Systemsäkerhetsdeklaration för [System]

[Ev. bild av det aktuella systemet]

**Anvisning Systemsäkerhetsdeklaration (SSD)**

Bilaga 5 (Anvisning/mall för Systemsäkerhetsdeklaration (SSD) för Led) till Handlingsregel 102 är en anvisning (ver 2) för hur en Systemsäkerhetsdeklaration utformas inom TC Leds ansvarsområde. Systemsäkerhetsdeklaration inom TC Led ansvarsområde ska till sitt innehåll motsvara den anvisning/mall som utgör bilaga till denna handlingsregel. Anvisningen är utformad så att textunderlag kan kopieras till dokument som ska utgöra en Systemsäkerhetsdeklaration och användas som stöd vid utformning av densamma. TC Led Handlingsregel nr 102 utgör grunden för denna anvisning, och innehåller en djupare beskrivning av systemsäkerhetsprocessen inom TC Led ansvarsområde.

VIKTIGT: Anvisningen utgörs dels av textdelar som ska finnas i det färdiga dokumentet, anges i svart text, samt övriga instruktioner angivna med inramad röd text. Dessa ramar med innehåll, samt ej tillämpbar text inom hakparenteser, används inte i slutversionen av dokumentet. Svart text inom [hakparenteser] utgör exempeltexter som behöver anpassas till aktuellt system.

För att tydligt markera vikten av detta dokument ska all svart text utan hakparentes samt alla tabeller nedan finnas kvar i det färdiga dokumentet. Om någon tabellrad inte behöver fyllas i, ska texten ”Inte tillämpligt” eller N/A skrivas i första rutan i resp. tabell. Detta avses leda till ett aktivt ansvarstagande för varje enskild faktauppgift, d.v.s. en egen kvalitetskontroll.

Systemsäkerhetsdeklaration är det dokument som deklarerar systemsäkerheten hos materielen inför överlämning till Försvarsmakten. Från denna version tas även ett första steg för att omhänderta området HFI i SSD. HFI är en systematisk process för att med framgång kunna integrera försvarssystemets komponenter (människor, processer och teknik) med varandra och därmed 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.

Benämningen på Systemsäkerhetsdeklarationen är alltid ren, dvs. utan epitet i form av ”preliminärt”, ”tidsbegränsat”, ”interimistiskt”, ”tillfälligt”, ”begränsat”, ”slutligt” m.m. (jmf H SystSäk 2022 kap 17.2).

För materiel som ska provas vid FMV eller hos leverantör utfärdas annat beslut i särskild ordning.

Denna anvisning kan användas för alla olika typer av tekniska system från enkla till komplexa. Detta innebär att föreliggande anvisning gäller oavsett vilken säkerhetsbevisning som åberopas och vilka val som gjorts enligt Vägvalsmetoden (VV1-7). Även för standardprodukter (COTS) som uppfyller krav enligt EU-direktiv och/eller branschstandarder och som man avser att användas autonomt och endast i enlighet med tillverkarens anvisningar, rekommenderas användning av föreliggande anvisning – se TC Led HR 102.

Kom ihåg att anpassa informationen i sidhuvudet vid användning av denna anvisning som mall. Beteckningen ”VHL-dokument” byts lämpligen ut mot ”Beslut”. För att möjliggöra spårbarhet bör datering och någon form av dokumentnumrering tillföras innan dokumentgranskning vid OSG.

FMV praxis (2022) gällande sekretess är, att handlingar som inte omfattas av sekretess inte ska märkas alls innan registrering i Platina.

Systemsäkerhetsprocessen inom FMV Ledningssystemområde ska ständigt vara föremål för förbättring. Synpunkter samt kommentarer till detta dokument tas tacksamt emot av CI Systemsäkerhet och HFI inom LedM.

Innehåll

[[Referenser] 4](#_Toc164870305)

[[Förkortningar och förklaringar] 4](#_Toc164870306)

[1 Bakgrund 5](#_Toc164870307)

[1.1 Omfattning 5](#_Toc164870308)

[1.2 Integrationsprodukter med egna Systemsäkerhetsbeslut 5](#_Toc164870309)

[2 Systemidentifiering 6](#_Toc164870310)

[2.1 Konfiguration och tekniskt utförande 6](#_Toc164870311)

[2.2 Gränsytor 7](#_Toc164870312)

[2.3 Publikationer och tekniska data 8](#_Toc164870313)

[2.4 Explosiva varor 9](#_Toc164870314)

[2.5 Övriga farliga varor 9](#_Toc164870315)

[3 Användningsområde 10](#_Toc164870316)

[3.1 Avsett användningsområde 10](#_Toc164870317)

[3.2 Avsedd användningsmiljö 10](#_Toc164870318)

[3.3 Användare 11](#_Toc164870319)

[4 Genomfört HFI- och systemsäkerhetsarbete 11](#_Toc164870320)

[4.1 Ingångsvärden 12](#_Toc164870321)

[4.2 Grunder för Vägval 1 COTS 13](#_Toc164870322)

[4.3 Grunder för Vägval 1 MOTS och Vägval 2-6 13](#_Toc164870323)

[4.4 Systemsäkerhets- och HFI-arbete enligt Vägval 7 14](#_Toc164870324)

[4.5 Oberoende systemgranskning 15](#_Toc164870325)

[5 Restriktioner 15](#_Toc164870326)

[6 Deklaration 16](#_Toc164870327)

[Bilagor 16](#_Toc164870328)

Innehållsförteckningen uppdateras via wordfunktionen Referenser/Uppdatera tabell.

