



TC Led Handlingsregel nr 102 - Process systemsäkerhet Led

I denna handlingsregel ges en övergripande beskrivning av hur systemsäkerhetsprocessen ska tillämpas inom TC Led ansvarsområde. Handlingsregeln är baserad på FMV VHL, H SystSäk, gällande delegeringsordningar, samt Samordningsavtal FM – FMV.

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

Handlingsregel 102 samlar också viktigare mallar som är framtagna för användning inom TC Led ansvarsområde, det vill säga mallar för framtagande av PHL samt Systemsäkerhetsbeslut Justering/Smärre Ändring.

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



Innehållsförteckning

TC Led Handlingsregel nr 102 - Process systemsäkerhet Led	1
1 Bakgrund	4
1.1 Krav och beslut.....	4
1.2 TC Led Designansvar.....	4
2 Övergripande beskrivning av Systemsäkerhetsprocessen	4
3 Framtagning av Systemsäkerhetsunderlag	6
3.1 Planering.....	6
3.2 Arbete inför Systemsäkerhetsdeklaration.....	6
3.3 Systemsäkerhetsdeklarationens innehåll	6
4 COTS/Trivial materiel.....	9
4.1 Klassning	9
4.2 Systemsäkerhetsdeklaration	9
5 Hantering av ändringar relaterat till systemsäkerhet	10
5.1 Allmänt om ändring	10
5.2 Bedömning av systemsäkerhetspåverkan.....	11
5.3 Dokumentera Systemsäkerhetsbeslut Justering/Smärre Ändring	12
6 Luftfartsprodukter.....	12
7 Flygsäkerhetspåverkande risker i övriga system	13
8 System av system.....	13
9 Återtagande av materiel från FM.....	14
10 Språk.....	14
11 Beslut	15

Terminologi

Följande terminologilista är gemensam för huvuddokument och bilagor.

Beteckning	Betydelse
BoA	Försvarsmaktens Beslut om Användning
CI	Chefsingenjör inom FMV
COTS	”Commercial off the Shelf”; hyllvara, färdig produkt. I systemsäkerhetsprocessen beteckning på en klassning av civilt godkända och certifierade system, utförd i enlighet med beskrivning nedan (se kap 4.2).
Delegeringsordning	Gällande delegeringsordning vid FMV, fastställd i t.ex. ”Besluts- och samrådsmatris inom TC Led ansvarsområde”.
FM	Försvarsmakten
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.
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 produktområde inom TC Led ansvarsområde.
Restriktion	Tillfällig inskränkning i tekniskt systems tillåtna brukande för att temporärt hantera viss risk och därigenom innehålla ställda krav på systemsäkerhet” (definition enligt H SystSäk).
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.
SS	Systemsäkerhetsgodkännande (FM från 2019, tidigare FMV)
SSD	Systemsäkerhetsdeklaration (FMV)
SSMP	System Safety Management Plan. FMV övergripande systemsäkerhetsplanering.
SSPP	System Safety Program Plan. Systemsäkerhetsplanering hos en leverantör eller på projektnivå, se H SystSäk.
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-, certifierings- och/eller godkännandeprocesser.
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 handlingsregler
Trivial materiel	Systemsäkerhetsrelaterad klassning av enkla produkter som används isolerat, såsom necessär, sport skor och som inte omfattas av lag eller författning med militärt undantag.
TTEM	Teknisk, Taktisk, Ekonomisk Målsättning; kravbild på en produkt.
VerkO LedM	Verksamhetsområde Ledningssystemmateriel inom FMV.
VHL	FMV Verksamhetsledningssystem

Datum	Diarienummer	Ärendetyp
2018-12-18	11FMV1262-10:1	3.1
	Dokumentnummer	Sida
	442892	4(15)

1 Bakgrund

1.1 Krav och beslut

FMV ansvarar för att den verksamhetsprocess som tillämpas för utförande av FM:s beställningar, såväl inom FMV som hos berörda leverantörer, även omfattar systemsäkerhetsverksamhet för person, egendom och miljö. FMV följer härvid de föreskrifter inom systemsäkerhetsområdet som FM fastställer. Systemsäkerhetsarbetet inom FMV ska därmed följa Handbok Systemsäkerhet (H SystSäk).

FM ska i målsättningar och kravdokument eller i uppdrag avseende statusanalys eller motsvarande ange systemsäkerhetskrav, kompletterat med krav avseende risknivå. FMV:s systemsäkerhetsdeklaration eller systemsäkerhetsanalysrapport ges därmed en fast grund.

