System av system på nivå 4

2013-06-18 13FMV5921-8:1

Härmed fastställs ”Leverans av ISD version 2.0” för delgivning till Försvarsmakten Högkvarteret till LedS CIO som remissutgåva.

Deltagare vid föredragningen har varit föredragande och beslutande.

Johan Wåhlén
Chef Generell Produktionsstöd vid AK Gemensam

Dan Olofsson

Tryck:

REVISIONSHISTORIK

Version	Datum	Uppdatering	Uppdaterad av	Fastställd av
2.0	2013-06-18	Fastställd version	Dan Olofsson	DAOLO
1.0	2012-03-14	Uppdateringar för fastställande 1.0	Dan Olofsson	DAOLO

Innehåll

1 Sammanfattning

Med begreppet ”system av system” avses ett system som sätts samman av ett antal mindre delsystem och/eller komponenter. Med ”verifiering system av system” avses det arbete som måste utföras för att säkerställa att informationssäkerheten upprätthålls i det sammansatta systemet.

”System av system” sätts samman på olika nivåer där den lägsta nivån representerar enskilda komponenter, mellanliggande nivåer representeras av sammansatta system i form av ledningssystem och plattformar och den högsta nivån representerar sammansättningar av system på förbandsnivå.

Tidigare har främst verifieringar för enskilda delsystem och komponenter genomförts. Denna instruktion har tagits fram för att FMV på ett effektiv sätt ska kunna garantera och verifiera helheten för ett ”system av system” på en högre nivå.

Genom instruktionen säkerställs att nya aspekter som tillkommer då ett antal delsystem sätts samman till ett större system kan tas om hand. Den tillser även att nytta kan dras av de kravbilder och granskningar som tidigare tagits fram för de delsystem som ska ingå i det större systemet.

Instruktionen riktar sig till personer som ska utföra verifiering på en sammansatt nivå men kan även användas av de som ska sätta samman ”system av system” samt de som tar fram Systemdefinitioner för att säkerställa att verifieringsaspekter kommer med. Även FM CIO auktorisationsgruppen och MUST utgör målgrupper.

Instruktionen är skriven dels utifrån ett antal generella aspekter som alltid måste beaktas då ett antal system sätts samman till ett större system, dels utifrån ett antal olika scenarion som kan uppstå när system integreras. Varje scenario representerar ett typfall. Syftet med scenariobeskrivningen är att den som tar del av instruktionen ska kunna identifiera vad som är viktigt för just det typfall som gäller för varje specifik verifiering.

Instruktionen innehåller dessutom ett kapitel som beskriver hur tidigare framtagna kravbilder och genomförda granskningar kan återanvändas. På det sättet säkerställs att allt arbete inte görs om i onödan och att förutsättningar om hur varje komponent är tänkt att användas omhändertas.

Fördelar med att följa instruktionen är att systemintegratören:

- Får en överblick över vilka krav som systemet har att uppfylla.
- Får förståelse hur helheten kan verifieras,
- Kan leverera på förmågenivå.
- Uppnår kostnadseffektivitet genom maximal optimering av ingående komponenter.
- Kan dra nytta av tidigare framtagna kravbilder och granskningar.

Läsaren bör ha erfarenheter av systemintegration och teknisk förståelse för systemarbete. Vidare bör läsaren vara bekant med Försvarsmaktens auktorisation av IT-system, med fokus på kravställning, målformulering och granskning/verifiering.

2 Inledning

Dokumentet beskriver olika aspekter att beakta och ta hänsyn till vid verifiering system av system på nivå 4 och är baserat på sju olika scenarion som kan uppstå då nivå 5-system sätts samman till ett system på nivå 4. Instruktionen kan även användas vid framtagning av SYD (SYstemDefinition) för stöd i de delar som omfattar informationssäkerhet (Information Assurance – IA). Det förutsättningsskapande arbetet som beskrivs i FMV AK Led:s Instruktion för säkerhetsaspekter vid framtagning av SYD, är input till denna instruktion, se *[2]*.

2.1 Syfte

Syftet med instruktionen är att möjliggöra verifiering system av system på nivå 4 ur ett informationssäkerhetsperspektiv. Instruktionen är framtagen för att säkerställa att nya aspekter som tillkommer då man sätter samman ett antal delsystem till ett större system tas om hand men även för att man ska kunna dra nytta av de kravbilder och granskningar som tidigare tagits fram för de system som ska ingå i nivå 4-systemet.

2.2 Målgrupp

Huvudsaklig målgrupp är de som ska verifiera system av system på nivå 4 men även de som ska ta fram system på nivå 4 för att tydliggöra hur ett resonemang ska föras för att tillse att system av system kan verifieras samt att system av system har de förutsättningar som krävs för att bli godkänt. Instruktionen kan även användas då Systemdefinitioner ska tas fram för att säkerställa att verifieringsaspekter kommer med i dessa. Instruktionens målgrupper utgörs även av FM CIO auktorisationsgruppen samt MUST i syfte att de ska förstå FMV:s arbetssätt vad gäller verifiering system av system.

2.3 Bakgrund

Följande bakgrundsbeskrivning till verifiering system av system är hämtat ur dokumentet Avsiktsförklaring IA, se *[3]*.

I nuläget får FMV i huvudsak beställningar från Försvarsmakten för produkter på nivå 5 och tar därför fram säkerhetstekniskt ackrediteringsunderlag (STAU 1.0 - 4.0) på nivå 5. Vid sammansättning av nivå 5-produkter i ett ledningssystem har FMV idag en utmaning i att genomföra ett effektivt arbete för att genomföra verifieringar och ta fram STAU för nivå 4. Detta begränsar möjligheten att garantera att helheten fungerar eller blir godkänd.

Ett centralt krav är verifiering av gränsytan utifrån ett säkerhetsperspektiv, dvs hotbild. Detta arbete ligger väl i linje med arbetet i ”SYD-fabriken” och för större funktionsobjekt.

Samordning i tiden vad gäller definierade beslutspunkter för utveckling av de enskilda delarna inom system av system är viktig utifrån ett IA-perspektiv. Utformningen av IT-säkerhetslösningen i system av system är beroende på vilka skyddsmekanismer som de olika delsystemen kan erbjuda, och vilka tekniska svagheter som faktiskt finns i de enskilda systemen på nivå 5 samt eventuella tillkommande risker, se 4.1. Det är viktigt att inte göra suboptimeringar som kan bli fallet om man inte har den helhetsbild som system av system erbjuder genom dess säkerhetsarkitektur.

Det är viktigt att kunna verifiera IT-säkerheten i system av system. Detta görs genom säkerhetsgranskning och verifieringar precis som för nivå 5. För detta krävs bl a en verifieringsmiljö. Planeringen för verifiering bör dels utgå från de sårbarheter och risker som identifierats i nivå 5- produkterna och kompletteras med den verifiering som behövs för tillkommande risker när man realiserar *system av system*.