[Referenser]

Relevanta dokument listas med benämning och nummer. Om tabellen inte används kan rubriken och hela avsnittet tas bort.

Exempel på referenstabell:

| Ref | Dokument | Nummer | Utgivare | Bedömning |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

[Förkortningar och förklaringar]

Relevanta förkortningar och uttryck listas vid behov. Om tabellen inte används kan rubriken och hela avsnittet tas bort.

| Förkortning | Beskrivning |
| --- | --- |
|  |  |
|  |  |

# Bakgrund

Denna Systemsäkerhetsdeklaration (SSD) är ett entydigt uttalande från TC Led att [System] uppfyller angivna systemsäkerhets- och HFI-krav, att eventuella ej uppfyllda säkerhetsvillkor är kompenserade, samt att produkten har en systemsäkerhetsmässigt acceptabel risknivå under de förutsättningar som anges.

Deklarationen åtföljs av en redovisning av det underlag som behövs för att visa att deklarationen är helt underbyggd. Systemsäkerhetsdeklarationen sammanfattar också all övrig säkerhetsbevisning som planer, specifikationer, DoC och rapporter i ett klart uttalande.

Om tillämpligt, beskriv rollfördelning och ansvarsfördelning (gärna med bild). Under rubriker som avhandlar områden utanför FMV:s ansvar ska ansvarig aktör anges, bl.a. för att förtydliga TC Led ansvarsområde.

## Omfattning

Mycket kortfattad sammanfattning av det tekniska system som denna SSD omfattar. Det är lämpligt att här nämna eventuell klassning som COTS. Utförligare beskrivning ges i kap 2.

Denna Systemsäkerhetsdeklaration omfattar [system]...

Om det tidigare har utfärdats en Systemsäkerhetsdeklaration (Systemsäkerhetsgodkännande) för här aktuellt tekniskt system och detta ersätts av denna Systemsäkerhetsdeklaration, så ska tidigare Systemsäkerhetsdeklaration (Systemsäkerhetsgodkännande) upphävas.

[Tidigare utfärdad Systemsäkerhetsdeklaration (Systemsäkerhetsgodkännande[[1]](#footnote-1)) upphävs härmed:]

| Dokumentnamn | Dokumentbeteckning | Datum |
| --- | --- | --- |
|  |  |  |

## Integrationsprodukter med egna Systemsäkerhetsbeslut

För aktuellt tekniskt system ska designansvar definieras. Designansvarig ska inhämta erforderligt underlag i form av Systemsäkerhetsdeklaration och/eller systemsäkerhetsutlåtanden för ingående tekniska delsystem och produkter. För integrationsprodukter ska Systemsäkerhetsdeklarationer och/eller systemsäkerhetsgodkännande finnas och redovisas i tabellen nedan. För explosiva och andra farliga varor finns ett särskilt avsnitt, se kap **Error! Reference source not found.** nedan.

Beskriv på vilket sätt ingående/underliggande Systemsäkerhetsbeslut omhändertas i denna övergripande Systemsäkerhetsdeklaration. Till exempel ska redovisas om identifierade risker i ingående/underliggande Systemsäkerhetsbeslut har infogats i en gemensam risklogg, eller om riskloggar från respektive Systemsäkerhetsbeslut biläggs och endast integrationsrisker samt nya risker hanteras i en gemensam risklogg på den högre systemnivån.

Förteckning över delsystem/produkter (integrationsprodukt) med egna Systemsäkerhetsbeslut:

| Delsystem | Dokumentnamn | Dokumentbeteckning | Datum |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

# Systemidentifiering

Här ges en beskrivning av systemet eller produkten, och eventuell ändring. Beskrivningen ska vara utformad så att en ej insatt läsare (granskare, förbandschef etc.) ska kunna bilda sig en övergripande förståelse för systemet. Lämplig omfattning: några meningar.

Samtliga förekommande förkortningar i systembenämningen ska skrivas ut.

## Konfiguration och tekniskt utförande

### Aktuell version

Identifiering av den version för vilken denna deklaration gäller.

|  |  |
| --- | --- |
| Systembenämning |  |
| Modellbeteckning |  |
| Typnummer |  |
| [Förrådsbeteckning] |  |
| [Förrådsbenämning] |  |
| [Övriga benämningar] | [Civil motsvarighet, tillverkarens namn och typbeteckning, eller annan identifierande benämning.] |
| [Konfiguration] |  |

### Beskrivning

[Systemet] är... avsett för...

[Systemets principiella uppbyggnad och materielinnehåll är enligt följande…]

Den tekniska, övergripande redovisningen som lämnas ovan kan stödjas av lämplig och övergripande teknisk dokumentation i form av förenklade skisser, beskrivningar och/eller ritningar/foton.