FMV:s Systemsäkerhetsdeklaration (SSD) utgör grund för FM Systemsäkerhetsgodkännande (SS), vilket i sin tur utgör underlag avseende Systemsäkerhet för utgivande av BoA (Beslut om Användning). Se vidare gällande *Samordningsavtal mellan Försvarmakten och Försvarets materielverk*, samt *H SystSäk* (2011).

1.2 TC Led Designansvar

Tekniskt designansvar 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 TC Led ett visst ansvar även efter överlämning.

Tekniskt designansvar, inklusive teknisk systemledning, innehas normalt av Designansvarig (DesignA) för alla nivåer av tekniska system som levererats till Försvarmakten.

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 Försvarmakten. Då FMV är leverantör av ett system till FM, innehar alltså FMV som regel rollen som DesignA inför överlämning.

Inom sitt ansvarsområde tar TC Led i egenskap av Head of Design fullt designansvar för systemet inför överlämning. FM har designansvar för resterande delar av livscykeln, men kan beställa vissa tjänster av FMV.

2 Övergripande beskrivning av Systemsäkerhetsprocessen

Nedanstående bild (Fig. 1) visar den övergripande systemsäkerhetsprocessen anpassad för verksamhet inom TC Led ansvarsområde.

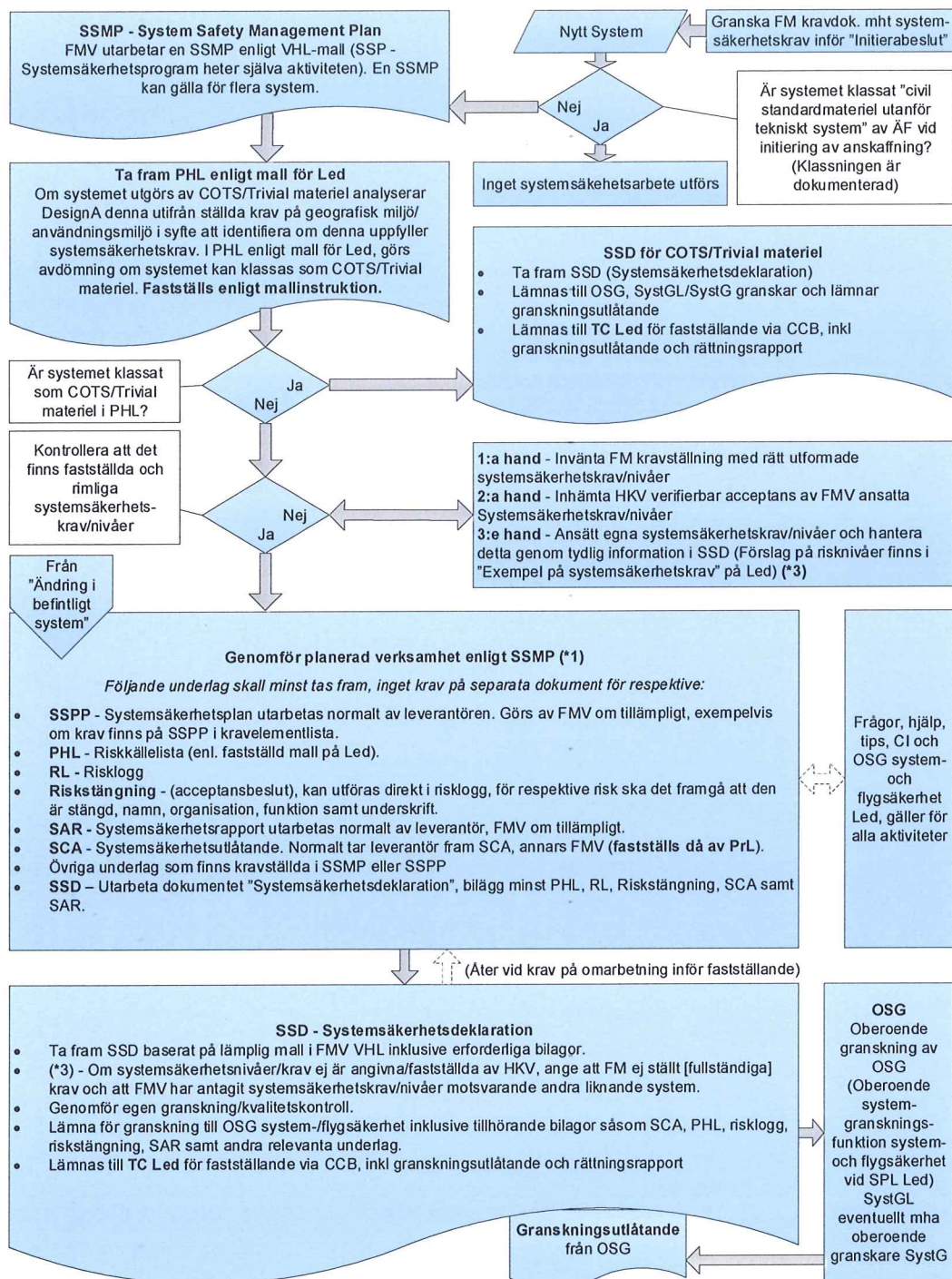


Fig. 1. Övergripande systemsäkerhetsprocess inom TC Led ansvarsområde.

3 Framtagning av Systemsäkerhetsunderlag

3.1 Planering

System Safety Management Plan (SSMP) och System Safety Program Plan (SSPP, även kallad Systemsäkerhetsplan) utgör underlag för system- och projektplanering avseende systemsäkerhet. SSMP beskriver den övergripande systemsäkerhetsplaneringen, och tas fram vid FMV. SSPP beskriver projektplanen avseende systemsäkerhet och utarbetas normalt av leverantör, men kan också utarbetas vid FMV.

3.2 Arbete inför Systemsäkerhetsdeklaration

Information om det underlag som minst ska tas fram inför en Systemsäkerhetsdeklaration (SSD) framgår kortfattat av processrutan "Genomför planerad verksamhet enligt SSMP" i processbilden (Fig. 1).