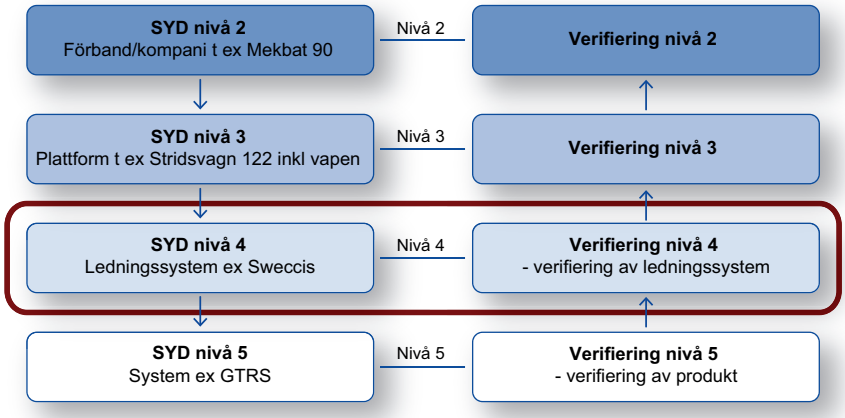

Bild 2:1 Olika nivåer av SYD och verifiering system av system.

2.4 Definitioner

Med begreppet ”*system av system*” avses ett system som sätts samman av ett antal mindre delsystem och/eller komponenter.

Med en ”*verifierad*” produkt avses en IT-säkerhetslösning som har blivit granskad gentemot uppställd kravbild. En produkt som är auktoriserad eller ackrediterad kan anses vara ”verifierad”. Kravbilden kan också vara på en högre nivå där t.ex. uppfyllnad av säkerhetsmål granskas, även detta inräknas då i begreppet verifiering.

Med ”*verifiering system av system*” avses det arbete som måste utföras för att säkerställa att informationssäkerheten upprätthålls i det sammansatta systemet (nivå 4).

Med begreppet ”*ackreditering*” avses dels ett sådant godkännande av ett IT-system från säkerhetssynpunkt som avses i 12 § tredje stycket säkerhetsskyddsförordningen (1996:633), dels ett godkännande från säkerhetssynpunkt i övrigt av övriga IT-system.

Med begreppet ”*auktorisation*” avses bemyndigande för produktägare att utveckla Försvarsmaktens IT-verksamhet.

3 Basfakta

3.1 Referenser

Ref.	Dokumentnamn	Dok. id.
[1]	FMV Vägledning ISD och SE	13FMV5921-3:1
[2]	FMV AK Led:s Instruktion för säkerhetsaspekter vid framtagning av SYD	Draft
[3]	Avsiktsförklaring för teknikområde Information Assurance (IA)	Draft
[4]	Direktiv för Försvarsmaktens informationsteknikverksamhet (DIT 04)	HKV 09 626:78369

3.2 Begrepp och förkortningar

Begrepp/förkortning	Förklaring
Ackreditering	Godkännande av ett IT-system från säkerhetssynpunkt, [se DIT 04 ref 4]
AD	Active Directory
Auktorisation	Bemyndigande för produktägare att utveckla Försvarsmaktens IT-verksamhet [se DIT 04 ref 4].
B1	Beslutspunkt i Försvarsmaktens IT-livscykelmodell avseende behovsberedning
B2	Beslutspunkt i Försvarsmaktens IT-livscykelmodell avseende konceptgenerering
B4	Beslutspunkt i Försvarsmaktens IT-livscykelmodell avseende anskaffning
B5	Beslutspunkt i Försvarsmaktens IT-livscykelmodell avseende beslut om användning
BKS	Behörighetskontrollsystem
CC	Common Criteria – standard och metod för utvärdering av säkerheten i IT-produkter och system
FFS	Försvarets författningssamling
FIB	Försvarsmaktens interna bestämmelser

Begrepp/förkortning	Förklaring
FM	Försvarsmakten
IA	Information Assurance
IT-system	System med teknik som hanterar och utbyter information med omgivningen
IT-verksamhet	Verksamhet för IT-system
KSF	Krav på Säkerhetsfunktioner
MUST	Militära underrättelse- och säkerhetstjänsten
Nivå 4	Sammansättning av nivå 5-system/komponenter
Nivå 5	Enskilt, avgränsat system eller komponent/produkt
SSS	System/Subsystem Specification
STAU	Säkerhetstekniskt ackrediteringsunderlag
SYD	Systemdefinition
Säkerhetsfunktion	En eller flera funktioner i ett IT-system som upprätthåller säkerheten enligt regler om hur uppgifter i IT-systemet ska skyddas
Säkerhetsmekanism	Teknik som används vid realisering av en säkerhetsfunktion eller del av denna
Säkerhetsmålsättning	Beskrivning av de säkerhetskrav och bedömanden som utgör underlag för utvecklingen av ett IT-system.
TAU	Tekniskt ackrediteringsunderlag
TOE	Target of Evaluation

4 Instruktion

Vid framtagning av SYD och verifiering system av system på nivå 4 finns sju dimensionerande scenarion definierade. För var och ett av dessa scenarion finns ett antal specifika aspekter som bör beaktas, se *avsnitt 4.2*. Det finns även ett antal generella aspekter att beakta vid verifiering system av system, se *avsnitt 4.1*. Dessa generella aspekter gäller oavsett vilket scenario som är tillämpligt. Instruktionen kan användas som underlag för informationssäkerhetsaspekter i SYD-fabriken, se instruktion i *[2]*.

4.1 Generella aspekter

Nedan presenteras de generella aspekter och frågeställningar som initialt måste tas ställning till då verifiering system av system görs på nivå 4. Dessa aspekter är även viktiga att inkludera i SYD-fabriken:

- Hur kan systemet avgränsas i delsystem?
- Vilka gränsytor måste beaktas? Alla gränsytor, från det fysiska lagret till applikationslagret, ska beaktas.
- Vilken är hotbilden mot de identifierade gränsytorna?
- Vilka nya förutsättningar tillkommer från delsystemen?
  - Hur ser säkerhetsarkitekturen ut?
  - Vilken säkerhetsnivå i sin helhet med organisation, personal, IT-säkerhet mm råder?
- Vilka nya förutsättningar utifrån nya tillämpningar tillkommer?
- I vilken kontext är godkända system verifierade? I vilken säkerhetsmiljö, med vilka antaganden om hot och styrande regler etc. har verifieringen gjorts?

Den som beslutar om att en förändring av ett system av system ska göras är också ansvarig för att en bedömning görs om huruvida detta är säkerhetspåverkande eller inte. Denna bedömning är inte trivial, utan det är en komplex fråga där god kompetens inom IT-säkerhet krävs. Bedömningen

görs genom en delta-beskrivning. I en delta-beskrivning ingår även en bakomliggande analys. En delta-beskrivning ska utföras och dokumenteras enligt:

1. Beskrivning av förändringen.
2. Analys av påverkan på säkerhetsfunktioner och/eller säkerhetsmiljö
3. Beslut, d v s bedömning, om huruvida detta är säkerhetspåverkande eller inte.