[Systemets tekniska utförande redovisas i följande dokument samt följande ritningsunderlag…]

| Dokumentnamn (Förrådsbenämning) | Dokumentbeteckning (Förrådsbeteckning) | Anmärkning |
| --- | --- | --- |
|  |  |  |

[Aktuell konfiguration framgår av baskonfigurationsrapport enligt referens X.]

### Ingående delsystem och viktigare produkter

Nedan görs i förekommande fall en uppräkning av ingående delsystem/produkter för att på ett fullständigt sätt ange vilka delar som omfattas av Systemsäkerhetsdeklarationen, och som därmed får lov att användas tillsammans med stöd av denna deklaration. Sammanställningen har även syftet att redovisa viktiga systeminterna gränsytor.

Hänvisning till bilagd sammanställning kan godtas om antalet ingående delsystem/produkter är omfattande.

Följande delsystem och produkter ingår i systemet:

|  |  |  |
| --- | --- | --- |
| Förrådsbenämning | Förrådsbeteckning | Anmärkning |
|  |  |  |
|  |  |  |

[Inga andra delsystem, produkter, apparater m.m. än vad som uppräknats här eller ingår i tillhörande satser, får användas tillsammans med stöd, av denna Systemsäkerhetsdeklaration.]

[N/A]

### Konfiguration för säker användning

Om det finns en viss minsta konfiguration av systemet för att detta ska fungera på ett säkert sätt, så ska detta särskilt redovisas här.

I systemet ska för säker användning minst följande delsystem och produkter ingå:

| Förrådsbenämning | Förrådsbeteckning | Anmärkning |
| --- | --- | --- |
|  |  |  |

[N/A]

### Säkerhetskritiska delsystem

Delsystem, produkter och/eller apparater som har en säkerhetskritisk betydelse för systemets funktion och som därför alltid måste ingå i systemet för att garantera systemsäkerheten, ska identifieras och redovisas här.

Följande delsystem och produkter har säkerhetskritisk betydelse för systemets funktion och ska därför alltid ingå i systemkonfigurationen:

| Förrådsbenämning | Förrådsbeteckning | Anmärkning |
| --- | --- | --- |
|  |  |  |

[N/A]

## Gränsytor

Här presenteras och beskrivs övergripande samtliga tekniska gränsytor till/mot andra system/bruksenheter, d.v.s. vilken interaktion mot andra tekniska system som är godkänd. Hänvisning ska göras till gällande specifikationer och deklarationer för dessa externa system.

Eventuella säkerhetskritiska konsekvenser ska vara utredda, hanterade och redovisas här.

Gränsytors funktion är viktig för säkerheten. I ett gränssnitt kan mötas system, signaler och hårdvara från olika tillverkare, organisatoriska enheter och kulturer. En bra genomförd systemsäkerhetsanalys av detta område bygger på en god sammanställning av vilka gränssnitt som förekommer, samt vilken interaktion med andra tekniska system och produkter som kan förekomma. Nedan görs en sådan sammanställning.

Krav på gränsytor kan även innefatta krav från designorganisationen på en operatör att tillse vidmakthållande av angränsande system.

Vid vägval 1-6: Enbart gränsytor enligt tidigare framtagen säkerhetsbevisning (DoC etc.) kan omfattas av deklarationen.

### Gränsytor mot andra system

Systemets gränsytor mot andra system…

|  |  |  |  |
| --- | --- | --- | --- |
| Eget system | Gränsyta | Anslutande system | Ev. dokumentnamn |
|  |  |  |  |
|  |  |  |  |

[Ev. fritext]

### Anläggnings- och transportgränsytor

Ange förutsättningarna som krävs för de gränsytor mot anläggningar där det tekniska systemet ska kunna installeras, anslutas, förrådshållas, transporteras eller brukas. Framför allt gäller detta för system som skall installeras i en anläggning, för övriga system i tillämpliga delar.

Anläggningar kan tillhandahålla skydd samt vissa anläggningstekniska basresurser såsom el, kraft, värme, kyla, gas, ventilation, tele, nätverk, vatten och avlopp för att upprätthålla funktion och säkerhet hos materielen.

Inte alla gränsytor är mot andra definierade system. Även gränsytor mot t.ex. mark eller andra fysiska fästpunkter ska redovisas.

Anläggningars gränsytor kan hanteras på olika sätt beroende på hur dessa definieras:

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.

Systemets gränsytor vid [installation, förrådshållning, transport…]

|  |  |  |  |
| --- | --- | --- | --- |
| Eget system | Gränsyta | Basresurs/motsv. | Ev. dokumentnamn |
|  |  |  |  |
|  |  |  |  |

[Ev. fritext]

## Publikationer och tekniska data

Här redovisas i förekommande fall den tekniska dokumentationen som utgör en nödvändig förutsättning för att aktuell Systemsäkerhetsdeklaration ska gälla. Den tekniska dokumentationen kan utgöras av handhavandebeskrivningar, manualer, skyltar och/eller dekaler, riskanalys inför CE-märkning samt eventuellt utbildningsunderlag, underlag för Truppslagsreglemente, underlag för SäkR m.m.