Risikkällelista (PHL) är ett grundläggande dokument för identifiering och bedömning av riskkällor. En mall för framtagande av PHL inom TC Led ansvarsområde finns bifogad till denna handlingsregel.

Mallar för framtagande av Risklogg (RL) återfinns i H SystSäk samt FMV VHL. I RL beskrivs hanteringen av identifierade risker på sådant sätt att riskreducering, åtgärder och acceptansbeslut klart framgår. Det är värt att notera att det är status vid "leveransfärdigt system" som ska speglas i dokumentet. Effekten av beslutade riskminimerande åtgärder ska tydligt framgå i slutkolumnen för risknivåer.

RL ska också beskriva detaljer om riskacceptans. Vid behov kan ett separat riskstängningsdokument användas för t.ex. signaturer och ytterligare kommentarer.

För djupare beskrivning av ovan nämnda och övriga dokument hänvisas till H SystSäk och framtagna mallar.

3.3 Systemsäkerhetsdeklarationens innehåll

Syftet med Systemsäkerhetsdeklarationen (SSD) är att formellt deklarerat systemsäkerheten hos utvecklat eller anskaffat system. Systemsäkerhetsdeklarationen är ett formellt beslut från DesignA, som innebär en deklaration att ställda systemsäkerhetskrav, inklusive krav på olycksrisk, är uppfyllda, och att gällande lagar och förordningar samt övriga tillämpliga bestämmelser har iakttagits. Systemsäkerhetsdeklarationen ska överlämnas till FM.

Det finns centrala mallar på FMV som stöd för att utforma en systemsäkerhetsdeklaration (tidigare FMV systemsäkerhetsgodkännande). En systemsäkerhetsdeklaration behöver innehålla information enligt nedanstående punkter. Informationen ska helst finnas angiven i huvuddokumentet, men i vissa fall kan hänvisning till beskrivning i bifogade underlag godtas. Observera att det kan krävas komplettering av mallens text för att nedanstående faktainnehåll ska täckas.