4.2 Dimensionerande scenarion

Det första steget som bör genomföras för att kunna verifiera system av system på nivå 4 är att definiera vilket av nedanstående scenarion som gäller. Scenario 1-3 beskriver fall där ett nytt nivå 4-system sätts samman av nivå 5-produkter medan scenario 4-7 beskriver fall där ett befintligt nivå 4-system utsätts för förändring.

Ta fram ett nivå 4-system:

- Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem (produkter).
- Scenario 2 – Bygga nivå 4-system av dels verifierade och dels ej verifierade nivå 5-produkter.
- Scenario 3 – Bygga nivå 4-system av ej verifierade nivå 5-produkter.

Ändra i ett nivå 4-system:

- Scenario 4 – Ändringar i ett verifierat nivå 4-system.
- Scenario 5 – Lägga till verifierad nivå 5-produkt i ett verifierat nivå 4-system.
- Scenario 6 – Ta bort verifierad nivå 5-produkt i ett verifierat nivå 4-system.
- Scenario 7 – Ändringar i omgivande miljö för ett verifierat nivå 4-system.

Om ett nivå 4-system inte inbegrips av något av ovanstående scenarion kan ändå aspekter från det eller de scenarion som bäst stämmer överens med tillståndet tillämpas. Hur de sju scenariona ska hanteras beskrivs nedan.

Varje scenario illustreras med en figur. Den yttre ramen motsvarar ett system på nivå 4 och de inre rutorna illustrerar de generiska delsystemen 1, 2 och 3. Varje system respektive delsystem kan vara verifierat (grön ring) eller ej verifierat (röd ring). Detsamma gäller för interna och externa gränsytor (grönt respektive rött streck). Nivå 4-systemet i sin helhet kan vara verifierat (grön ram) eller ej verifierat (röd ram).

4.2.1 Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem (produkter)

Följande figur illustrerar scenariot.

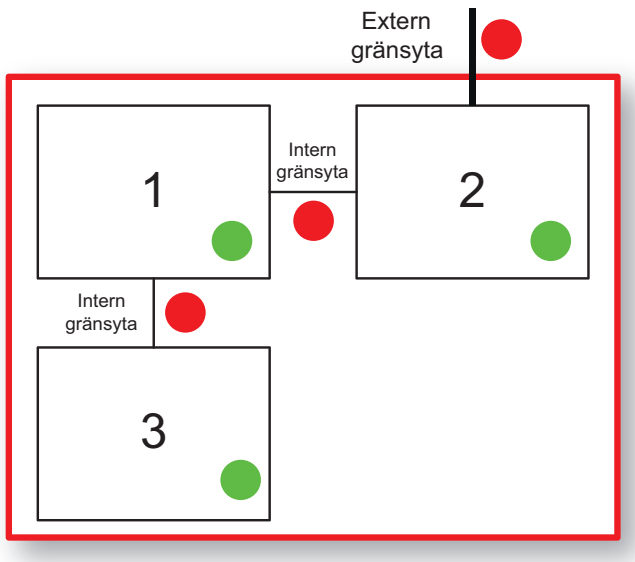

Bild 4:1 Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem (produkter)

4.2.1.1 Förutsättningar

Vid verifiering av ett system där samtliga delsystem redan är verifierade finns STAU för samtliga delsystem. Delsystemen är redan verifierade på nivå 5 och respektive delsystem verifieras då inte på nytt, endast helheten verifieras.

Verifiering på nivå 4 i detta fall sker med utgångspunkt från hela systemets förutsättningar såsom:

- miljö
- hotbild
- systemkontext (hur systemet ska användas)
- delsystemkontext (hur delsystemen är avsedda att användas)
- fastställda designprinciper.

En ytterligare parametrar att ta hänsyn till är om det nya systemet gör något som strider mot de STAU1–4 som redan tagits fram.

4.2.1.2 Leverabler

Det som ska tas fram för helheten (d v s nivå 4) är:

1. Krav på systemdesign:
   1.1. Systemarkitektur.
   1.2. Säkerhetsrelaterade krav för samverkan.
   1.3. Gemensamma säkerhetsfunktioner (t ex BKS, AD och central säkerhetsloggning).
2. Säkerhetsmålsättning[1] (för helheten, nivå 4):
   2.1. Säkerhetsanalys (för att klarlägga sekretessnivån och aggregering av information).
   2.2. Hot-, risk- och sårbarhetsanalys (inkl gränsytor mellan delsystemen, hela protokollstacken samt vad som finns på mottagarsidan ska beskrivas).
   2.3. Verksamhetsanalys.
   2.4. Författningsanalys
   2.5. Granskning av ingående delsystems (nivå 5) säkerhetsmålsättning för att klarlägga dessas kontext och miljörelaterade krav.
3. Systembeskrivning på nivå 4:
   3.1. Beskrivning av interna och externa gränsytor.
   3.2. Visa den gemensamma säkerhetsarkitekturen.
   3.3. Redovisa eventuellt val av konfiguration om ett delsystem på nivå 5 har gett olika konfigurering att välja mellan vid sammansättning till större systemet.

4. STAU (för nivå 4):
   4.1. Granskning av säkerhetsmålens uppfyllnad
   4.2. Redovisning av hur kvarstående brister ska omhändertas och visa på att det finns en åtgärdslista.
   4.3. Redovisning av vilka krav på användning som finns för systemet i sin helhet.

4.2.1.3 Tester

Tester som måste göras för att verifiera helheten:

- Teoretisk säkerhetsgranskning.
- Funktionstester.
- Verifiering (granskning mot teknisk specifikation, ska göras av oberoende instans).
- Validering (granskning på funktionsnivå, görs ofta av användaren/representant).
- Penetrationstester (oberoende instans).

1. Under förutsättning att det inte redan finns en Säkerhetsmålsättning för nivå 4-systemet.

4.2.2 Scenario 2 – Bygga nivå 4-system av dels verifierade och dels ej verifierade nivå 5-produkter

Följande figur illustrerar scenariot.

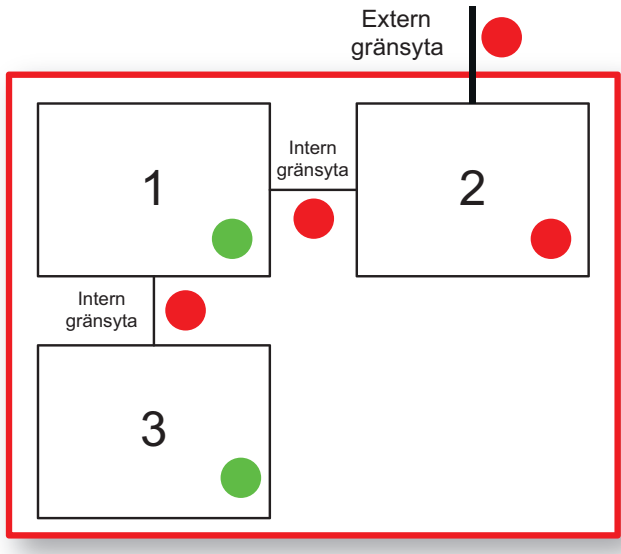

Bild 4:2 Scenario 2 - Bygga nivå 4-system av dels verifierade och dels ej verifierade nivå 5-produkter

4.2.2.1 Förutsättningar

För att kunna hantera verifieringen av ett helt nytt system måste detta avgränsas i delsystem, vilket sker i designfasen.

