från 2019, tidigare FMV) (tidigare även förkortat SS) |
| SSD | Systemsäkerhetsdeklaration (FMV) |
| SSMP | System Safety Management Plan. Övergripande systemsäkerhetsledningsplanering vid FMV Led. Även Försvarsmakten i rollen som kravställare ska utarbeta en Systemsäkerhetsledningsplan för ett produktområde. |
| SSPP | System Safety Program Plan. Systemsäkerhetsplanering hos en leverantör eller på projektnivå inom FMV roll som beställare, se H SystSäk. |
| SSV | Systemsäkerhetsvärdering; eng. System Safety Evaluation (SSV) |
| System | Uttrycket system används i detta dokument som en förenklande term för de tekniska produkter och system inom TC Led ansvarsområde som omfattas av systemsäkerhets- och/eller godkännandeprocesser. |
| Systemsäkerhets­beslut | Samlingsbegrepp för Systemsäkerhetsutlåtande (SCA), Systemsäkerhetsdeklaration (SSD) samt Försvarsmaktens Systemsäkerhetsgodkännande (SSG), vilka är beslut som överräckes ifrån en roll till nästa.Bör inte förkortas så att det förväxlas med Systemsäkerhetsbedömning (SSB), en aktivitet som genomförs före kravställning, se H SystSäk.Beslutsdokumentet som tidigare betecknades ”Systemsäkerhetsbeslut Justering/Smärre ändring” är ersatt av TC Led ”Deklaration Mindre ändring systemsäkerhet”. |
| Systemsäkerhetsmål | Mål uppsatta för ett produktområde eller tekniskt system för att uppfylla Tolerabel risknivå. Mål uttrycks normalt i form av en riskmatris med tillåtna risknivåer. |
| Säkerhetsmål | Säkerhetsmål är den övergripande inriktningen avseende vilken tolerabel risk en verksamhet kan acceptera. Inbegriper mål och krav inom HFI- och systemsäkerhetsområdena. |
| TC Led | Teknisk Chef Ledningssystem vid FMV. |
| TC Led ansvars­område | TC Led ansvarsområde innefattar bland annat tekniskt designansvar och teknisk styrning inom området Ledningssystem vid FMV.  |
| TC Led HR | TC Led Teknisk Handlingsregel/Handlingsregler |
| Trivial materiel | Systemsäkerhetsrelaterad klassning av enkla produkter som används isolerat, såsom necessär, sportskor och som inte omfattas av lag eller författning med militärt undantag. |
| VerkO LedM | Verksamhetsområde Ledningssystemmateriel inom FMV. |
| VHL | FMV Verksamhetsledningssystem |
| Ändring | Med ändringar avses dels modifieringar av tekniska system, dels förändringar av t.ex. materieldokumentation, underhåll, utbildning, förrådshållning eller transportsätt för det tekniska systemet. I denna handlingsregel är påverkan inom systemsäkerhets- och HFI-området avgörande för klassning av ändring. |

# Bakgrund

## Försvarsmaktens livscykelmodell för tekniska system

För tekniska system använder Försvarsmakten en livscykelmodell, som omfattar följande skeden:

* Koncept
* Utveckling (Förberedelse och Anskaffning)
* Produktion
* Vidmakthållande
* Avveckling

Systemsäkerhetsarbete behöver genomföras inom ramen för de olika livscykelskedena. För att förflytta ett tekniskt system eller produkt mellan livscykelskeden krävs bland annat systemsäkerhetsdokumentation.

Försvarsmakten kan inneha samtliga roller i systemsäkerhetsprocessen, d.v.s. agera som Kravställare, Beställare, Systemintegratör och Konstruktör.

Försvarsmakten ska säkerställa relevant kravställning gällande användbarhet och HFI.

## FMV:s roller i anskaffningsprocessen

FMV kan verka i rollerna Beställare och Systemintegratör. FMV kan biträda Försvarsmakten i arbetet redan under Försvarsmaktens utvecklingsskede.

**FMV i rollen som beställare** anskaffar tekniska system och produkter från olika konstruktörer (här även kallade leverantörer) såsom utvecklande industrin, annan stat, Försvarsmaktens verkstäder eller Fortifikationsverket. FMV Led tar i denna roll fram en systemsäkerhetsplan (SSMP) som på strategisk nivå beskriver det systemsäkerhetsarbete som ska genomföras för tekniska system och produkter. FMV SSMP utformas utifrån Försvarsmaktens Systemmålsättning (SMS 2) samt Försvarsmaktens SSMP.

I samband med systemöverlämning (SÖL) till Försvarsmakten överlämnas från FMV en Systemsäkerhetsdeklaration (SSD) med nödvändig säkerhetsbevisning – se Fig. 1.

**FMV i rollen som systemintegratör** säkerställer FMV samfunktion mellan tekniska system till ett ”system av system” i de fall sekretess föreligger eller då en annan leverantör/konstruktör inte kan ta detta ansvar. FMV genomför i denna roll det systemsäkerhets- och HFI-arbete som behöver genomföras för att säkerställa samfunktion mellan olika tekniska system till ett ”system av system”. Vid de tillfällen FMV ansvarar för integrationen av olika delsystem ska FMV, utöver SSD, även fastställa en Systemsäkerhetsrapport (SAR) och ett säkerhetsutlåtande (SCA) för det integrerade systemet.

FMV ska i sitt arbete med användbarhet och HFI samverka med Försvarsmakten i erforderlig omfattning. Försvarets materielverks HFI- och användbarhetsarbete ska genomföras enligt ”Designregel Integration av humanfaktorer och användbarhet i försvarssystem”.



Fig. . Roller, krav och beslut för tekniska system och produkter,
med FMV LedM i rollen som Beställare (bild efter H SystSäk).

## Krav och beslut

FMV ansvarar för att den verksamhetsprocess som tillämpas för utförande av Försvarsmaktens beställningar, såväl inom FMV som hos berörda leverantörer, även omfattar HFI-verksamhet och systemsäkerhetsverksamhet för person, egendom och miljö. FMV följer härvid de föreskrifter inom systemsäkerhetsområdet samt HFI-området som Försvarsmakten fastställer. Systemsäkerhetsarbetet inom FMV Led integreras med HFI arbete och ska därmed följa Handbok Systemsäkerhet (H SystSäk) samt Handbok Human Factors Integration (H HFI)[[1]](#footnote-1).

Försvarsmakten ska i målsättningar och kravdokument eller i uppdrag avseende statusanalys eller motsvarande ange HFI- och systemsäkerhetskrav kompletterat med krav avseende risknivå i form av Systemsäkerhetsmål. I konceptskedet för ett planerat system utarbetar Försvarsmakten i rollen som kravställare en första Systemmålsättning (SMS 1). Efter beslut om utveckling fastställs en Systemsäkerhetsledningsplan (FM SSMP) som utgår från framtagna säkerhetsmål, ur vilka systemsäkerhetsmål definieras. Systemsäkerhetsmålen inkluderar krav på Tolerabel risknivå (TR) uttryckt i riskmatriser.

Med systemsäkerhetsmålen som grund kan Systemsäkerhetskrav (SSK) definieras baserat på EU-rätt, svensk lagstiftning, standarder, andra regelverk, Designregler samt konstruktionskrav. I en andra Systemmålsättning (SMS 2) beskrivs den systemlösning som fyller behovet, och antagna Systemsäkerhetskrav (SSK) anges.

Försvarsmaktens SSMP och SMS 2 utgör den systemsäkerhetsdokumentation som behövs för att gå in i utvecklingsskedet, bestående av förberedelse och anskaffning. En tydlig plan med sammanställning av definierade krav ger en god grund för det fortsatta säkerhetsarbetet hos såväl FMV som leverantör.