Åberopade publikationer ska ha ett M-nr och/eller vara diarieförda för att tillse tillgänglighet under systemets livslängd.

[Följande publikationer innehåller sådana beskrivningar och/eller tvingande hanteringsregler/förfaringssätt som är nödvändiga att följa för att denna Systemsäkerhetsdeklaration ska gälla:]

| Förrådsbenämning | Förrådsbeteckning | Anmärkning |
| --- | --- | --- |
|  |  |  |

[Publikationer som innehåller beskrivningar och/eller tvingande hanteringsregler/förfaringssätt som är nödvändiga att följa för att här aktuell Systemsäkerhetsdeklaration ska gälla, finns förtecknade i…]

[N/A]

## Explosiva varor

Om det tekniska systemet omfattar ammunition eller andra explosiva varor ska detta redovisas här. Alternativt ska i SSD redovisas att ”Det tekniska systemet innehåller ingen ammunition eller några andra explosiva varor”.

Det är av stor vikt att det tydliggörs om och var i det tekniska systemet explosiva varor ingår eftersom dessa dels har stor olyckspotential.

Ammunition och andra explosiva varor som ingår i det tekniska systemet och som överlämnas/har överlämnats till FM, ska vidare alltid ha egna systemsäkerhetsdeklarationer. Dessa tas fram enligt gällande regler och FMV Tjänsteföreskrift.

I den mån ammunition ingår i det anskaffade tekniska systemet eller då det tekniska systemet ska kunna skjuta befintlig FM ammunition, ska ammunitionens förrådsbeteckning, förrådsbenämning och systemsäkerhetsdeklaration redovisas här. En särskild tabell enligt nedan upprättas för varje vapen i det tekniska systemet.

[Det tekniska systemet innehåller ingen ammunition eller några andra explosiva varor.]

[Följande ammunition får skjutas i det tekniska systemets vapen, samt förvaras och transporteras i vapnet och plattformen på för dessa angivet/avsett sätt:]

| Ammunition | Förrådsbeteckning | Förrådsbenämning | Systemsäkerhetsdeklaration |
| --- | --- | --- | --- |
|  | Mxxxx-xxxxxx |  |  |

[Följande explosiva varor ingår i det tekniska systemet. De är därmed konstruerade och klassificerade för att ingå i det tekniska systemet under alla de faser och användningssätt som det tekniska systemet är specificerat för:]

| Explosiv | Förrådsbeteckning | Förrådsbenämning | Systemsäkerhetsdeklaration |
| --- | --- | --- | --- |
|  | Mxxxx-xxxxxx |  |  |

## Övriga farliga varor

Här redovisas övriga farliga varor/ämnen som ingår i systemet och fordrar särskild redovisning, och sådant som lyder under särskild lagstiftning – t.ex. drivmedel, kemiska ämnen, laser, batterier, ackumulatorer.

Referens ska i förekommande fall göras till aktuell underhållsdokumentation/miljöplan, för att säkerställa att säkerhetspåverkande kemiska produkter hanteras enligt regelverket.

För enklare system kan produkterna listas. Hänvisning kan göras till särskilt genomförd miljöanalys, t.ex. Riskanalys för yttre miljö (EHA, Environmental Hazard Analysis). Säkerhetsdatablad kan bifogas SSD, alternativt redovisas i förekommande miljöarbete.

[Det tekniska systemet innehåller inga säkerhetspåverkande kemiska produkter eller andra farliga varor.]

[Följande säkerhetspåverkande kemiska produkter och farliga varor/ämnen ingår i det tekniska systemet:]

[Följande varor/ämnen som lyder under särskild lagstiftning ingår i det tekniska systemet:]

| Kemisk produkt | Förrådsbeteckning | Förrådsbenämning | Säkerhetsdatablad / datum |
| --- | --- | --- | --- |
|  |  |  |  |

[Det tekniska systemets säkerhetspåverkande kemiska produkter ska hanteras enligt underhållsdokumentation/miljöplan, se referens Y.]

[Se bilaga Z, Säkerhetsdatablad/EHA/etc.]

# Användningsområde

Användningsområdet beskriver hur systemet ska användas, i vilka miljöer det tekniska systemet är avsett att användas i, samt vilka krav som ställs på användare. Dessa beskrivningar definierar ramen för SSD:s giltighet.

Även om tänkt användningsområde och -miljö exakt överensstämmer med beskrivning i leverantörens tekniska dokumentation (t.ex. i Vägval 1 COTS), ska denna beskrivning infogas i alternativt bifogas SSD. Det räcker alltså inte att hänvisa till ”användning i enlighet med beskrivning i leverantörens dokumentation” eller dylikt.

Om produkten ska användas på annat sätt eller i en användningsmiljö utöver det som finns beskrivet i leverantörens tekniska dokumentation behöver ett systemsäkerhetsarbete i någon omfattning genomföras. Detta innebär att enklare vägval (t.ex. Vägval 1) inte är tillräckliga, utan vidare systemsäkerhetsarbete i form av bl.a. Risklogg behöver utföras (Vägval 7).