- Tydlig identifiering av systemet, exempelvis förrådsbeteckning och förrådsbenämning.
- Viktiga förkortningar ska skrivas ut. Om beteckningen på systemet utgörs av en förkortning ska denna uttydas redan i dokumentets inledning.
- Om systemet bedömts vara COTS/Trivial Materiel, ska detta tydligt framgå.
- Vid mer komplexa system ska viktigare delsystem/produkter redovisas.
- Om det för systemsäkerheten krävs en minimiomfattning av delsystem, ska detta redovisas.
- Delssystem som har en för systemets funktion säkerhetskritisk betydelse och därför alltid måste ingå i systemet för att garantera systemsäkerheten, ska redovisas.
- En beskrivning av systemets tekniska utförande ska finnas. Denna ska vara utformad så att en ej insatt läsare (granskare, förbandschef etc.) ska kunna bilda sig en övergripande förståelse för systemet.
- Det ska anges publikationer vilka innehåller sådana tvingande hanteringsregler/förfaringssätt som är nödvändiga att följa för att aktuell systemsäkerhetsdeklaration ska gälla. Dessa ska ha ett M-nr och/eller vara diarieförda för att tillse tillgänglighet under systemets livslängd.
- Det ska vara angivet på vilket sätt systemet är tillåtet att användas – systemets användningsområde. Detta ska anges på ett sådant sätt att felanvändning rimligen undviks.
- Det ska vara angivet inom vilka miljöer systemet är tillåtet att användas, exempelvis tillåten temperatur, fuktighet, inom/utomhus, skakningar osv. Detta ska anges på ett sådant sätt att användning i ej tillåten miljö rimligen undviks.
- Det ska vara angivet vilka gränssytor som är tillåtna för systemet.
- Om explosiva varor ingår i systemet ska dessa redovisas.
- Det ska vara redovisat vilken systemsäkerhetsverksamhet som ligger till grund för aktuell systemsäkerhetsdeklaration.
- Redovisning av särskilda lagar, förordningar, EU-direktiv och standarder som är tillämpliga på olika teknikområden i det tekniska systemet samt hur de ev. uppfylls. Här får man välja de som är av signifikant betydelse. Om produkter är CE-märkta eller har en annan motsvarande certifiering, ska dessa certifieringar redovisas som referenser.
- Vissa säkerhetsområden kan behöva lyftas särskilt i en Systemsäkerhetsdeklaration, exempelvis 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.
- Det ska redovisas vilken kravställning som ligger till grund för aktuell systemsäkerhetsdeklaration. Detta inkluderar redovisning av risknivåer (deras ursprung – angivet av FM, antaget av FMV), eller angivelse att risknivåer inte används med hänsyn till klassning "COTS/Trivial materiel" när sådan är aktuell. Vidare ska det ges en kort redovisning av om och hur denna kravställning är uppfylld, exempelvis antal risker totalt varav antal på nivå BT.
- Redovisning av riskdokumentationen, vilka underlag som är framtagna – d.v.s. RL, PHL, SCA, SAR m.m.
- Om systemet kräver någon särskild uppföljning ska detta anges.
- Om systemet har några restriktioner (tillfälliga begränsningar i användningsområde, se Fig. 2) ska dessa redovisas. Begränsningar som inte är av tillfällig art, exempelvis sett till en

ursprunglig kravställning, ska inte vara definierade som restriktioner. Sådana begränsningar ska vara omhändertagna under tillåtet användningsområde för systemet. Exempelvis restriktionsområden för radioantennar är ingen restriktion enligt H SystSäk definition, utan en del av beskrivningen av tillåten användning.



Fig. 2. Tillåtet användningsområde.

- Det ska framgå att aktuell systemsäkerhetsdeklaration omfattar det totala tekniska systemet som identifieras i dokumentet.
- Det ska framgå att Systemsäkerhetsdeklarationen grundas på att komplett systemsäkerhetsverksamhet utan begränsningar har genomförts för det tekniska systemet. Vidare ska det framgå att genomförandet av alla de riskminskande åtgärder som finns angivna för att kunna stänga identifierade olycksrisker, är beslutade. (COTS/Trivial materiel – se kap 4.2.)
- Det ska framgå att leverantören, respektive ansvarig på FMV, i sitt Systemsäkerhetsutlåtande (SCA) intygar (inför TC Led) att det tekniska systemet uppfyller gällande lagkrav samt de ställda systemsäkerhetskraven. (COTS/Trivial materiel – se kap 4.2)
- I Systemsäkerhetsdeklarationen ska FMV intyga att det aktuella tekniska systemet uppfyller gällande lagkrav och samtliga systemsäkerhetskrav. (COTS/Trivial materiel – se kap 4.2.)
- Om risknivåer antagits av FMV, ska det tydligt framgå i SSD.
- I Systemsäkerhetsdeklarationen ska också framgå att FMV utfärdar en systemsäkerhetsdeklaration för det aktuella tekniska systemet, i aktuell konfiguration för användning i enlighet med och för brukande i den användningsmiljö som finns beskriven i huvuddokument samt i refererad teknisk dokumentation. Det ska även framgå att aktuell systemsäkerhetsdeklaration inte gäller för annan användning eller i annan användningsmiljö.
- I Systemsäkerhetsdeklarationen ska framgå vem som är föredragande, vem som har deltagit i den slutgiltiga beredningen, vem som fastställer samt vem som samråder beslutet.