FMV LedM som beställare utvecklar en egen SSMP som beskriver den interna övergripande strategiplaneringen för systemsäkerhetsarbetet, för ett eller flera tekniska system. Ett dokument kan omfatta såväl denna planering som uttryckta säkerhetsmål, vilket inbegriper mål och krav inom HFI- och systemsäkerhetsområdena. Se vidare kap. 3.1.

I de fall där systemsäkerhets- och/eller HFI-krav och mål är otydliga, behöver i första hand Försvarsmaktens kravställning inhämtas. I andra hand ansätts HFI- och systemsäkerhetsmål vid FMV, det vill säga krav och risknivåer, varefter verifierbar acceptans inhämtas från Försvarsmakten. I tredje hand ansätts HFI- och systemsäkerhetsmål vid FMV, och delges Försvarsmakten genom tydlig information i överlämnad systemsäkerhetsdokumentation.

Från och med fastställandet av denna utgåva av TC Led HR 102 kompletteras SSD med ett uttalande att även HFI och användbarhet har analyserats och omhändertagits. Det totala systemsäkerhetsarbetet hos FMV och leverantör, inklusive HFI, resulterar i FMV:s Systemsäkerhetsdeklaration (SSD). Denna deklaration utgör ett entydigt uttalande från FMV att det tekniska systemet är säkert under givna förutsättningar, d.v.s. uppnår ställda säkerhets- och HFI-mål, samt att såväl lagkrav som ställda HFI- och systemsäkerhetskrav är uppfyllda.

FMV:s Systemsäkerhetsdeklaration (SSD) utgör grund för Försvarsmaktens Systemsäkerhetsgodkännande (SSG), vilket i sin tur utgör underlag inom systemsäkerhetsområdet för utgivande av BOAC/BOAL (Beslut Om Användning på central respektive lokal nivå). Se vidare gällande Samordningsavtal mellan Försvarsmakten och Försvarets materielverk, samt H SystSäk och H HFI.

## TC Led Designansvar

FMV utövar tekniskt designansvar 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).

Tekniskt designansvar vid FMV innebär att för ett tekniskt system:

* Fastställa teknisk struktur och konstruktion.
* Fastställa vilken integration som omfattas av viss tillåten konfiguration.
* Säkerställa att denna uppfyller lagkrav, fastställda målsättningar och övriga krav avseende prestanda, funktion, informations- och systemsäkerhet inför överlämning till FM.
* FM kan beställa tjänster som ger FMV TC Led ett visst ansvar även efter överlämning.

Tekniskt designansvar, inklusive teknisk systemledning, innehas normalt av rollen Designansvarig för alla nivåer av tekniska system som levererats till Försvarsmakten.

Industri och leverantör har ett produktansvar och kan ha ett tekniskt designansvar inför anskaffande organisation, men det är normalt den anskaffande organisationen som är tekniskt designansvarig inför Försvarsmakten. Då FMV är leverantör av ett system till Försvarsmakten, innehar alltså FMV som regel rollen som Designansvarig inför överlämning.

Inom sitt ansvarsområde tar FMV TC Led fullt designansvar för systemet inför överlämning. Försvarsmakten har designansvar för efterföljande delar av livscykeln, men kan beställa vissa tjänster av FMV.

# Systemsäkerhet och HFI – övergripande beskrivning

## Systemsäkerhet och HFI

Systemsäkerhet fokuserar på att egenskaperna hos ett tekniskt system inte ska skada personer, miljö eller andra system. HFI handlar om att matcha människa och system, att öka total systemeffekt samt stärka människans förmåga. Försvarsmaktens materiel ska leverera önskad effekt för organisationens verksamhet, gruppens uppgift och enskild individs behov; dessutom ska det vara förhållandevis enkelt att lära sig, handha och reparera.

För tekniska system behöver både systemsäkerhets- och HFI-aspekter beaktas i hela livscykeln. Liksom systemsäkerhetsarbetet syftar till att identifiera och eliminera risker, är det viktigt att i HFI-arbetet hantera risker, problem etc. (se RAIDO) i samtliga livscykelskeden.

Det finns inom FMV olika processer för systemsäkerhet respektive HFI, men i båda processerna finns bland annat krav på strategi- och målsättningsdokument, krav på analys och hantering av risker, samt krav på att inför systemleverans deklarera kravuppfyllnad. På grund av dessa likheter används SSD inom Ledningssystemområdet för att deklarera kravuppfyllnad och riskhantering utifrån både systemsäkerhets- och HFI-aspekter. Ytterligare en anledning är att ett antal HFI-aspekter behöver behandlas och deklareras som systemsäkerhetsrisker, vilket underlättas av en gemensam process.

## Systemsäkerhetsprocessen

H SystSäk redovisar systemsäkerhetsaktiviteter som genomförs alltid respektive selektivt. Inför leverans av ett system redovisas normalt följande aktiviteter:

* Riskhanteringssystem (HTS) redovisas i Riskloggen och/eller SAR.
* Funktionell riskanalys (FHA) redovisas i Riskloggen.
* Riskkälleanalys (PHA) redovisas i Riskloggen.
* System Requirement Hazard Analysis (SRHA) redovisas i SAR.
* System-of-Systems Hazard Analysis (SoSHA) redovisas i förekommande fall i Riskloggen.
* Riskanalys inför avveckling av system (RADS) redovisas i Riskloggen.

Om anvisningar/mallar enligt bilagor till denna HR används, bör samtliga kravställda aktiviteter bli redovisade.

Nedanstående bild (Fig. 2) visar den övergripande systemsäkerhetsprocessen, inklusive HFI-aspekter, anpassad för verksamhet inom TC Led ansvarsområde.



Fig. . Övergripande systemsäkerhetsprocess inom TC Led ansvarsområde.

## HFI-risker

H HFI beskriver nio HFI-domäner: Arbetskraft, Personal, Human Factors Engineering, Omvärldmiljö, Systemsäkerhet, Arbetsrelaterad hälsa, Överlevnad samt Arbets- och boendemiljö.

I en analys av HFI-relaterade utmaningar, risker, antaganden, begränsningar och krav kan två huvudspår urskiljas i relation till systemsäkerhet.

* Det ena spåret är risker som relaterar till ren systemsäkerhet. Exempelvis dåligt utformade reglage medför ökad risk för olycka med person och/eller egendomsskada. Dessa ska omhändertas som vanliga systemsäkerhetsrisker, bland annat genom dokumentation i risklogg.
* Det andra spåret är risker för effektförluster eller skador som inte orsakas av rena systemsäkerhetsbrister och därmed inte normalt omhändertas som systemsäkerhetsrisker. Inom område Led dokumenteras dessa på liknande sätt som systemsäkerhetsrisker, i den mån sådana risker kan identifieras i HFI-delen av PHL. Fortsatt hantering av sådana risker görs i särskilt anpassade delar av riskloggen, enligt särskild anvisning/mall giltig inom TC Led ansvarsområde.

Effektförluster kan bedömas i ekonomiska värden eftersom utebliven effekt innebär att Försvarsmakten inte kan utföra sitt uppdrag på ett optimalt sätt. Här inräknas effektförluster som uppstår då delar av personalstyrkan inte kan använda systemet effektivt beroende till exempel på kön, kroppsutformning eller andra personliga förutsättningar. Minskad effektivitet i systemanvändningen kan uppstå t.ex. av följande orsaker:

* Materiel är svår att handha eller underhålla.
* Användandet kräver lång utbildning.
* Användarnas levnads- eller arbetsmiljö är inte tillfredsställande.
* Grundläggande mänskliga behov uppfylls inte (t.ex. hygien, återhämtning, sömn, integritet, och möjligheter till social interaktion).
* System har en negativ påverkan på personalens motivation och arbetstillfredsställelse.