För varje respektive delsystem måste beslutas vilket av följande alternativ som gäller:

a. Delsystemet är användbart endast i detta system.

b. Delsystemet ska användas även i andra sammanhang.

4.2.2.2 Alternativ A – Delsystemet är användbart endast i detta system

För alternativ A gäller:

- Delsystemet betraktas som systemunikt.
- Delsystemet måste ingå i STAU för hela systemet (dvs nivå 4).
- Utökad hot-, risk- och sårbarhetsanalys.
- Det måste tillses att granskningen på nivå 4 är tillräckligt detaljerad för att motsvara en granskning av en nivå 5-produkt.

Verifieringen utförs enligt *Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem (produkter)*.

För alternativ A måste hänsyn tas till följande risker vid framtagning av Säkerhetsmålsättning samt genomförande av granskning:

- Säkerhetsmålsättningen för nivå 4-system blir för detaljerad.
- Säkerhetsmålsättningen för den overifierade nivå 5-produkten blir för översiktlig.

4.2.2.3 Alternativ B – Delsystemet ska användas även i andra sammanhang

För alternativ B gäller:

- Delsystemet är möjligt att avgränsa
- En separat Säkerhetsmålsättning ska tas fram på nivå 5.
- Ett separat STAU ska tas fram på nivå 5
- STAU och Säkerhetsmålsättning blir användbart även i andra sammansättningar på nivå 4
- Separat säkerhetsgranskning av delsystemet mot Säkerhetsmålsättning.

För alternativ B utförs två aktiviteter; först separat verifiering av delsystemet på nivå 5, därefter verifiering enligt *Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem (produkter)*.

4.2.3 Scenario 3 – Bygga nivå 4-system av ej verifierade nivå 5-produkter

Följande figur illustrerar scenariot.

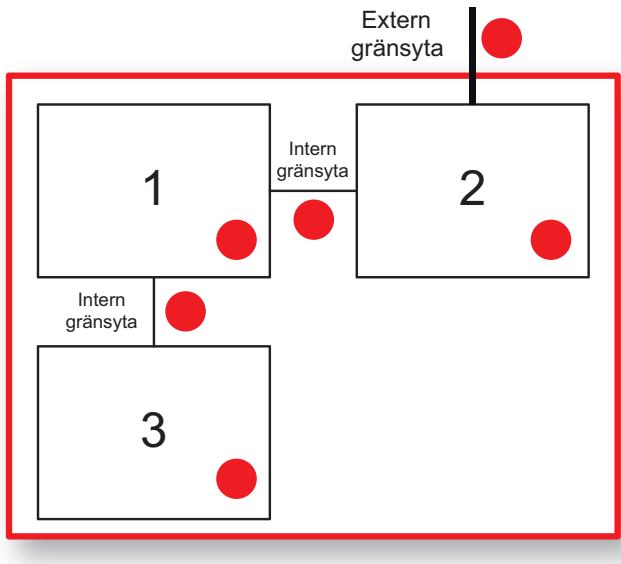

Bild 4:3 Scenario 3 - Bygga nivå 4-system av ej verifierade nivå 5-produkter

Verifiering för detta scenario sker enligt motsvarande steg som *Scenario 2 – Bygga nivå 4-system av dels verifierade och dels ej verifierade nivå 5-produkter*. Skillnaden är att omfattningen av verifieringsarbetet ökar eftersom samtliga delsystem är overifierade.

4.2.4 Scenario 4 – Ändringar i ett verifierat nivå 4-system

Följande figur illustrerar scenariot.

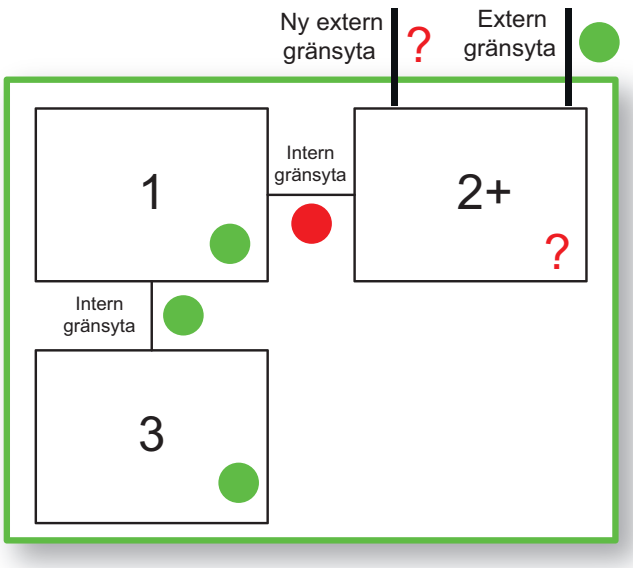

Bild 4:4 Scenario 4 - Ändringar i ett verifierat nivå 4-system

4.2.4.1 Förutsättningar

För att avgöra huruvida säkerhetsfunktionaliteten/säkerhetsarkitekturen påverkas eller inte vid ändring av något delsystem eller förändringar i interna och/eller externa gränsytor måste en bedömning[1] göras genom att värdera förändringar i:

- Systemarkitektur inklusive säkerhetsarkitektur och gränsytor.
- Systembeskrivning.

Om det nya systemet skiljer sig avseende säkerhetsfunktionalitet måste en ny verifiering göras där:

- Ställning tas till konsekvenserna av förändringen och hur stora dessa är.
- Avgränsning till berört område kan göras.
- information om förändringar i konfiguration och hur detta påverkar systemet och gränssnitt ska beskrivas.

1. Bedömningen ska initieras av den som fattar beslut om förändringen.

En bedömning måste göras av vilket av följande alternativ som gäller:

a. Det nya nivå 4-systemet är endast en ny version av det gamla

b. Det nya nivå 4-systemet ska betraktas som ett helt nytt system.

Se också *avsnitt 4.1*.

4.2.4.2 Alternativ A – Det nya nivå 4-systemet är endast en ny version av det gamla

För alternativ A ovan kan den nya verifieringen dokumenteras i ett delta-STAU. I ett delta-STAU beskrivs endast förändringen som gjorts. Här avgörs om förändringen har påverkan på systemet eller på miljön som system är avsett att verka i. Förändringar ska dokumenteras, men inget övrigt säkerhetsarbete behöver göras. Här finns det krav på dokumenterade beslut.

4.2.4.3 Alternativ B – Det nya nivå 4-systemet ska betraktas som ett helt nytt system

Verifieringen utförs enligt Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem och följande gäller:

- En separat Säkerhetsmålsättning ska tas fram på nivå 4.
- Ett separat STAU ska tas fram på nivå 4.

4.2.5 Scenario 5 – Lägga till verifierad nivå 5-produkt i ett verifierat nivå 4-system

Följande figur illustrerar scenariot.