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.

4 COTS/Trivial materiel

4.1 Klassning

Möjligheterna att klassa ett system som COTS eller "Trivial materiel" är ganska begränsade enligt H SystSäk. Eftersom viss tolkningsmån finns, kan bedömningen ibland vara svår. "Merarbetet" som det innebär att inte kunna klassa ett system som "COTS/Trivial materiel" får dock inte ge upphov till några genvägar.

System som klassas som COTS ska vara civilt godkända och certifierade produkter, ofta via CE-märkning. Av DesignA godkänd 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.

Förutom bedömningskriterier enligt ovan samt i PHL-mall 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, höjder...)?

Om svaret på någon av de ovanstående frågorna är "Ja", är det troligt att systemet inte kan klassas som "COTS/Trivial materiel". Om svaret på samtliga ovanstående frågor är ett tydligt "Nej" och övriga villkor är uppfyllda, bl.a. enligt PHL (mall för Led), ska systemet kunna klassas som "COTS/Trivial materiel".

4.2 Systemsäkerhetsdeklaration

Det finns centralt framtagna mallar för FMV Systemsäkerhetsgodkännande/ Systemsäkerhetsdeklaration på FMV. I de fall mall för Systemsäkerhetsdeklaration saknas, kan mall för FMV systemsäkerhetsgodkännande användas tills vidare för att utforma FMV SSD. Då behöver lämpliga ändringar göras som att byta ut "Systemsäkerhetsgodkännande" till "Systemsäkerhetsdeklaration".

En särskild sådan mall finns för COTS och Trivial materiel f, men det finns goda anledningar att ändå använda mallen för mer komplexa system. Bland annat behöver tillåtet användningsområde och -miljö beskrivas, och krav- och restriktionshantering ska redovisas lika noggrant för COTS och Trivial materiel som för andra system.

En systemsäkerhetsdeklaration ska innehålla information motsvarande avsnitt 3.3, dock med följande tillåtna skillnader:

Datum	Diarienummer	Ärendetyp
2018-12-18	11FMV1262-10:1	3.1
	Dokumentnummer	Sida
	442892	10(15)

- SSD för COTS och ”Trivial materiel” behöver normalt endast PHL som bilaga (se Fig. 1). Andra bilagor kan också behöva bifogas. Exempel: om det i huvuddokumentet inte återges väsentlig information, ska denna information åtminstone vara hänvisad till och bifogad som en bilaga/del av bilaga.
- Det behöver inte framgå att riskstängning m.m. är utförd. Det ska framgå att processen för COTS/Trivial materiel har följts, med bedömningar gjorda i PHL, och att t.ex. leverantörens arbete inför CE-märkning (eller annan kravställd civil certifiering) anses tillräcklig.
- Det bör framgå att ett SCA inte krävs och inte är framtaget, m.h.t. klassning som COTS/Trivial materiel, enligt gällande process.
- Information om att samtliga systemsäkerhetskrav är uppfyllda behöver kompletteras med information om att risknivåer inte har använts m.h.t. klassning som COTS/Trivial materiel enligt gällande process.

5 Hantering av ändringar relaterat till systemsäkerhet

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 FM har beställt stöd avseende ändringshantering (eller ej överlämnade system) ska nedan process följas så länge detta inte går emot instruktionerna i respektive beställning.

5.1 Allmänt om ändring

Tekniskt utförande, användningsområde och användningsmiljö för systemet är definierat i gällande FMV systemsäkerhetsdeklaration respektive FM (tidigare FMV) Systemsäkerhetsgodkännande. Vid ändringar av systemet krävs det en systemsäkerhetsrelaterad ändringshantering. Det finns i grunden tre sätt att utföra en systemsäkerhetsändring (Fig. 3):

1. **Större ändring** (Ändrat tekniskt system)
Större ändring gäller då systemsäkerheten vid införd ändring påverkas mer än försumbart. Då krävs det en ny FMV Systemsäkerhetsdeklaration och ett nytt FM Systemsäkerhetsgodkännande. Systemsäkerhetsarbete utförs enligt normala rutiner för en ny Systemsäkerhetsdeklaration (samt därefter ett nytt Systemsäkerhetsgodkännande från FM) och beslut tas enligt gällande delegeringar.
2. **Justering/Smärre ändring** (Justerat tekniskt system)
Justering/Smärre ändring gäller för enklare ändringar, där 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 mallen ”Systemsäkerhetsbeslut Justering/ Smärre Ändring” ska användas.
3. **Beslut om 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.