HFI-domänen Överlevnad hanterar frågor om egenskaper hos ett system som höjer användarnas chanser att överleva olyckor eller möten med motståndaren. Skador på grund av militär bekämpning innebär förluster avseende personal och/eller egendom med värde för Sverige och dess försvar. Även sådana skador kan bedömas i ekonomiska värden. Därtill bedöms skador på egen personal i nivåer från dödsfall till lätt skada. Frågeställningar i en sådan riskanalys belyser t.ex. avvägningar mellan personligt skydd, skydd för det tekniska systemet, och kamouflage. Kostnader för förluster kan bedömas som en följd av ökad risk av fiendens bekämpning.

Det finns exempel på att rena systemsäkerhetsrisker kan stå i motsatsförhållande till HFI-relaterade risker. Ett exempel kan vara belysning till en nödutgång, som behövs ur ett systemsäkerhetsperspektiv men som samtidigt riskerar att avslöja en position för motståndaren. Därmed står en systemsäkerhetsaspekt mot en överlevnadsaspekt inom HFI-området. Sådana överväganden kan underlättas av att riskbedömningen sker inom samma process.

Inom HFI finns också områden där det egna systemet inte rimligen kan omfatta alla konsekvenser, och där i stället det överordnade systemet ska ställa krav på funktion och effektivitet. För att ha en rimlig möjlighet att bedöma konsekvenser i en HFI-analys måste avgränsningar göras och redovisas.

## Övrig lagstiftning

Handbok systemsäkerhet, beställningar, handlingsregler etc. gäller vid arbete med HFI och systemsäkerhet vid FMV. Utöver detta är det FMV skyldighet att följa gällande lagar, förordningar och relevanta föreskrifter. Sådana regler går före handböcker och handlingsregler.

Ett exempel är riskområden som behandlas i föreskrifter om arbetsmiljö, avseende t.ex. krisstöd och risk för psykiska konsekvenser av olyckor. Inom TC Led ansvarsområde ska risk för psykiska skador hanteras i HFI- och systemsäkerhetsarbetet, om inte Försvarsmakten uttryckligen angett annat i beställning till FMV. (Se vidare AFS 1999:7 och AFS 2001:1.)

# Framtagning av Systemsäkerhetsunderlag

## Planering och kravsammanställning

Systemsäkerhetsunderlag är sådan dokumentation som tillsammans utgör *tillräcklig säkerhetsbevisning* för ett system. Sådan säkerhetsbevisning utgör grunden för en Systemsäkerhetsdeklaration. För att åstadkomma tillräcklig bevisning måste uppställda mål och krav analyseras, risker hanteras, samt kravuppfyllnad påvisas.

Försvarsmakten ska utifrån verksamhetens behov och tidigare erfarenheter av liknande tekniska system formulera systemsäkerhetskrav och mål på nya eller ändrade tekniska system, eller för ändrat användningsområde. I Försvarsmaktens dokumentation, t.ex. Systemsäkerhetsledningsplan (FM SSMP), Systemmålsättning (FM SMS) och HFI-plan, kan sökas information om:

* Systemsäkerhetsmål och eventuella systemsäkerhetskrav.
* HFI-mål och eventuella HFI-krav.
* Uppgifter om avsedd användning.
* Eventuell inriktning gällande vägval i systemsäkerhetsprocessen samt kriterier för uppfyllande.
* Uppgifter om materiel med militärt undantag (se H SystSäk kap 5.3.5).
* Andra eventuella kravställningar och relevanta uppgifter.

I de fall sådan information inte enkelt kan inhämtas ska FMV i första hand invänta Försvarsmaktens kravställning med rätt utformade mål och krav. I andra hand kan verifierbar acceptans av FMV ansatta mål och krav inhämtas från Försvarsmakten.

I tredje hand ansätts egna mål och krav vid FMV. Detta förfarande synliggörs sedan för Försvarsmakten genom tydlig information i SSD (se anvisning/mall SSD).

Inom TC Led ansvarsområde tar FMV i rollen som beställare fram en egen Systemsäkerhetsledningsplan (SSMP) som beskriver FMV:s övergripande strategiplanering inklusive grundläggande kravställningar inför anskaffning. Inom TC Led ansvarsområde ska SSMP omfatta såväl systemsäkerhets- som HFI-strategi, och SSMP kan spegla den strategiska planeringen för ett eller flera tekniska system.

I SSMP redovisas systemets samtliga säkerhetsmål, vilka sammanställts från systemmålsättningsdokument och egen kravanalys. Systemsäkerhetsmål och HFI-mål kan redovisas i form av antagna risknivåer med riskklassificeringar och riskmatris. I SSMP anges också vilka förutsättningar som Försvarsmakten har angett för att kunna godkänna system och/eller enstaka riskkällor.

På projektnivå inom FMV genomförs även en systemsäkerhets- och HFI-planering i form av en System Safety Program Plan (SSPP). En SSPP som inkluderar HFI-aspekter utgör därmed också en HFI-plan. HFI-planering kan även presenteras i ett eget dokument. SSPP inklusive HFI-planering ska dels redogöra för det planerade arbetet som erfordras för att uppfylla kraven, dels beskriva hur resultaten av detta arbete ska dokumenteras.

SSPP inklusive HFI-planering kan även samordnas i t.ex. en generell projektplan.

Normalt utarbetar även leverantör en egen SSPP.

## Vägvalsmodellen

Vägvalsmodellen (VVM) är en iterativ metod som kan användas vid olika tillfällen under ett systems livscykel, t.ex. vid anskaffning och vid ändring av tekniska system och produkter. Vägvalen används av FMV i dess olika roller vid kravställning, konstruktions- och integrationsarbete.

Vägvalsmodellen omfattar enligt H SystSäk 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

Ett viktigt användningsområde för VVM inom FMV Led är under systemsäkerhetsvärderingsarbetet, där metoden används för att verifiera kravuppfyllning. I princip kan samtliga vägval övervägas i systemsäkerhetsvärderingen.

I praktiken är det ofta så att delar av ett systemsäkerhetsarbete kan uppfylla standarder etc. enligt vägval 2-6, men att en riskmatris ändå behöver tas fram i enlighet med vägval 7. Inom TC Led ansvarsområde anses det därför som rimligt att i första hand enbart använda Vägval 1 och 7. Denna förenklade vägvalsprocess innebär att i riskkälleanalysen (PHL) först avgöra huruvida författningsenliga krav är uppfyllda, främst genom CE-märkning (VV1). Vid behov hanteras därefter kvarvarande riskkällor var för sig i en risklogg (VV7).

Detta arbetssätt stämmer väl överens med tidigare använd systemsäkerhetsmetodik, där CE-märkt COTS och ”Trivial materiel” har kunnat undantas kraven på fullständigt systemsäkerhetsarbete inkluderande risklogg.

I följande kapitel appliceras denna förenklade vägvalsmodell vid systemsäkerhetsvärdering inför utgivande av TC Led Systemsäkerhetsdeklaration. Viss hantering av andra vägval diskuteras också nedan. För mer detaljer om hur vägvalsmodellen kan appliceras i FMV:s roll som beställare, se H SystSäk kap 16.3.

## Systemsäkerhets- och HFI-värdering

I rollen som beställare ska FMV inför överlämning av ett system kunna påvisa att betryggande säkerhet uppnåtts för hela systemet. I FMV SSPP ska ingå samtliga krav gällande systemsäkerhet och HFI. Värderingen av kravuppfyllnad omfattar det samlade resultatet av allt genomfört systemsäkerhetsarbete.