Nedan beskrivs systemets användningsområde, användningsmiljö samt användare för vilka denna systemsäkerhetsdeklaration är giltig. Denna deklaration är giltig enbart när systemet används på det sätt och i den omgivningsmiljö som finns beskrivet här.

## Avsett användningsområde

Beskriv hur det tekniska systemet är avsett att användas. Observera att användningsområdet ska beskrivas på ett sådant sätt att man med rimlig säkerhet kan säga att systemet inte kommer att användas på ett annat sätt. Samtidigt måste användningsområdet preciseras så långt det är rimligt, så att såväl operatör som granskare får en tydlig bild av systemets användning.

Vid vägval 1-6: Enbart användningsområden enligt tidigare framtagen säkerhetsbevisning (DoC etc.) kan presenteras som tillåtet användningsområde.

Systemet är avsett för användning inom nedan beskrivet användningsområde.

[Fritext]

## Avsedd användningsmiljö

Här ska tydligt framgå i vilka miljöer som systemet är avsett att användas i. Detta är avgörande information för att bedöma systemets risker samt att minimera risken för felanvändning. Sådana användningsförhållanden som rimligen kan förutses ska anges på ett sådant sätt att användning i ej avsedd miljö rimligen undviks.

T.ex: Temperaturintervall; luftfuktighet; vindstyrkor; inomhus/utomhus/i fordon; på land/i vatten; personburet; mastmontering; vibrationer; etc. Se även PHL (bilaga).

Vid vägval 1-6: Enbart användningsmiljöer enligt tidigare framtagen säkerhetsbevisning (DoC etc.) kan presenteras som avsedda användningsmiljöer.

Systemet är avsett för användning inom nedan angiven användningsmiljö.

[Fritext]

## Användare

HFI-aspekt: Beskriv användare (persona) som är tänkta att använda och hantera systemet på något sätt. Observera att användarna ska beskrivas på ett sådant sätt att man med rimlig säkerhet kan säga att oavsiktlig användning inte sker av andra användare. Utöver grundläggande kunskaper som angivna användargrupper förväntas ha, ska eventuella särskilda krav anges. Dessa kan vara krav på utbildning och erfarenhet, eller medicinska, biometriska och liknande krav. Sådana krav kan t.ex. ha ställts från myndighet, tillverkare, FMV eller Försvarsmakten.

Grundläggande utbildningar som angiven användartyp förväntas ha (t.ex. grundskola, soldatutbildning) behöver inte specificeras här. Om användarbeskrivningen ger erforderlig information och inga särskilda krav behöver lyftas, anges ”Inte tillämpligt” eller ”N/A” i tabellens kravbeskrivning.

Systemet är avsett att användas och hanteras av användare (persona) enligt följande beskrivning.

[Fritext]

|  |  |  |
| --- | --- | --- |
| Särskilt krav | Kravbeskrivning | Ev. dokumentnamn |
| Medicinska krav |  |  |
| Biometriska krav |  |  |
| Krav på erfarenhet |  |  |
| Utbildningskrav |  |  |
| Övriga krav |  |  |

# Genomfört HFI- och systemsäkerhetsarbete

En Systemsäkerhetsdeklaration inom TC Led ansvarsområde ska omfatta HFI och systemsäkerhet för hela det tekniska systemet. Genomförd HFI- och systemsäkerhetsanalys ska omfatta alla de delsystem, komponenter, apparater m.m. som avses användas tillsammans med stöd av aktuell Systemsäkerhetsdeklaration.

HFI- och systemsäkerhetsarbete ska utföras i enlighet med System Safety Management Plan (FMV SSMP) inom TC Leds ansvarsområde. Hänvisning kan ske till FMV-projektets systemsäkerhetsplan (FMV SSPP) om sådan finns.

Väsentliga delar ur FMV projektplan, avsnittet Systemsäkerhet, kan infogas.

Vid modifiering av ett tekniskt system ska den nya deklarationen omfatta hela det tekniska system som efter modifieringen avses användas tillsammans. De modifierade delarna ska därvid utgöra en integrerad del av systemet och därigenom omfattas av allt det HFI- och systemsäkerhetsarbete som ska leda fram till den nya Systemsäkerhetsdeklarationen.

I PHL har bedömningen gjorts om något av vägvalen 1-6 är tillämpbara. I SSD presenteras de grunder på vilka aktuella Vägval åberopas. För Vägval 1 COTS anges DoC. För MOTS och andra vägval (VV2-6) anges vilka kriterier som FM har satt och hur dessa uppfylls.

SSD ska omfatta allt nödvändigt säkerhetsbevisande underlag, i enlighet med TC Led HR 102 (kap 3.7) och genomförda vägval 1-7. Detta innebär bifogat underlag minst i form av PHL (inkluderande HFI-aspekter). För Vägval 7 gäller dessutom att samtliga relevanta säkerhetsanalyser, Risklogg med riskstängning, samt SAR/SCA ska bifogas SSD.

Vägval 1, CE-märkta varor eller motsvarande: FMV kan redan i anbudsinfordran ha krävt in den riskanalys som ligger till grund för eventuell CE-märkning, och tidigt utvärderat denna. Allt som oftast sker endast en kontroll i samband med att leverantörens leveransanmälan inkommer till FMV.