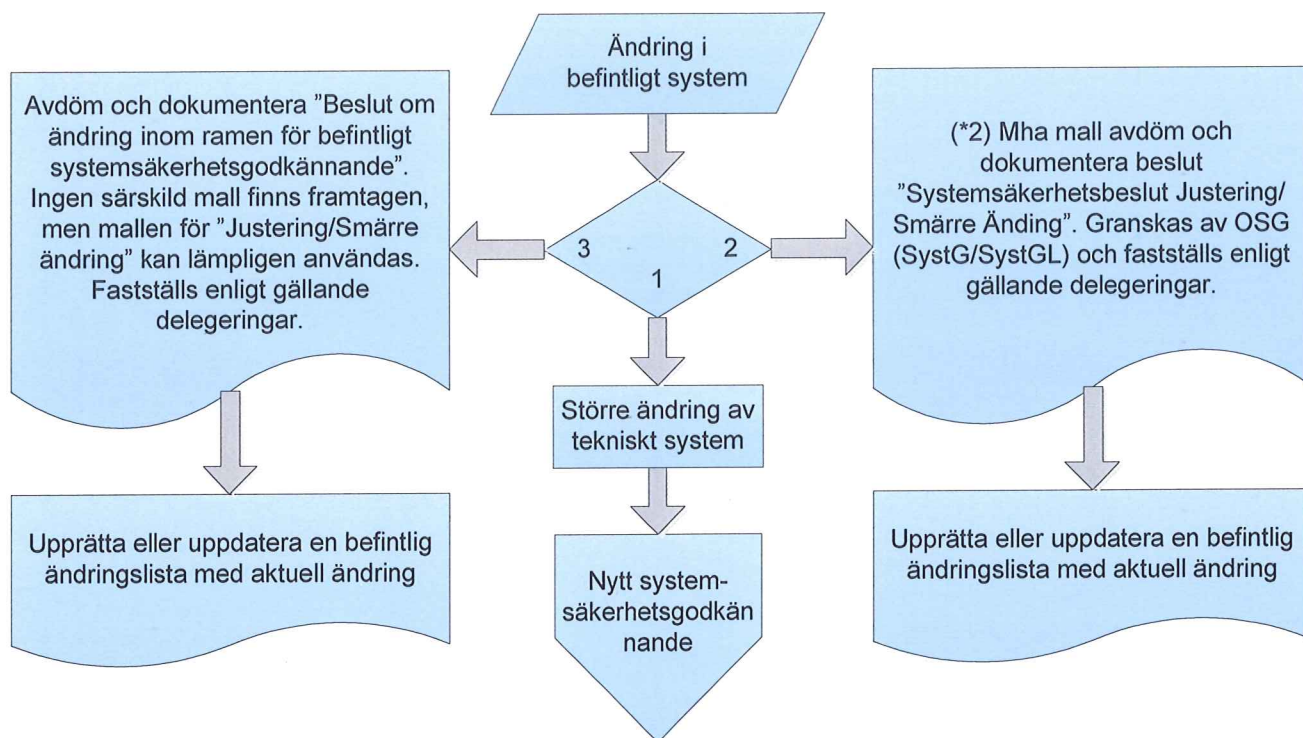


Fig. 3. Systemsäkerhetshantering av ändringar i befintligt system.

5.2 Bedömning av systemsäkerhetspåverkan

Följande råd finns som hjälp vid bedömning och vid dokumentering av bedömning, ifall systemsäkerhetspåverkan finns (d.v.s. mer än försumbar påverkan) eller ej (d.v.s. försumbar påverkan), för bedömd ändring.

Om *ingen* av följande villkor uppfyllts, kan hela ändringen klassas som "Försumbar" (ingen alternativt försumbar 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.