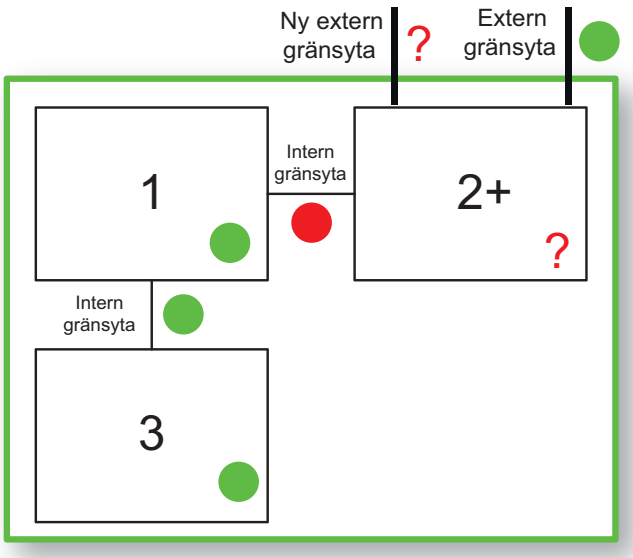

Bild 4:5 Scenario 5 - Lägga till verifierad nivå 5-produkt i ett verifierat nivå 4-system

4.2.5.1 Förutsättningar

I detta scenario bör följande punkter kontrolleras:

- Är det ett säkerhetsrelevant delsystem som läggs till?
- Tillkommer det några nya externa gränsytor?
- Tillkommer det några nya interna gränsytor?
- Påverkar det nya delsystemet det verifierade systemet på ett negativt sätt (t ex prestandamässigt)?
- Tillkommer det några nya hot mot systemet?

För att avgöra huruvida säkerhetsfunktionaliteten/säkerhetsarkitekturen påverkas eller inte vid tillägg av ett delsystem måste en analys göras för att värdera förändringar i:

- Systemarkitektur inklusive säkerhetsarkitektur.
- Systembeskrivning.
- Interna gränsytor (tillkommande gränsytor är inte verifierade).

Om det nya systemet skiljer sig avseende säkerhetsfunktionalitet måste en ny verifiering göras där:

- Ställning tas till konsekvenserna av förändringen och hur stora dessa är.
- Avgränsning till berört område kan göras.
- Information om förändringar i konfiguration och hur detta påverkar systemet och gränssnitt ska beskrivas.

Ovanstående punkter gäller även då det tillkommer nya hot då delsystemet läggs till.

En bedömning måste göras av vilket av följande alternativ som gäller:

a. Det nya nivå 4-systemet är endast en ny version av det gamla.

b. Det nya nivå 4-systemet ska betraktas som ett helt nytt system.

4.2.5.2 Alternativ A – Det nya nivå 4-systemet är endast en ny version av det gamla

För alternativ A ovan kan den nya verifieringen dokumenteras i ett delta-STAU. I ett delta-STAU beskrivs endast förändringen som gjorts.

4.2.5.3 Alternativ B – Det nya nivå 4-systemet ska betraktas som ett helt nytt system

Verifieringen utförs enligt Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem och följande gäller:

- En separat Säkerhetsmålsättning ska tas fram på nivå 4.
- Ett separat STAU ska tas fram på nivå 4.

4.2.6 Scenario 6 – Ta bort verifierad nivå 5-produkt i ett verifierat nivå 4-system

Följande figur illustrerar scenariot:

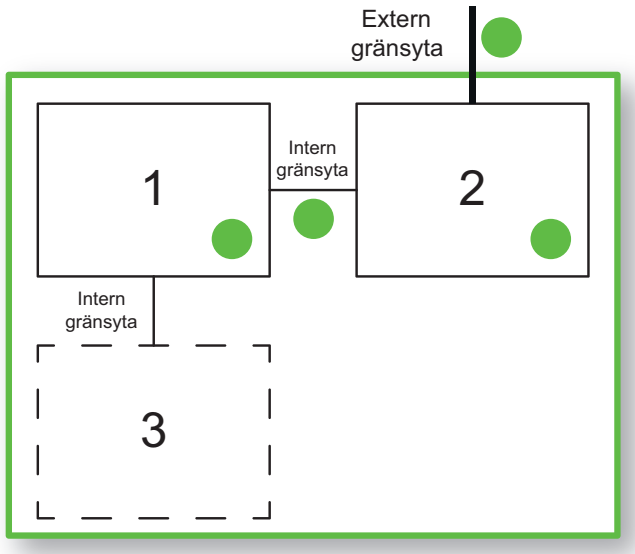

Bild 4:6 Scenario 6 - Ta bort verifierad nivå 5-produkt i ett verifierat nivå 4-system

4.2.6.1 Förutsättningar

I detta scenario bör följande punkter kontrolleras:

- Är det ett säkerhetsrelevant delsystem som tas bort?
- Påverkar det borttagna delsystemet det verifierade systemet på ett negativt sätt (t ex prestandamässigt)?
- Tillkommer det några nya hot mot systemet då delsystemet tas bort?
- Reduceras befintlig hotbild då delsystemet tas bort?
  I detta fall kan det då finnas säkerhetsfunktioner som blir överflödiga.

För att avgöra huruvida säkerhetsfunktionaliteten/säkerhetsarkitekturen påverkas eller inte vid borttagning av ett delsystem måste en bedömning göras genom att värdera förändringar i:

- Systemarkitektur inklusive säkerhetsarkitektur.
- Systembeskrivning.

Om det nya systemet skiljer sig avseende säkerhetsfunktionalitet måste en ny verifiering göras där:

- Ställning tas till konsekvenserna av förändringen och hur stora dessa är
- kan avgränsas till berört område
- information om förändringar i konfiguration och hur detta påverkar systemet och gränssnitt ska beskrivas

Ovanstående gäller också om det tillkommer nya hot då delsystemet tas bort.

En bedömning måste göras av vilket av följande alternativ som gäller:

a. Det nya nivå 4-systemet är endast en ny version av det gamla.

b. Det nya nivå 4-systemet ska betraktas som ett helt nytt system

4.2.6.2 Alternativ A – Det nya nivå 4-systemet är endast en ny version av det gamla

För alternativ A ovan kan den nya verifieringen dokumenteras i ett delta-STAU. I ett delta-STAU beskrivs endast förändringen som gjorts.

4.2.6.3 Alternativ B – Det nya nivå 4-systemet ska betraktas som ett helt nytt system

Verifieringen utförs enligt Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem och följande gäller:

- En separat Säkerhetsmålsättning ska tas fram på nivå 4.
- Ett separat STAU ska tas fram på nivå 4.

4.2.7 Scenario 7 – Ändringar i omgivande miljö för ett verifierat nivå 4-system

Följande figur illustrerar scenariot.