Säkerhetsvärderingen resulterar i säkerhetsbevisning, argument och belägg från olika källor, samt genomförda analyser gentemot kraven i SSPP. När värderingen är färdig sammanställs den i en Systemsäkerhetsdeklaration (SSD) med tillhörande systemsäkerhetsdokumentation.

Information om det underlag som minst ska tas fram inför en Systemsäkerhetsdeklaration (SSD) framgår i kapitel 3.8, samt kortfattat av processbilden ”FMV Led Systemsäkerhetsprogram” (Fig. 2).

Riskkällelista (PHL) är ett grundläggande dokument för identifiering och bedömning av riskkällor, se kapitel 3.4 nedan. En anvisning/mall för framtagande av PHL inom TC Led ansvarsområde finns bifogad till denna handlingsregel.

HFI-arbetet inför SSD inom TC Led ansvarsområde utförs normalt integrerat i systemsäkerhetsprocessen. Genom PHL och fortsatt hantering i bl.a. risklogg omhändertas erforderliga delar avseende HFI och användbarhet på ett sätt som motsvarar HFI RAIDO (Risks, Assessments, Issues, Dependencies, and Opportunities – Risker, antaganden, problem, beroenden och möjligheter) inom TC Led ansvarsområde.

För ytterligare beskrivning av inriktning, arbetssätt och krav inom HFI-området, se FMV Handbok ”Human Factors Integration” (H HFI) samt FMV Designregel ”Integration av humanfaktorer och användbarhet i försvarssystem”.

Nedan ges mer information om riskanalys, Vägvalsmodellen samt framtagande av SSD, SAR och SCA. För djupare beskrivningar hänvisas till H SystSäk och framtagna anvisningar.

## Riskanalys

Riskhantering består av riskanalys, riskvärdering och riskreducering/riskstyrning.

TC Led Riskkälleanalys (PHL) används som ett första steg i riskanalysen. Genom denna analys identifieras enskilda riskkällor, och en bedömning visar om aktuellt system kan klassas som CE-märkt COTS eller inte.

En riskkälla är en farlig egenskap eller ett förhållande som kan leda till skada på person, egendom eller yttre miljö. Anvisning/mall för Riskkällelista (PHL) för Led (”PHL-mallen”, se bilaga) innehåller en generell lista över sådana egenskaper eller förhållanden, som ger stöd vid grundläggande identifiering av riskkällor.

PHL-mallen omfattar riskkällor avseende både systemsäkerhet och HFI. Analys av samtliga dessa riskkällor lägger också grunden till Funktionell riskanalys (FHA).

Riskkälleanalysen kan för enklare system visa att samtliga identifierade riskkällor är omhändertagna genom att författningsenliga krav är uppfyllda, främst genom CE-märkning. Sådana system kan omhändertas genom Vägval 1, vilket innebär att säkerhetsbevisning sammanställs i form av DoC och att ingen Risklogg behövs. Se kap. 3.5.

Skulle vägval 2-6 vara aktuella i enlighet med underlag från Försvarsmakten, ska samtliga riskkällor bedömas utifrån aktuella vägval.

Om analysen visar att det finns enskilda riskkällor som behöver hanteras genom systemsäkerhetsanalys och riskvärdering i Vägval 7, ställs krav på riskbedömning mot en Tolerabel risknivå (TR) uttryckt i en riskmatris. Sådan riskmatris ska vara definierad i grundläggande kravdokumentation, t.ex. FMV SSMP. Se kap. 3.6.

## Vägval 1: COTS och CE-märkta produkter

### Författningsenliga krav

Syftet med vägval 1 (VV1) är att säkerställa att aktuellt system uppfyller de författningsenliga kraven, t.ex. EU-rätt och svensk lagstiftning samt harmoniserade standarder. Vägval 1 kan användas för COTS-produkter (Commercial off the shelf), d.v.s. produkter som är civilt godkända och certifierade, ofta via CE-märkning. Vägval 1 har stora likheter med avgöranden enligt tidigare upplagor av H SystSäk huruvida ett system kunde klassas som ”COTS/trivial materiel”.

Om produkten är CE-märkt 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.

### Bedömningsgrunder COTS

Några exempel på godtagbar säkerhetsbevisning i Vägval 1 är DoC gällande CE-märkning samt EU-direktiv för elektromagnetisk kompatibilitet (EMCD) respektive maskindirektivet (MD).

Förutom bedömningskriterier enligt ovan samt i PHL-anvisning bör man i bedömningen ställa sig frågor som:

* Kan aktuellt system bedömas som komplext, d.v.s. sammansatt av flera systemsäkerhetsmässigt kopplade (kopplingar med noterbar systemsäkerhetspåverkan) delsystem eller produkter?
* Inom ramen för aktuell systemsäkerhetsdeklaration, skiljer sig användningen av systemet eller integration med annat system från det som tillverkaren baserar sin CE-märkning/certifiering på?
* Finns det komplexa risker och risker som omfattas av lagstiftning, t.ex. AFS (strålning, el, höjder...)?

Om svaret på samtliga ovanstående frågor är ett tydligt ”Nej”, övriga villkor är uppfyllda och detta påvisas i PHL, kan Vägval 1 användas. Om svaret på någon av de ovanstående frågorna är ”Ja”, är det troligt att man behöver genomföra systemsäkerhetsarbete med Risklogg (vägval 7).

I Systemmålsättning (SMS 2) bör finnas en lista över vilka godkännanden som behövs för att det tekniska systemet eller produkten ska kunna tas i bruk.

### Användningsmiljö och användningsområde

En grundförutsättning för vägval 1 är att de riskkällor som anges omhändertagna genom CE-märkning har genomgått en riskbedömning som är giltig för det avsedda användningsområdet och avsedd användningsmiljö. Planerad och redovisad användning för systemet ska vara inom det användningsområde och inom de begränsningar som produkten är certifierad för, och i enlighet med vad som anges av leverantören.

För många tekniska system och produkter kan de civila författningskraven på säkerhet och skydd anses tillräckliga om avsedd användning ryms inom tillverkarens bruksanvisningar och underhållsföreskrifter. Om detta inte är fallet behöver Vägval 7 sannolikt genomföras, se Fig. 3.

### Deklaration för COTS-produkter

Om säkerhetsarbetet visar att vägval 1 är tillämpligt ska SSD tas fram i enlighet med TC Led anvisning/mall. Underlag till SSD:

* Säkerhetsbevisande underlag ska biläggas, minst i form av PHL. Av PHL ska tydligt framgå att samtliga riskkällor är omhändertagna.
* DoC ska vara tillgängliga och presenterade åtminstone som referensdokument i SSD.
* SAR/SCA är inte nödvändiga att ta fram i VV1.

För olycksrisker som inte kan hanteras genom hänvisning till CE-märkning eller motsvarande i vägval 1, genomförs systemsäkerhetsarbete med Risklogg (vägval 7).



Fig. 3. Vägval 1 – Författningsenliga krav.

## Vägval 7: Fullständigt systemsäkerhetsarbete

### Riskmatriser och risklogg

Vägval 7 innebär att fullständigt systemsäkerhetsarbete genomförs. Baserat på genomförd PHL identifieras kvarstående risker och sammanställs i en Risklogg. Genom fortsatt systemsäkerhetsanalys (PHA, Risklogg, EHA, FHA etc.) bedöms om de kvarstående enskilda olycksriskerna ryms inom Tolerabel risknivå (TR) uttryckt i riskmatriser, som ska vara fastställda som HFI- och systemsäkerhetsmål i SSMP/SSPP.