Datum	Diarienummer	Ärendetyp
2018-12-18	11FMV1262-10:1	3.1
	Dokumentnummer	Sida
	442892	12(15)

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 gränssytor.

Endast i de fall där en ändring klassas som försumbar ska Systemsäkerhetsbeslut Justering/Smärre ändring tas fram enligt nedan.

5.3 Dokumentera Systemsäkerhetsbeslut Justering/Smärre Ändring

Dokumentera Systemsäkerhetsbeslut Justering/Smärre ändring med ingen eller försumbar systemsäkerhetspåverkan.

Beslutet ska bland annat innehålla följande delar:

- Information om att nuvarande SS (och SSD) bedöms vara giltigt även för den nya versionen/konfigurationen av systemet.
- Information om att en ny bedömning har gjorts som ger att systemsäkerhetspåverkan vid ändring endast är försumbar
- En beskrivning av bedömningen, hur den är utförd.
- Versionsidentifikation på systemet före och efter ändring.
- I det samlade underlaget skall det klart framgå hela systemets omfattning efter uppdatering. Det ska bl.a. finnas angivet en systembeskrivning, tillåtna miljöer, gränssytor och relevanta delsystem.
- Gällande SS och/eller i förekommande fall SSD skall bifogas och hänvisas till.
- Namn, organisation och befattning på beslutande samt andra relevanta roller.

Om inget annat framgår ska fastställd mall "Systemsäkerhetsbeslut Justering/Smärre Ändring" för Led användas. Systemsäkerhetsbeslut Justering/Smärre ändring fastställs enligt gällande delegeringar.

6 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 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.

7 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.

8 System av system

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

1. En systemsäkerhetsdeklaration och ett systemsäkerhetsutlåtande tas fram för det övergripande systemet.
2. Befintliga systemsäkerhetsgodkännanden (och/eller SSD) för ingående delsystem kan användas som del av Systemsäkerhetsdeklaration för övergripande system. Dessa ska då refereras till samt biläggas inklusive viktiga bilagor som rikslistor/risklogg inklusive riskstängning. Kontroll av kvalitén ska göras och exempelvis mycket gamla godkännanden bör inte återanvändas utan en förnyad process. Kontroll ska även göras att systemsäkerhetsnivån, mot vilken tidigare delsystem är godkända, inte väsentligt skiljer sig från kravet som gäller för det övergripande systemet.
3. För tidigare ej godkända delsystem och för det övergripande systemet (inklusive integrationsrisker), görs normal systemsäkerhetsverksamhet inklusive riskbedömningar och riskstängning. Risker för tidigare godkända 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 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 risker på ett enkelt sätt. Detta oavsett om dessa risker är bedömda inom ramen för ett tidigare systemsäkerhetsgodkänt/deklarerat 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.

9 Återtagande av materiel från FM

FM har vidmakthållandeansvar för system som är överlämnade från FMV. Det innebär bland annat att FM 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 FM som deklarerar systemets aktuella status vid tidpunkten för återtagande på FMV. Detta underlag ska normalt användas som grund för vidare systemsäkerhetsarbete. Om inte sådant underlag erhålls, behöver FMV utföra systemsäkerhetsarbete från grunden, likt för ett helt nytt system.

10 Språk

H SystSäk¹ ställer vissa krav på språk i systemsäkerhetsdokumentation som manualer etc. Bland annat anges att ”DesignA ansvarar för att specificera krav på dokumentation och säkerställer att erforderliga dokument översätts till svenska”.

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.

¹ Se H SystSäk 2011 del 1 kap 5.10.4.



Datum	Diarienummer	Ärendetyp
2018-12-18	11FMV1262-10:1	3.1
	Dokumentnummer	Sida
	442892	15(15)

11 Beslut

Beslut att föreliggande handlingsregel gäller från och med 2019-01-01 samt att tidigare utgåva 11FMV1262-9:2 upphävs från och med samma datum, har fattats av TC Led Lars Burström. 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 mallar för Preliminär Riskkällelista (PHL) samt Systemsäkerhetsbeslut Justering/Smärre ändring.

Lars Burström
TC Led

Adam Narel
CI system- och flygsäkerhet Led

Sändlista:

Arkiv

Bilagor

- | | |
|----------|---|
| Bilaga 1 | Mall med anvisning för Riskkällelista (PHL) för Led |
| Bilaga 2 | Mall med anvisning för Systemsäkerhetsbeslut Justering/Smärre ändring |