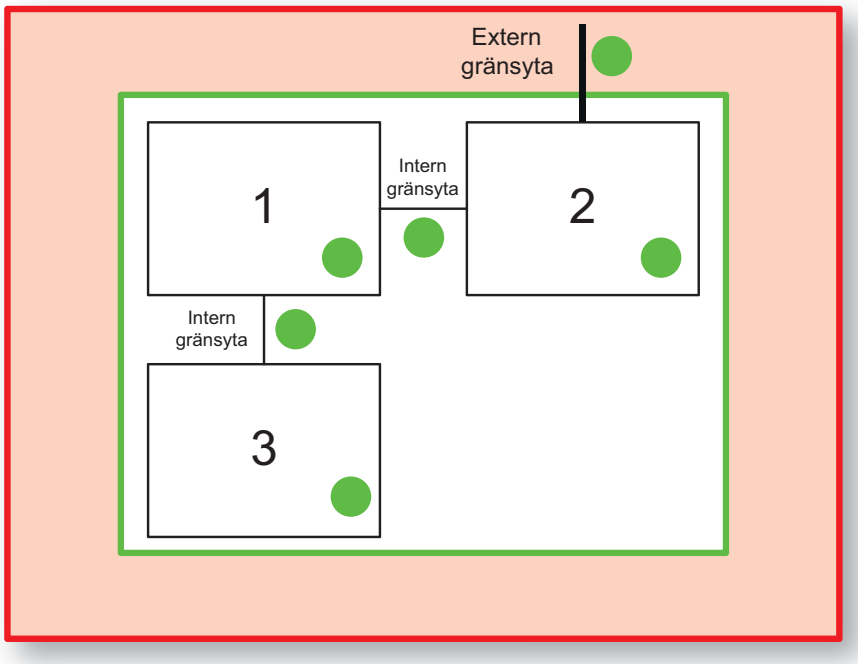

Bild 4:7 Scenario 7 - Ändringar i omgivande miljö för ett verifierat nivå 4-system

4.2.7.1 Förutsättningar

I detta scenario bör följande punkter kontrolleras:

- Tillkommer det några nya hot mot systemet då säkerhetsmiljön förändras?
- Reduceras befintlig hotbild då säkerhetsmiljön förändras?
  I detta fall kan det då finnas säkerhetsfunktioner som blir överflödiga.

Scenariot innebär förändringar i den omgivande säkerhetsrelaterade miljön, systemet i sig är redan verifierat. Ändringar i miljön har påverkan på hot-, risk- och sårbarhetsanalysen, vilket i sin tur påverkar Säkerhetsmålsättningen. Säkerhetsmålsättningen är grunden för systemets design, inklusive säkerhetsfunktioner, och ligger på så sätt till grund för verifieringen.

För att avgöra huruvida säkerhetsfunktionaliteten/säkerhetsarkitekturen påverkas eller inte vid förändringar i omgivande säkerhetsmiljö måste en bedömning göras genom att värdera förändringar i:

- Hot-, risk- och sårbarhetsanalys.
- Befintliga säkerhetsmål.

Om Säkerhetsmålsättningen skiljer sig avseende säkerhetsfunktionalitet måste systemet verifieras på nytt enligt *Scenario 1 – Bygga nivå 4-system av redan verifierade nivå 5-delsystem (produkter)*.

5 Återbruk av assuransarbete från nivå 5

5.1 Övergripande struktur

I detta kapitel beskrivs hur assuransarbete från nivå 5 kan återbrukas på nivå 4. Arbetet med att ta fram säkerhetsmålsättning, systembeskrivning och STAU är detsamma oberoende av nivå men effektiviseras av återbruk, delta-analyser och jämförelser av nivå 5-resultat med nivå 4-behov. Genom analyser avgörs vilken dokumentation från nivå 5-systemen som går att återanvända på nivå 4 och hur denna analys går till. Figuren nedan illustrerar de dokument som tas fram.

Huvudflödet, i enlighet med FM IT-livscykelmodel, går från krav-/målbild, via systemutformning, till verifiering och godkännande (auktorisation/ackreditering). Detta gäller såväl för nivå 4 som för nivå 5. Figuren nedan illustrerar flödet.

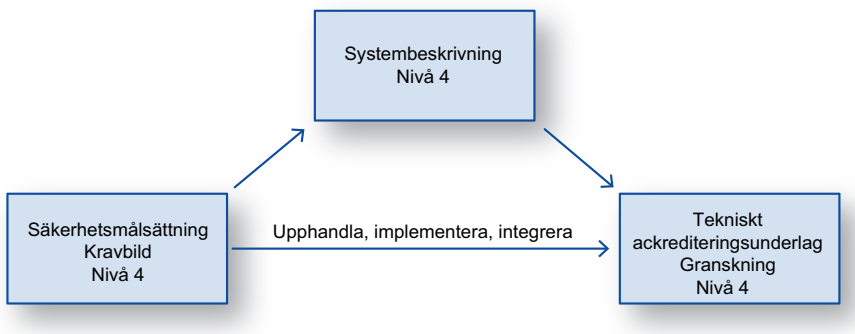

Bild 5:1 Nivå 4 flöde

I syfte att återanvända dokumentation och verifieringsresultat, ska underlag från respektive nivå 5-system granskas och beaktas. Med detta menas att de säkerhetsmålsättningar som finns på nivå 5 ska användas i samband med framtagning av nivå 4, liksom resultat från verifiering på nivå 5 kan underlätta verifieringen på nivå 4.

I samband med verifieringen på nivå 4 är det viktigt att kontexten (säkerhetsmiljön) för respektive nivå 5-system stämmer med den tänkta användningen på nivå 4. Detta för att bevara assuransen i nivå 5-granskningarna när motsvarande granskning görs på nivå 4. Figuren nedan illustrerar återanvändning av nivå 5-underlag.

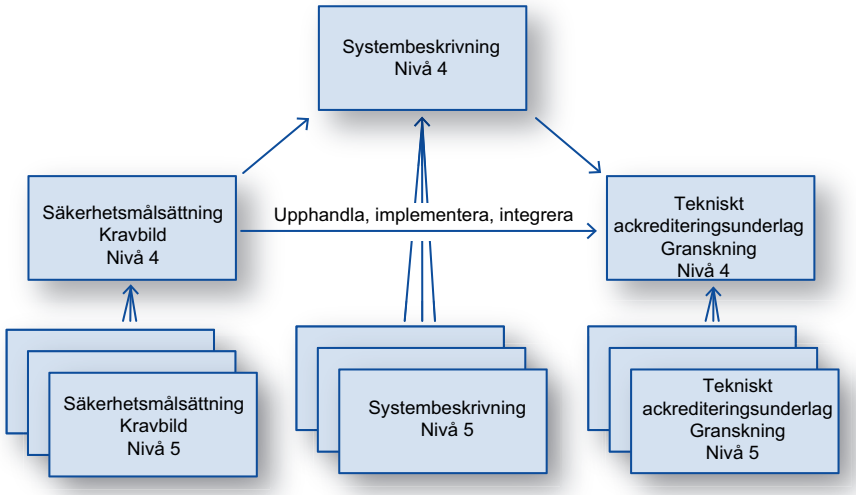

Bild 5:2 Återanvändning av underlag

Analysen förutsätter att denna dokumentation tagits fram på nivå 5. Stringens i underlagen underlättar analysen (fastställda mallar bör därför användas).