Riskmatriser kan vara kvalitativa eller kvantitativa. Kvalitativa riskmatriser används normalt inom TC Led ansvarsområde. I vissa fall, för olycksrisker med överskådliga orsakssamband och tillförlitliga numeriska data (inhämtade eller skattade), kan kvantitativ riskmatris tillämpas.

HFI- och systemsäkerhetsmål, i form av riskmatriser som antagits i tidig systemsäkerhetsplanering (t.ex. SSMP), kan behöva omprövas i ett senare skede av systemsäkerhetsprocessen. Eftersom riskmatriser är ett ingångsvärde till beställningar behöver FMV Led ge sin syn, och acceptera eller omförhandla antagen riskmatris med hänsyn till möjlighet att genomföra anskaffnings- eller integrationsuppdrag.



Fig. . Vägval 7 – Riskmatriser.

Anvisning/mall för framtagande av Risklogg (RL) återfinns som bilaga. I RL beskrivs hanteringen av identifierade risker på sådant sätt att riskreducering, åtgärder och acceptansbeslut klart framgår. Det bör framgå i vilket läge systemet är bedömt innan riskminskande åtgärder är införda och bedömda. Det viktigaste är dock status vid ”leveransfärdigt system”, som ska speglas i dokumentet. Effekten av beslutade riskminimerande åtgärder ska tydligt framgå i slutkolumnen för risknivåer. RL ska även omfatta de HFI-risker och konsiderationer som identifierats.

RL ska också beskriva detaljer om riskacceptans. Vid behov kan ett separat dokument som påvisar stängning av riskhanteringen användas för t.ex. signaturer och ytterligare kommentarer.

### Systemsäkerhetsrapport

Syftet med en Systemsäkerhetsrapport (Safety Assessment Report, SAR) är att samlat redovisa all relevant säkerhetsdokumentation från leverantör. SAR utgör underlag för Systemsäkerhetsutlåtande (SCA), se kap 3.5. SAR och SCA är i första hand leverantörens ansvar att färdigställa.

SAR baseras på utförd systemsäkerhetsanalys (PHL, PHA, Risklogg, EHA, FHA etc.) samt säkerhetsföreskrifter. Dessa olika underlag kan inarbetas i SAR alternativt utgöra referensdokument.

För enklare tekniska system som godkänts genom Vägval 1 måste inte SAR tas fram. Vid behov kan motsvarande information i stället redovisas direkt i SSD.

För övriga vägval (VV2-6), se kap. 3.7 samt H SystSäk.

SAR ska innehålla relevant information för:

* identifiering av aktuellt tekniskt system
* identifiering av användningsområde, användningsmiljö och avgränsningar
* spårbar redovisning av genomförd systemsäkerhetsanalys (och eventuellt HFI-analys, se nedan)
* sammanfattande redovisning av identifierade risker, riskminskande åtgärder, samt hanterade respektive kvarvarande risker
* framtagande av säkerhetsrestriktioner
* framtagande av säkerhetsföreskrifter.

Systemsäkerhetsrapporten kan i vissa sammanhang utformas som en Safety Case Report. För ytterligare beskrivning av SAR, se H SystSäk (Aktiviteter, Task 301).

SAR måste inte utgöra ett fristående dokument utan kan slås samman med SCA till ett SAR/SCA.

Redovisning av genomförd HFI-analys, redovisande av HFI-risker och påvisande av kravuppfyllnad på HFI-området kan inkluderas i SAR. Om SAR inte omfattar HFI-området ska motsvarande HFI-rapport tas fram som underlag till SSD.

### Systemsäkerhetsutlåtande

Systemsäkerhetsutlåtande (Safety Compliance Assessment, SCA) är ett av de systemsäkerhetsbeslut som överlämnas från en roll till nästa. FMV i rollen som leverantör begär normalt ett SCA som leverantörens ställningstagande till att det tekniska systemet uppfyller ställda mål och krav.

För tekniska system som godkänts genom Vägval 1 måste inte SCA redovisas. För övriga vägval (VV2-6), se H SystSäk.

SCA ska innehålla eller tydligt referera till identifiering av aktuellt tekniskt system, samt identifiering av användningsområde, användningsmiljö och avgränsningar.

SCA ska innefatta ett ställningstagande från utvecklande leverantör eller ansvarig på FMV, att det tekniska systemets säkerhet är acceptabel för användning, förutsatt att angivna säkerhetsföreskrifter följs.

SCA kompletteras med ett uttalande att HFI-aspekter har analyserats och omhändertagits.

Systemsäkerhetsrapporten SAR kan inkluderas i samma dokument som SCA (SAR/SCA).

För ytterligare beskrivning av SCA, se H SystSäk (kap 17.3).

### Deklaration med risklogg

Inför färdigställande av SSD då åtminstone någon identifierad risk omhändertagits i risklogg (vägval 7) ska minst nedanstående underlag tas fram. Det ställs inga krav på att alla informationsdelarna måste utgöras av separata dokument.

* SSPP – Systemsäkerhetsplan, samt en HFI-planering. SSPP och HFI-plan ska redovisa planerat arbete för kravuppfyllnad och beskriva säkerhetsdokumentationen. SSPP och HFI-plan måste inte utgöras av separata dokument, utan kan samordnas i t.ex. SSMP.
* PHL – Riskkällelista inkl. HFI (enligt bifogad anvisning/mall).
* RL – Risklogg: Systemsäkerhet och HFI.
* Stängning av riskhanteringen (”riskstängning”). Kan utföras direkt i RL. För respektive risk ska framgå att den är hanterad, samt namn, organisation, funktion och underskrift.
* SAR – Systemsäkerhetsrapport. Utarbetas normalt av leverantör; FMV om tillämpligt.
* SCA – Systemsäkerhetsutlåtande. Tas normalt fram av leverantör, annars av FMV (se gällande delegeringsordning). Kan ingå som del i ett SAR/SCA-dokument.
* Övrigt underlag som finns kravställt i SSMP eller SSPP.

Som bilagor till SSD ska följande dokument inkluderas:

* PHL inkl. HFI-aspekter
* Eventuella andra säkerhetsanalyser (t.ex. O&SHA, FHA, EHA, RADS, FRACAS - se H SystSäk)
* RL och Stängning av riskhanteringen
* SAR och SCA.

## Övriga vägval

### Allmänt

Som tidigare nämnts anses normalt vägval 1 och 7 vara tillämpbara inom TC Led ansvarsområde. H SystSäk medger dock Vägval 1 för vissa produkter som genomgått en ”CE-liknande process”, t.ex. MOTS, och andra vägval (VV 2-6) för produkter som exempelvis godkänts av annan stat, tillverkats enligt en erkänd standard, eller utgör så kallat ”beprövat system”.

Gemensam nämnare för samtliga vägval är att *tillräcklig säkerhetsbevisning ska bifogas SSD.* Hur denna säkerhetsbevisning ser ut och sammanställs är beroende på gjorda vägval.

En princip inom TC Led ansvarsområde är att efterfråga Försvarsmaktens inriktning gällande vägval. Om Försvarsmakten angett som inriktning att något eller några av vägvalen 2-6 ska användas, ska denna inriktning också innefatta tydliga förutsättningar för uppfyllande. Exempelvis ska för VV2 anges vilka godkännanden och vilka stater som kan accepteras; för VV3 godkända parter och acceptabla godkännanden; för VV4-5 vilka standarder och designregler som kan appliceras. För VV6 kan det kräva en djupare analys av vad som ska uppfyllas och vilka statistiska underlag som finns för att kunna bedöma uppfyllnad.