FMV intygande om genomfört HFI- och systemsäkerhetsarbete kan i förekommande fall baseras på leverantörens riskhanteringsarbete, bl.a. efter kontroll av att detta har genomförts korrekt och lett till att varje identifierad risk har hanterats.

Korrekt genomfört riskhanteringsarbete ska leda till att varje enskild risk hanteras. Detta förutsätter att risken har identifierats, samt att eventuella riskminskande åtgärder har identifierats och beslutats.

Här redovisas det HFI- och systemsäkerhetsarbete som har genomförts. Redovisningen omfattar ingångsvärden i form av krav och/eller kriterier, t.ex. säkerhetsmål, samt vilka vägval som har tillämpats i enlighet med H SystSäk 2022. Här redovisas också en HFI- och systemsäkerhetsvärdering, baserat på den säkerhetsbevisning som åberopas.

## Ingångsvärden

Följande ingångsvärden i form av krav och/eller kriterier avseende systemsäkerhet har identifierats, inklusive kriterier gällande Vägval 1-7:

| **Ingångsvärde/kriterium** | **Källa** | **Anmärkning** |
| --- | --- | --- |
| [Exempel: ”NATO-godkännande medger Vägval 1 MOTS”] | [Försvarsmaktens SMS/SSMP] | [Försvarsmaktens inriktning och kriterier avseende vägval enligt HSS 2022] |
| [Exempel: ”DoC avseende CE-märkt COTS medger vägval 1 COTS”] | [H SystSäk 2022] |  |
| [Exempel: ”Systemsäkerhetsmål finns, riskbedömning görs enligt Vägval 7”] | [Försvarsmaktens SMS/SSMP] [Antaget av FMV] | [Presenteras enligt nedan] |
| [Exempel: ”Systemsäkerhetskrav: Nödutrymning enligt xx”] | [AFS] |  |
|  |  |  |

[N/A]

[Förutom DoC för CE-märkt COTS enligt HSS 2022, har inga ytterligare ingångsvärden avseende systemsäkerhet identifierats.]

Följande ingångsvärden i form av krav och/eller kriterier avseende HFI har identifierats:

| **Ingångsvärde/kriterium** | **Källa** | **Anmärkning** |
| --- | --- | --- |
| [Exempel: ”Mål finns, riskbedömning görs enligt Vägval 7”] | [Försvarsmaktens SMS/HFI-plan] [Antaget av FMV] | [Presenteras enligt nedan] |
|  | [H HFI] |  |
|  | [FSD 9251] |  |
|  |  |  |

[Inga ingångsvärden avseende HFI har identifierats.]

[Följande Systemsäkerhetsmål och HFI-mål har använts.] [Dessa har hämtats ur FM kravställning.] [Dessa har antagits av FMV i brist på FM kravställning.]

[Fritext]

## Grunder för Vägval 1 COTS

Om Vägval 1 COTS inte är aktuellt för systemet, kan hela texten i kap. 4.2 ersättas med ”Ej tillämpbart”, ”N/A” eller texten ”Vägval 1 COTS är inte aktuellt för detta system.”

[För detta system görs Vägval 1 COTS i enlighet med Försvarsmaktens kriterier (kap. 4.1). PHL visar att relaterade risker är omhändertagna på ett godtagbart sätt i leverantörens riskanalys inför CE-märkning, avseende systemsäkerhet och HFI-aspekter, genom påvisad uppfyllnad gentemot författningsenliga krav eller annan säkerhetsbevisning. Ingen ytterligare riskhantering behövs. Därmed har ingen Risklogg och ingen SCA tagits fram. Följande DoC ligger till grund för Vägval 1 COTS.]

[Vägval 1 COTS är inte aktuellt för detta system i sin helhet. PHL visar dock att ett antal, men inte alla relaterade risker är omhändertagna på ett godtagbart sätt i leverantörens riskanalys inför CE-märkning, avseende systemsäkerhet och HFI-aspekter. Följande DoC åberopas som säkerhetsbevisning för delar av systemet.]

Här redovisas de särskilda lagar, förordningar, EU-direktiv och standarder som är tillämpliga på olika teknikområden i det tekniska systemet. Här får man välja de som är av signifikant betydelse, d.v.s. används som säkerhetsbevisning.

Observera att det måste finnas en tydlig koppling mellan åberopade DoC och aktuellt system. Om till exempel tillverkarens modellbeteckning anges i åberopade dokument ska denna beteckning återfinnas i SSD kap. 2 Systemidentifiering.

Vissa säkerhetsområden kan behöva lyftas särskilt i en Systemsäkerhetsdeklaration, exempelvis bullerkrav samt Elsäkerhet och relaterad kravställning (ref H SEPS 2015).

Vad som särskilt ska vara framlyft utöver grundkrav enligt gällande SAMO och H SystSäk, bör vara reglerat i avtal/beställning samt redovisat i FMV SSMP.