Då arbetet med att ta fram en säkerhetsmålsättning (nivå 4) delvis bygger på ingående delsystems säkerhetsmålsättningar (d v s nivå 5) ska även de underlag som ligger till grund för säkerhetsmålsättningen (säkerhetsanalys, hot-, risk- och sårbarhetsanalys, verksamhetsanalys samt författningsanalys) analyseras. Detta görs för att initialt granska lämpligheten i val an nivå 5-system, se *avsnitt 5.2* nedan. Vidare analyser görs för att undersöka att respektive delsystem (nivå 5) passar i det system av system som ska tas fram.

På samma sätt ska granskningsunderlag och tekniska ackrediteringsunderlag (TAU) för delsystem på nivå 5 analyseras, för att se om det är möjligt att behålla assuransen till dessa delsystem. Är detta möjligt, dvs delsystemen integreras i en kontext som stämmer med tidigare genomförd gransk-

ning, är det högst sannolikt att dessa delsystem inte behöver verifieras i någon djupare mening på nivå 4, utan de kan ses som ”tidigare godkända delar”.

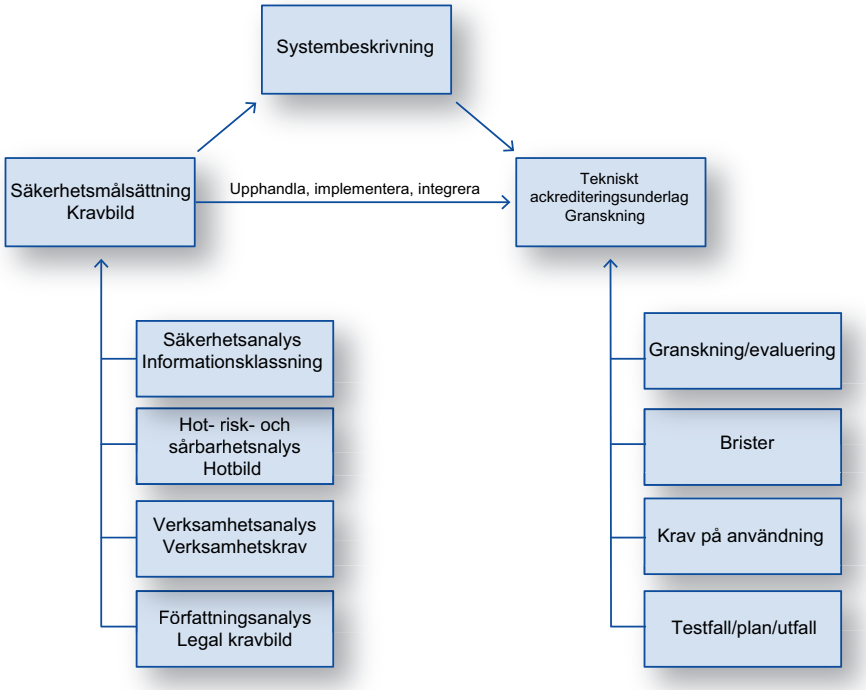

Bild 5:3 Ackrediteringsdokumentation

Säkerhetsmålsättning ska först tas fram på nivå 4, dvs mot det system av system som avses att tas fram. Grunden för detta arbete läggs redan i auktorisationsbeslut B1, enligt FM livscykelmodell. I detta beslutssteg identifieras behovet av nivå 4-systemet och sannolikt vilka system/komponenter på nivå 5 som kan tänkas behövas för att realisera (åtminstone på en övergripande nivå).

När detta arbete är gjort vidtar arbetet med att analysera huruvida det är möjligt att återanvända nivå 5-dokumentation och att assuransen vidhålls vid integration på nivå 4.

5.2 Initial analys (nivå 4)

En initial analys är viktig för att säkerställa att hela processen ”verifiering system av system” inte genomgås i onödan. Det går dock inte att säga entydigt hur den ska se ut men aspekter att beakta är:

- Säkerhetsmålsättningen
  - Ny information som tillkommer (dvs nya informationstyper).
  - Nya hot som tillkommer, på grund av ändrad säkerhetsmiljö
  - Ändrad verksamhet/användning.
- Ändrad arkitektur
  - Påverkan på säkerhetsfunktionaliteten.
  - Skillnaden mellan olika versioner av ingående delsystem.

5.3 Säkerhetsmålsättning (nivå 4)

Enligt beslutspunkt B2 i Försvarsmaktens IT-livscykelmodell, se *[4]*, ska en Säkerhetsmålsättning med ingående bilagor, enligt *bild 5:3* ovan, tas fram. I beslutspunkt B2 är krav och miljöbeskrivning centrala. Säkerhetsmålsättningen blir sedan ingångsvärde till den tekniska kravspecifikationen som används i System/Subsystem Specification (SSS) eller motsvarande kravspecifikation. Säkerhetsmålsättningen och dess bilagor utgör således grunden i verifieringsarbetet eftersom det är säkerhetsmålen som systemet ställs emot då det ska verifieras.

Analysen genomförs lämpligen i följande steg:

Steg 1: Ta fram Säkerhetsmålsättning på nivå 4 (om sådan inte redan finns).

Steg 2: Jämföra nivå 5-Säkerhetsmålsättningarna (och dess bilagor). Börja med bilagorna.

Steg 3: Identifiera eventuella nya nivå 4-säkerhetsmål utöver nivå 5-säkerhetsmålen.

Steg 4: Analysera eventuell diskrepans mellan säkerhetsmål.

Nedan beskrivs steg 2 för respektive bilaga.

5.3.1 Säkerhetsanalys (granskning av nivå 5-underlag)

Vid analys av ingående nivå 5-systems säkerhetsanalyser bör följande aspekter beaktas:

- Är det samma informationstyp i de olika systemen
  Om det är olika informationstyper måste en bedömning göras om huruvida det är acceptabelt eller inte samt vilka konsekvenser det medför.
- Blir det höjd informationsklassning pga aggregering av information?
  Aggregering av information kan leda till att ytterligare säkerhetsfunktioner behöver tillföras.
- Har nivå 5-systemen samma klassning?
  Lägst informationsklassning är dimensionerande, se alternativ nedan.

a. Det finns nivå 5-system med högre informationsklassning än övriga, som går att degradera till en lägre informationsklass.
b. Det går inte att degradera det nivå 5-system med högre informationsklassning än övriga nivå 5-system.

5.3.1.1 Alternativ A

Analysen kan fortsätta enligt nedan men det bör beaktas att högre klassat nivå 5-system har sannolikt onödiga krav/säkerhetsmål vilket påverkar kravbilden avseende (främst) MUST KSF.

5.3.1.2 Alternativ B

Utred möjligheten att dela in nivå 4-systemet i olika zoner med olika tillåten informationsklassning. Om zonindelning ej är möjlig måste nivå 5-systemet ersättas av ett annat nivå 5-system. Allt annat är otillåtet.