### CE-liknande process

Utöver CE-märkt COTS kan Vägval 1 användas för vissa produkter som genomgått en CE-liknande process. En sådan process innebär att samma metodik och krav gäller som vid CE-märkning av produkter enligt ett visst EU-direktiv, men att den aktuella produkten inte ska (får) CE-märkas.

I vägval 1 behöver avgöras om systemet kan klassas som ”Militär materiel” (Military off the shelf, MOTS), eller som ”Materiel med civil eller militär bakgrund utan undantag för viss militär materiel”, alternativt ”Materiel med civil eller militär bakgrund med undantag för viss militär materiel”.

”Materiel med civil eller militär bakgrund utan undantag för viss militär materiel” ska vara CE-märkt, och behandlas i enlighet med detta.

Till MOTS-produkter hör tekniska system och produkter som är framtagna för särskilt militärt ändamål. Dessa är tagna i bruk hos minst en stat och kan därmed finnas tillgängliga för försvarsmyndigheter efter att kontrakt tecknats mellan involverade stater.

Eventuella undantag i lagstiftningen för militär materiel, respektive för materiel som är ”särskilt konstruerad och tillverkad för visst militärt ändamål”, är inte alltid enkla att tolka. Försvarsmakten har tolkningsföreträde avseende möjligheten att nyttja sådana undantag i lagstiftningen. Vidare har FMV alltid bättre rätt än leverantör att tolka lagstiftningen.

För att en MOTS-produkt ska kunna säkerhetsvärderas enligt VV1 måste den ha genomgått en CE-liknande process. Vidare måste Vägval 1 vara beslutat av Försvarsmakten, med uppgivande av vilken typ av DoC som kan godtas.

FMV ska i rollen som beställare säkerställa att en MOTS-produkt uppfyller svensk lagstiftning och kan tas i bruk vid Försvarsmakten. För MOTS-produkter får den avsedda användningen inte skilja sig mot den utländska försvarsmyndighetens anvisningar. Produkten får heller inte ändras.

Befintligt systemsäkerhetsarbete för en MOTS-produkt måste fullt ut analyseras innan godkännanden som erhålls från annan stat kan accepteras. En sådan analys kan visa sig vara resurskrävande, och i vissa fall kan det vara mer kostnadseffektivt att genomföra eget systemsäkerhetsarbete. Systemsäkerhetsdeklaration ska alltid avges.

För GFE-utrustning (Government Furnished Equipment), även kallad ”tillhandahållen materiel”, se H SystSäk (kap 10.5).

### Beprövat system

H SystSäk medger ett alternativt vägval för ett tekniskt system som redan används och är välkänt. Syftet med vägval 6 (VV6) är att beskriva kriterier för att kunna åberopa trovärdiga och spårbara drifterfarenheter för ett sådant så kallat ”beprövat system”. Med drifterfarenheter avses användning och underhåll i Försvarsmakten, och förfarandet utgår från att systemets utförande eller användning inte förändras.

Eventuellt godkännande att överväga vägval 6 ska vara specificerade av Försvarsmakten i SMS 2, och ska omfatta kriterier för uppfyllnad.

Vägval 6 ställer mycket höga kriterier på bl.a. ursprungsdokumentation, driftuppföljning, incident- och olycksrapportering, relevant riskbedömning m.m. Vidare ska framtida avsedd användning av systemet tydligt omfattas av tidigare godkännanden och sammanfalla med det användningsområde som det finns drifterfarenheter från. Resultatet av systemsäkerhetsanalysen i Vägval 6 ska dokumenteras i en Systemsäkerhetsrapport (SAR).

Den som vill göra en riskvärdering grundad på drifterfarenheter (Proven-in-use) måste noggrant motivera varför jämförelsen kan göras. För mer avancerade system som inte har en tydligt spårbar och relevant historik är vägval 6 sannolikt inte relevant, eftersom kraven på dokumentation och giltighet gör ett komplett systemsäkerhetsarbete enligt vägval 7 mer tidseffektivt.

För kvarstående riskkällor som inte omhändertas genom vägval 6, till exempel genom att avsett användningsområde eller användningsmiljö ändrats, ska vägval 7 tillämpas. Omfattningen av den analys som kan krävas för att bedöma möjligheten till vägval 6 kan i praktiken innebära att vägval 7 är det mest effektiva arbetssättet.

## Systemsäkerhetsdeklaration

### Syfte och bakgrund

Syftet med Systemsäkerhetsdeklarationen (SSD) är att för ett utvecklat eller anskaffat system formellt deklarera systemsäkerheten, samt inom LedM även HFI. Systemsäkerhetsdeklarationen är ett formellt beslut från TC Led som innebär en försäkran om att ställda säkerhetsmål bedöms vara uppfyllda, samt att gällande lagar och förordningar och övriga tillämpliga bestämmelser har iakttagits.

Systemsäkerhetsdeklaration inom TC Led ansvarsområde ska till sitt innehåll motsvara den anvisning/mall som utgör bilaga till denna handlingsregel.

Systemsäkerhetsdeklarationen med erforderliga bilagor ska överlämnas till Försvarsmakten och utgör en grund för Systemsäkerhetsgodkännande (SSG), se Fig. 1.

### Förarbete

Bifogad anvisning/mall är konstruerad så att den kan användas oavsett vilka vägval som gjorts i PHL. Grundläggande information och tillräcklig säkerhetsbevisning ska alltid presenteras i SSD, oavsett vägval. Krav- och restriktionshantering ska redovisas för såväl CE-märkt materiel som andra system. Vidare ska tillåtet användningsområde och -miljö alltid beskrivas i SSD.

Observera att oavsett vägval i säkerhetsvärderingsarbetet får det inte finnas några oklarheter vad gäller det aktuella systemets avsedda användning. Den beskrivna användningen får inte avvika från den användning för vilken systemet innehar DoC eller annan åberopad säkerhetsbevisning.

Grunden för Systemsäkerhetsdeklarationen ska framgå av FMV SSMP, bl.a. vilka säkerhetsmål som är giltiga. HFI- och Systemsäkerhetsmål kan här vara uttryckta som nivåer i form av antagna riskmatriser.

### Restriktionshantering

Restriktioner finns för kvarstående olycksrisker, det vill säga där riskreducerande åtgärder ännu inte är införda. I samtliga systemsäkerhetsbeslut (SAR, SSD) ska restriktioner redovisas, samt vilka kriterier som gäller för att restriktionerna kan hävas. Se H SystSäk (bl.a. kap 17.2, 17.3).



Fig. 5. Tillåtet användningsområde.

### Granskning och godkännande

Efter framtagande av Systemsäkerhetsdeklaration ska egen granskning/kvalitetskontroll genomföras inom projektet. Därefter ska underlaget överlämnas för granskning vid OSG (Oberoende systemgranskningsfunktion) Systemsäkerhet.

I underlaget som lämnas in för granskning ska ingå SSD bilagor enligt ovan. Samtliga dokument ska vara spårbara och färdigställda så långt det är möjligt. OSG-funktionen kan med fördel kontaktas före granskning vid behov av stöd i processen.

Efter granskningsutlåtande från OSG hanteras eventuella identifierade brister i underlaget. Omarbetning och/eller omgranskning av underlaget kan bli aktuellt om större brister identifierats.

Efter rättning enligt granskningsutlåtandet överlämnas underlaget för fastställande enligt gällande rutiner. Normal rutin innebär att deklarationen med underlag, inklusive granskningsutlåtande och rättningsrapport, överlämnas till CCB inför TC Led fastställande.