För Vägval 1 COTS gäller att EU-rätt och svensk lagstiftning har tillämpats utan undantag för militär materiel. Om undantag för militär materiel åberopas används andra vägval (t.ex. Vägval 1 MOTS).

| System/delsystem | Direktiv/föreskrift/ harmoniserad standard | DoC, beteckning |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## Grunder för Vägval 1 MOTS och Vägval 2-6

Om Vägval 1 COTS använts för systemet i sin helhet (eller i kombination med Vägval 7) enligt kapitel ovan och detta anses tillräckligt, kan hela texten i kap. 4.3 ersättas med ”Ej tillämpbart” eller ”N/A”.

[För detta system görs [Vägval 1 MOTS] [Vägval [2-6]] i enlighet med Försvarsmaktens kriterier (kap. 4.1). PHL visar att relaterade risker är omhändertagna på ett godtagbart sätt i relevant och tillgänglig dokumentation avseende systemsäkerhet och HFI-aspekter, genom godkännanden eller standarder enligt detta vägval.]

[Varken Vägval 1 MOTS eller Vägval 2-6 är aktuella för detta system. PHL visar dock att ett antal, men inte alla relaterade risker enligt givna ingångsvärden (kap. 4.1) är omhändertagna på ett godtagbart sätt avseende systemsäkerhet och HFI-aspekter, genom godkännanden eller standarder enligt dessa vägval.]

[Följande godkännanden från annan part, standarder, Designregler m.m. åberopas i enlighet med kriterier för [Vägval 1 MOTS] [Vägval x] som säkerhetsbevisning för det aktuella systemet:]

Om något av Vägval 1 MOTS eller Vägval 2-6 är aktuella ska i detta kapitel redovisas eventuella godkännanden, t.ex. från annan stat (VV2), från annan part (VV3), påvisad uppfyllnad i enlighet med standarder (VV4) alternativt Designregler (VV5) som åberopas i säkerhetsbevisningen för det tekniska systemet.

Registreringsbesiktning för fordon, respektive annan typ av besiktning/certifiering/ackreditering av komponenter och delsystem som är utförd av oberoende part redovisas här tillsammans med uppgift om vem som har utfört den och när.

För exempel på godkännanden och standarder som kan åberopas vid säkerhetsbevisning, se TC Led HR 102.

| System/delsystem | Godkännande/standard/ designregel etc | Anmärkning |
| --- | --- | --- |
|  |  |  |
|  |  |  |

[Vägval 1 MOTS är inte aktuellt för detta system.] [Vägval [2-6] är inte aktuella för detta system.]

## Systemsäkerhets- och HFI-arbete enligt Vägval 7

Om Vägval 1-6 använts enligt kapitlen ovan och detta anses tillräckligt, kan hela texten i kap. 4.4 ersättas med ”N/A”.

I det fall Vägval 7 är aktuellt beskrivs här det systemsäkerhets- och HFI-arbete som genomförts av FMV och leverantören och som ligger till grund för aktuell deklaration. Riskdokumentation med framtaget underlag redovisas – d.v.s. PHL, RL, SCA, SAR etc.

Vägval för riskhantering ska alltid redovisas i bifogad Riskkällelista (PHL). Observera att olika vägval kan göras för identifierade risker. Detta innebär att omhändertagande av vissa enskilda risker kan redovisas här som t.ex. ”godkännande från annan part”, medan andra risker behöver hanteras i enlighet med Vägval 7 och därmed redovisas i Risklogg.

[PHL visar att alla risker inte är omhändertagna på ett godtagbart sätt i dokumentation från t.ex. tillverkare, avseende systemsäkerhet och HFI-aspekter. Därmed har systemsäkerhets- och HFI-arbete genomförts i enlighet med Vägval 7.

Genomfört systemsäkerhetsarbete har dokumenterats i följande dokument:

|  |  |  |
| --- | --- | --- |
| **Dokumentnamn** | **Dokumentbeteckning** | **Genomfört av** |
| Riskkälleanalys (PHL) |  |  |
| Systemsäkerhetsutlåtande (SCA) |  |  |
| Systemsäkerhetsrapport (SAR) |  |  |
| Risklogg (RL) [inkl. stängning av riskhantering] |  |  |
| Granskningsprotokoll från OSG |  |  |
| [Övrigt underlag] |  |  |
|  |  |  |

Samtliga identifierade risker är hanterade och redovisas i Riskloggen.]

[Totalt har XX risker identifierats, analyserats och klassificerats under systemsäkerhetsarbetet utifrån de risknivåer som redovisas i riskmatriser i målsättningsdokumentet (dokbet).]

I de fallen det finns risker som bedöms Ej Tolerabla ska FM svar på FMV:s hemställan om undantag från kravställning bifogas. Om svar saknas ska hemställan bifogas.

[Av de identifierade riskerna är [X st.] [samtliga] hanterade i enlighet med riskloggen] [och Y st. kvarstående.] [Kvarstående risker medför restriktion[er] enligt kapitel 5.]

## Oberoende systemgranskning

Här anges i vilken omfattning oberoende granskning enligt TC Led HR 1 har genomförts/kommer att genomföras. Eventuella granskningsrapporter ska ingå i referenslistan. Uppgifter i detta kapitel kan vara preliminära vid inlämning till OSG (d.v.s. uppgiften ”har genomförts” samt ref.dok) eftersom texten syftar på läget vid inlämning till CCB.

Oberoende granskning enligt TC Led HR 1 har genomförts vid LedM Oberoende Systemgranskningsfunktion.

[Ref: Granskningsrapport samt rättningsprotokoll.]

# Restriktioner

Det tekniska systemets samtliga restriktioner ska redovisas nedan.

En restriktion är, enligt definition i H SystSäk, en ”tillfällig inskränkning i det tänkta nyttjandet” av ett tekniskt system. En restriktion ska betraktas som tillfällig och något som ska åtgärdas. Ibland kan dock avvecklingen av ett tekniskt system inträffa före åtgärden.

Instruktion för normalt handhavande, krav på viss utbildningsnivå hos brukaren, eller krav på att följa en viss teknisk dokumentation utgör inte en restriktion enligt H SystSäk definition.

Om det finns restriktioner från tillverkare för aktuella system eller framtagna inom FMV ska dessa restriktioner redovisas i SSD. Om det inte finns några gällande restriktioner, från leverantör eller framtagna inom FMV, ska detta framgå i SSD.

Om det av systemsäkerhetsskäl rekommenderas en särskild uppföljning för att säkerställa att viss teknisk gräns inte överskrids under användning, så redovisas här vilken typ av uppföljning som krävs.

[Inga restriktioner är aktuella för systemet.]

[För att denna Systemsäkerhetsdeklaration ska vara giltig ska samtliga nedanstående restriktioner följas.]

| Restriktions-nummer | ID i risklogg | Beskrivning | Krav/förutsättning för hävande |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

# Deklaration

Systemsäkerhetsdeklarationen ska utgöra ett entydigt uttalande från FMV att det tekniska systemet är säkert under givna förutsättningar och att såväl lagkrav som ställda krav är uppfyllda, med hänsyn till ovan redovisat HFI- och systemsäkerhetsarbete. Texten nedan beskriver TC Led ställningstagande och ärendets beredning, samt utgör beslut om fastställande av deklarationen.

Fastställande sker enligt gällande delegeringsordning. Föredragande ska vara den produktansvarige för det tekniska systemet, vilket ska anges nedan. I den slutliga beredningen av denna Systemsäkerhetsdeklaration bör även projektledaren ha deltagit.

Denna Systemsäkerhetsdeklaration omfattar det totala tekniska systemet som identifieras i kap. 2 ovan, med användningsområde redovisat i kap. 3 ovan. Systemsäkerhetsdeklarationen grundas på genomfört HFI- och systemsäkerhetsarbete redovisat i kap.4, med eventuella restriktioner redovisade i kap. 5.

Denna deklaration utgör ett entydigt uttalande från FMV att det tekniska systemet uppfyller relevanta lagkrav och är säkert under givna förutsättningar.

Mot bakgrund av ovanstående utfärdas härmed denna Systemsäkerhetsdeklaration för det tekniska systemet [XXX] i sin nuvarande konfiguration, för användning i enlighet med de förekommande publikationer och restriktioner, det användningsområde och den användningsmiljö samt av de användare som finns beskrivna i denna Systemsäkerhetsdeklaration. För annan användning eller i annan användningsmiljö gäller inte denna Systemsäkerhetsdeklaration.

[Tidigare [utfärdad systemsäkerhetsdeklaration] [utfärdat systemsäkerhetsbeslut] [dokumentbeteckning, datum, version] upphävs.]

Beslut i detta ärende har fattats av [XXX]. [XXX] har varit föredragande. [I den slutgiltiga beredningen har även [XXX] deltagit.] [Samråd har tagits med [XXX].]

FÖRSVARETS MATERIELVERK

Namn  
TC Led Namn  
 Befattning

Bilagor

Exempel på bilagor. PHL ska normalt utgöra bilaga till SSD.

Bilaga 1 Riskkällelista (PHL)

Bilaga 2 [Systemsäkerhetsrapport (SAR) inkl. bilagor]

Bilaga 3 [Systemsäkerhetsutlåtande (SCA) inkl. bilagor]

Bilaga 4 [Risklogg med stängning av riskhanteringen]

Bilaga 5 [Underlag för leverantörens CE-märkning (DoC)]

Bilaga 6 …

Sändlista

[Försvarsmakten HKV FST STÖD [org.enhet] (avsett för [namn/befattning/roll])]

[…]

Arkiv

För kännedom inom Försvarsmakten

[HKV SÄKINSP]

[HKV FLYGI]

[Organisation] (avsett för [namn])

[Organisation] (avsett för [roll])

För kännedom inom FMV

[Organisation] (avsett för [namn])

[Organisation] (avsett för [roll])

FMV centrala systemsäkerhetsgrupp ([systemsakerhet.fmv@fmv.se](mailto:systemsakerhet.fmv@fmv.se)) kan erhålla en kopia i syfte att förbättra relevanta mallar och vägledningar.

[[systemsakerhet.fmv@fmv.se](mailto:systemsakerhet.fmv@fmv.se) (ej bilagor)]

1. FMV Systemsäkerhetsgodkännande som är författat/beslutat före 2019-01-01. [↑](#footnote-ref-1)