Bilagor ska finnas redovisade, liksom eventuell sändlista. Om väsentlig information inte återges i Systemsäkerhetsdeklarationen, ska denna information åtminstone vara hänvisad till och bifogad huvuddokumentet som en bilaga/del av bilaga.

### Systemsäkerhetsintyg

Ett Systemsäkerhetsintyg (SSI) kan utfärdas inför verifiering och validering av tekniska system och produkter då FMV ansvarar för verksamheten. Ett Systemsäkerhetsintyg ska till sin omfattning och innehåll motsvara en Systemsäkerhetsdeklaration (SSD), men kan vara begränsad till planerad verksamhet beskriven i ett visst provprogram eller provplan.

# Hantering av ändringar

## Allmänt om ändring

Försvarsmakten ansvarar för designen under vidmakthållandeskedet och därmed även ändringshantering. Det är endast för stora ändringar som FMV återtar designansvaret. Försvarsmakten kan dock beställa vissa tjänster från FMV efter överlämning. För de system där Försvarsmakten har beställt stöd avseende ändringshantering (eller ej överlämnade system) ska nedan process följas så länge detta inte går emot instruktionerna i respektive beställning.

Tekniskt utförande, användningsområde och användningsmiljö för systemet är definierat i gällande FMV Systemsäkerhetsdeklaration respektive Försvarsmaktens Systemsäkerhetsgodkännande. Vid ändringar av systemet krävs det en systemsäkerhetsrelaterad ändringshantering.

Motsvarande appliceras i tillämpliga delar relaterat till HFI. Vid ändring i SSD där HFI-aspekter inte tidigare är omhändertagna behöver dessa behandlas i full utsträckning i samband med Större ändring.

Det finns i grunden tre sätt att utföra en systemsäkerhetsändring (Fig. 6):

1. **Större ändring** (Ändrat tekniskt system)
Större ändring gäller då HFI samt systemsäkerheten vid införd ändring påverkas mer än försumbart. Då krävs det en ny FMV Systemsäkerhetsdeklaration och ett nytt Systemsäkerhetsgodkännande från Försvarsmakten. HFI och systemsäkerhetsarbete utförs enligt normala rutiner för en ny Systemsäkerhetsdeklaration och beslut tas enligt gällande delegeringar.
2. **Mindre ändring** (Justerat tekniskt system)
Mindre ändring gäller för enklare ändringar, där HFI och systemsäkerheten inte påverkas mer än försumbart men där ändringen ändå går utanför tidigare fastställd Systemsäkerhetsdeklaration och/eller tidigare fastställt Systemsäkerhetsgodkännande. Då befintlig Systemsäkerhetsdeklaration och Systemsäkerhetsgodkännande påverkas motsvarar beslutet nya sådana. Motsvarande rutiner följs för fastställande som för ett ny Systemsäkerhetsdeklaration, enligt gällande delegeringar. Dock är dokumentationen förenklad, och anvisningen/mallen *”Mindre ändring systemsäkerhet”* ska användas.
3. **Ändring inom ramen för en befintlig Systemsäkerhetsdeklaration och ett befintligt Systemsäkerhetsgodkännande**
Detta beslut gäller för alla ändringar som inte går utanför fastställd Systemsäkerhetsdeklaration och Systemsäkerhetsgodkännande och därför inte heller påverkar systemsäkerheten mer än försumbart. Ändring fastställs enligt gällande delegeringar.



Fig. 6. Systemsäkerhetshantering av ändringar i befintligt system.

## Bedömning av systemsäkerhets- och HFI-aspekter

Följande råd finns som hjälp vid bedömning och vid dokumentering av bedömning, ifall påverkan avseende systemsäkerhets- eller HFI-aspekter finns (mer än försumbar påverkan) eller ej (försumbar påverkan), för bedömd ändring.

Om ändringen (modifieringen) sker inom ramen för ett tidigare godkännande behöver inget systemsäkerhetsarbete utföras om det kan påvisas att ändringen ligger inom ramen för detta godkännande, och att godkännandet fortfarande är fullt giltigt, och att det ryms inom Försvarsmaktens tänkta användning. Beslut om så är fallet fattas till exempel i samband med fastställandet av Teknisk Order (TO). ”Inom ramen” betyder att tidigare utfärdat godkännande/deklaration tillåter aktuell förändring, och inbegriper bl.a. specificerat användningsområde och gränsytor.

Om ovanstående förutsättningar inte är uppfyllda, samt för system som systemsäkerhetsvärderats med hjälp av risklogg, ska ändringar bedömas enligt följande kriterier.

Om *inget* av följande villkor uppfyllts, kan hela ändringen klassas som försumbar (Mindre ändring) (ingen alternativt försumbar HFI-/systemsäkerhetspåverkan). Om *ett eller flera* av villkoren uppfylls, kan ändringen inte klassas som ”Försumbar”:

* Förändringar införs i systemet som påverkar risken (mer än försumbart) för nya riskkällor eller vådahändelser.
* Förändringar införs i systemet som påverkar risken (mer än försumbart) för identifierade vådahändelser (sannolikheten att de inträffar eller dess konsekvens).
* Förändringar införs i systemet som medför att dokumenterade antaganden/förutsättningar eller skallkrav i systemsäkerhetsdokumentationen för systemet inte längre är giltiga.

Uttrycket ”påverkar risken (mer än försumbart)” medger visst tolkningsutrymme. Det finns alltid teoretiska möjligheter att minsta ändring i systemet ändrar risknivån. Dock finns det ändringar som har så liten konsekvens för systemsäkerheten att de kan bedömas som försumbara. Beslutsmall används som stöd vid sådana avvägningar.

I de fall en bedömning resulterar i att ändringen inte kan klassas som försumbar, ska en ny Systemsäkerhetsdeklaration tas fram. Denna SSD ska omfatta hela systemet, men aktuell ändring ska beskrivas i samband med systemidentifieringen. De följder som systemändringen medför ska tydliggöras avseende användningsområde och gränsytor.

Endast i de fall där en ändring klassas som försumbar ska ”Mindre ändring systemsäkerhet” tas fram enligt nedan.

## Mindre ändring systemsäkerhet

Mindre ändring innebär en ändring med ingen eller försumbar systemsäkerhetspåverkan, utanför ramen för befintligt systemsäkerhetsbeslut. Ett sådant beslut innebär en utökning av gällande systemsäkerhetsbeslut.

För system där FMV har beslutsmandat att fastställa en ändring, fattas ett ändringsbeslut vid FMV. Detta kan ske genom *”Beslut Mindre ändring systemsäkerhet”*. I övriga fall deklarerar FMV sin bedömning genom *”Deklaration Mindre ändring systemsäkerhet”*.

Anvisning/mall ”Mindre ändring systemsäkerhet” ska användas. Gällande SSD ska bifogas, samt eventuella tidigare ändringsbeslut.

## Ändring inom ram

Ändring inom ram innebär en ändring med ingen eller försumbar systemsäkerhetspåverkan, inom ramen för befintligt systemsäkerhetsbeslut.

För system där FMV har beslutsmandat att fastställa en sådan ändring, fattas ett ändringsbeslut vid FMV. Detta kan ske genom *”Beslut Ändring inom ram”*. I övriga fall deklarerar FMV sin bedömning genom *”Deklaration Ändring inom ram”*.

Anvisning/mall ”Mindre ändring systemsäkerhet” bör användas, dock med ändrad rubrik. Gällande SSD ska bifogas, samt eventuella tidigare ändringsbeslut.

# Luftfartsprodukter

Om systemet är en luftfartsprodukt behöver risker gällande flygsäkerhet hanteras genom en separat flygsäkerhetsprocess. Kravens ursprung samt slutgiltig mottagare av underlag skiljer sig mellan systemsäkerhet (människa, egendom, miljö) och flygsäkerhet. Därför är det viktigt att det klart och tydligt går att följa kravställning och kravuppfyllnad för respektive säkerhetsområde. Det lämpligaste sättet är att särskilja flygsäkerhets- och systemsäkerhetsunderlag, för att minska risken för missförstånd. Samtidigt har processer och anvisningar/mallar för system- respektive flygsäkerhet inom TC Led ansvarsområde utformats på liknande sätt, för att förenkla arbetet då båda områdena måste hanteras.

Se TC Led Handlingsregler 1-6 för hantering av flygsäkerhet och dess koppling till systemsäkerhet.

# Flygsäkerhetspåverkande risker i övriga system

System som inte är luftfartsprodukter kan också ha risker som har påverkan på flygsäkerhet. Dessa hanteras som vanliga systemsäkerhetsrisker och klassas mot risknivå gällande systemsäkerhet. Dock behöver en rimlighetsbedömning göras mot de flygsäkerhetskrav som ställs på luftfartsprodukter, så att inte dessa krav överskrids. Flygsäkerhetskrav är inte direkt översättningsbara till systemsäkerhetskrav. Stöd i rimlighetsbedömning kan ges av CI system- och flygsäkerhet Led.

# System av system

FMV kan vid behov agera i rollen som systemintegratör. Systemintegratören är den som säkerställer samfunktion mellan tekniska system till ett ”system av system” och som därmed ger efterfrågad förmåga eller funktionalitet. FMV genomför härvid det systemsäkerhetsarbete som behöver genomföras för att säkerställa samfunktion mellan ingående tekniska system.

När system av system byggs, där vissa eller alla delsystem har egna Systemsäkerhetsdeklarationer, gäller följande:

1. En Systemsäkerhetsdeklaration (SSD), en Systemsäkerhetsrapport (SAR) ett Systemsäkerhetsutlåtande (SCA) och Risklogg (RL) tas fram för det övergripande systemet i enlighet med Vägval 7. HFI-aspekter ska vara inkluderade.
2. Befintliga SSD för ingående delsystem kan användas som del av Systemsäkerhetsdeklaration för övergripande system. Dessa ska då refereras till samt biläggas, inklusive viktiga underbilagor som t.ex. Risklogg med riskstängning. Kontroll av kvalitén ska göras och exempelvis mycket gamla godkännanden/deklarationer bör inte återanvändas utan en förnyad process bör genomföras som inkluderar HFI-aspekter. Kontroll ska även göras att systemsäkerhetsnivån mot vilken tidigare delsystem är godkända inte väsentligt skiljer sig från kravet som gäller för det övergripande systemet. Notera att sammansatta system av system mycket väl kan omfatta HFI-aspekter som inte tidigare omhändertagits inom respektive system.
3. För tidigare ej godkända eller deklarerade delsystem och för det övergripande genomförs normal systemsäkerhetsverksamhet med fokus på integrationsrisker. Risker för tidigare godkända/deklarerade delsystem ska kontrolleras och vid behov omvärderas för användning som en del av det övergripande systemet. Ändrade bedömningar ska då tydligt framgå i dokumentationen.
4. I Systemsäkerhetsdeklarationen för det övergripande systemet ska det tydligt framgå hänvisningar till de olika ingående delsystemens riskdokumentation, så att läsaren enkelt hittar alla riskkällor och risker som finns i det övergripande systemet, inklusive de ingående delsystemen. De viktigaste riskerna ska även redovisas i systemsäkerhetsdeklarationen för det övergripande systemet.

Det är viktigt att mottagaren av en systemsäkerhetsdeklaration har en rimlig möjlighet att bedöma hela systemets risknivå och kunna ta del av alla identifierade riskkällor och risker på ett enkelt sätt. Detta oavsett om dessa är bedömda inom ramen för ett tidigare beslutat delsystem eller är exempelvis nya integrationsrisker.

Det bör beaktas att användning av många delsystems systemsäkerhetsunderlag kan göra att slutresultatet blir svårt att överblicka. Arbetet med att hålla samman alla dessa kan också vara krävande. Detta gäller även i tillämpliga delar avseende HFI.

# Återtagande av materiel från Försvarsmakten

Försvarsmakten har vidmakthållandeansvar för system som är överlämnade från FMV. Det innebär bland annat att Försvarsmakten kan utföra vissa ändringar samt modifieringar efter överlämningen från FMV.

FMV kan behöva ta över designansvar för sådana system inför större modifieringar. För att FMV TC Led ska kunna ta ett sådant ansvar, behöver TC Led ha underlag från Försvarsmakten som deklarerar systemets aktuella status vid tidpunkten för återtagande på FMV. Detta underlag ska normalt användas som grund för vidare systemsäkerhetsarbete. Motsvarande kan gälla i de fall FMV ska stödja Försvarsmakten i dess designansvarsarbete.

Om inte sådant underlag erhålls, behöver FMV utföra systemsäkerhetsarbete från grunden, likt vad som skulle erfordras för ett helt nytt system.

# Språk

Följande gäller om inget annat framkommer i beställning från FM.

H SystSäk (kap 9) ställer vissa krav på språk i systemsäkerhetsdokumentation som manualer etc. Bland annat anges att SSD ska vara skriven på svenska, och att tillverkare i redovisande och beslutsdokument som t.ex. SCA och RL ska skriva ”på svenska eller på det språk som avtalats i kontrakt”.

Säkerhetsdatablad för kemiska produkter som släpps ut på den svenska marknaden vara skrivna på svenska, enligt EU-förordningen REACH (Registrering, utvärdering, godkännande och begränsning av kemikalier).

Inom TC Led ansvarsområde gäller generellt minimikrav (inriktning) att utrustning som ska användas av GSS (gruppbefäl, soldater och sjömän) ska ha en svenskspråkig dokumentation som täcker in det som användaren behöver för att kunna använda produkten/systemet på ett säkert sätt och med avsedd funktion. TC Led kan vid behov göra en särskild bedömning från fall till fall.

För övrigt gäller grundläggande krav på att språket i dokumentation ska vara läsbart och förståeligt. Dokument som författas på svenska ska vara i enlighet med Språkrådets ”Myndigheternas skrivregler”.

# Beslut

Föreliggande handlingsregel gäller från och med 2023-06-01. Tidigare utgåva 11FMV1262-10:1 upphävs från och med samma datum. Beslutet har fattats av TC Led Jakob Innergård. I den slutliga handläggningen har Chefsingenjör system- och flygsäkerhet Ledningssystem Adam Narel deltagit. Föredragande har varit CI Adam Narel. Beslut tas samtidigt om fastställande av bifogade anvisningar/mallar.

*(Digitalt fastställd i Platina)*

Jakob Innergård *(Digitalt kontrasignerad i Platina)*

TC Led Adam Narel

 CI system- och flygsäkerhet Led

Sändlista:

Arkiv

Bilagor

Bilaga 1 Anvisning/mall för Riskkällelista (PHL) för Led

Bilaga 2 Anvisning/mall för Mindre ändring systemsäkerhet

Bilaga 3 Anvisning/mall för SSMP, HFI- och systemsäkerhetsstrategi för Led

Bilaga 4 Anvisning/mall för Risklogg (RL) för Led

Bilaga 5 Anvisning/mall för Systemsäkerhetsdeklaration (SSD) för Led

1. H HFI 2016 beskriver Försvarsmaktens koncept och FMV systematiska arbetssätt för användbara och ergonomiska system. Handboken bygger på bl.a. Försvarsstandard 5291, Integration av humanfaktorer i försvarssystem. [↑](#footnote-ref-1)