5.3.1.3 Output

Vid jämförelse av ingående nivå 5-systems säkerhetsanalyser erhålles en samlad bild för vad som är möjligt på nivå 4. Detta ger främst information om följande:

- Informationsklass, lämplig och/eller dimensionerande
- KSF-inriktning (beror på vald informationsklass).
- Nivå 4-systemets arkitektur, se *avsnitt 5.4* nedan.
- Hotbilden, se *avsnitt 5.3.2* nedan

5.3.2 Hot-, risk- och sårbarhetsanalys (granskning av nivå 5-underlag)

På nivå 4 är det summan av de hotrelaterade kraven för de ingående nivå 5-systemen som råder, men hotbilden kan förändras då nivå 5-systemen integreras. De tidigare identifierade hotbilderna för respektive nivå 5-system är sannolikt olika, vilket innebär att alla hot bör beaktas. Högsta hotbilden är dimensionerande, under förutsättning att säkerhetsmiljön för nivå 4-systemet överensstämmer med nivå 5-systemen.

I granskningen av nivå 5-systemens hot-, risk, och sårbarhetsanalyser är kontexten, dvs säkerhetsmiljön, en viktig aspekt att beakta.

En annan faktor är att vissa nivå 5-system kan ha säkerhetsmål som även möter hot mot övriga nivå 5-system.

5.3.2.1 Output

Säkerhetsmål relaterade till hotbild på nivå 4

5.3.3 Verksamhetsanalys (granskning av nivå 5-underlag)

På nivå 4 är det summan av verksamhetskraven för de ingående nivå 5-systemen som råder tillsammans med eventuella tillkommande verksamhetskrav på nivå 4.

Här är det viktigt att identifiera eventuella motstridiga krav. I sådana fall måste avgöras om det går att sätta samman nivå 5-systemen till nivå 4. Eventuellt kan det ställas olika krav på de olika delsystemen även efter att de sätts samman till ett nivå 4-system. Ett exempel på motstridiga krav är att ett nivå 5-system kravställer inloggning med TAK/PIN, medan ett annat kravställer inloggning med namn/lösenord.

5.3.3.1 Output

Säkerhetsmål relaterade till verksamhetskrav på nivå 4.

5.3.4 Författningsanalys (granskning av nivå 5-underlag)

På nivå 4 är det summan av författningskraven för ingående nivå 5-system som råder tillsammans med eventuella tillkommande författningskrav på nivå 4. Författningskrav beror på vilken information som behandlas i systemet, d v s vilka lagar och förordningar som är aktuella.

Om nivå 5-Säkerhetsmålsättningarna är från olika år kan förändringar i lagar, författningar, FFS:er och FIB:ar leda till att författningskraven ser olika ut för de olika nivå 5-systemen. Dessa krav ändras då inte för respektive nivå 5-system så länge nivå 5-systemet i sig förblir oförändrat.

5.3.4.1 Output

Säkerhetsmål.

5.3.5 Sammanställning av Säkerhetsmålsättning (på nivå 4)

När ovanstående jämförelser mellan nivå 5-systemens underliggande analyser är gjorda, är det möjligt att lyfta arbetet till nivå 4. I samband med detta bör det säkerställas att de sammanställda säkerhetsmålen från nivå 5 är förenliga med varandra. Det kan vara olika säkerhetsmål på olika delar.

Olika informationsklass enligt *avsnitt 5.3.1* ovan leder till att onödiga krav/säkerhetsmål ska rensas bort. Detta påverkar kravbilden avseende KSF.

Resultatet av detta arbete illustreras med följande summering:

$$\sum SM_{\text{nivå 4}} = \sum SM_{\text{nivå 5}} + \text{ev } SM_{\text{nivå 4}}$$

5.4 Systembeskrivning (nivå 4)

Enligt beslutspunkt B4 i Försvarsmaktens IT-livscykelmodell, se *[4]*, ska en systembeskrivning tas fram.

5.4.1 Input

Systembeskrivningar från nivå 5 blir direkt input till systembeskrivningen på nivå 4. Säkerhetsarkitekturen på nivå 4 bör också beakta t ex:

- Defence-in Depth
- förändrade säkerhetsfunktioner pga av att nivå 5-system sätts samman till nivå 4, enligt *avsnitt 5.3.5* ovan
- gemensamma funktioner (t ex tid, central säkerhetslogg, AD)
- flaskhalsar
- topologi
- zoner
- protokoll
- den totala systemuppbyggnaden
- interna gränsytor
- externa gränsytor.

5.4.2 Struktur

Systembeskrivningen på nivå 4 bör vara tillräckligt detaljerad för att en läsare dels ska kunna få en övergripande förståelse för systemet och dels en tillräckligt djup förståelse för säkerhetsfunktionernas implementation/realisering.

Djupare tekniska beskrivningar av ingående delsystem (nivå 5) kan med fördel utelämnas på nivå 4. Istället bör referenser till sådan dokumentation förtecknas.

Figuren nedan illustrerar strukturen på systembeskrivningen

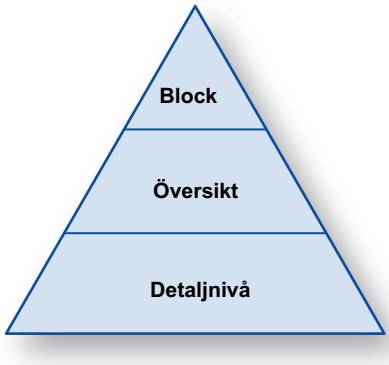

Bild 5:4 Struktur för systembeskrivningen på nivå 4

”Block” är de block som är illustrerade i scenariobeskrivningen i *avsnitt 4.2* ovan och ”Översikt” är mer ingående detaljer för nivå 4-systemet. ”Detaljnivå” är delsystemen på nivå 5.

Samtliga dessa nivåer måste finnas med i nivå 4-systembeskrivningen för att ge en fullständig förståelse.

5.4.3 Sammanställning av systembeskrivning (på nivå 4)

Resultatet av ovanstående arbete illustreras med följande summering:

$\sum$ Systembeskrivning$_{\text{nivå 4}}$ = $\sum$ Systembeskrivningar $_{\text{nivå 5}}$ + gemensamma funktioner $_{\text{nivå 4}}$ + säkerhetsarkitektur $_{\text{nivå 4}}$ + interna gränsytor $_{\text{nivå 4}}$ + externa gränsytor $_{\text{nivå 4}}$.

5.5 Tekniskt ackrediteringsunderlag (nivå 4)

Enligt beslutspunkt B5 i Försvarsmaktens IT-livscykelmodell, se *[4]*, ska ett tekniskt ackrediteringsunderlag tas fram.

Förutsättningar för detta är att:

- En nivå 4-säkerhetsmålsättning har tagits fram enligt *avsnitt 5.3*
- En nivå 4-systembeskrivning har tagits fram enligt *avsnitt 5.4*.

Nedan beskrivs ingående delar i det tekniska ackrediteringsunderlaget.

5.5.1 Granskning/evaluering (nivå 4)

Ingångsvärden till granskning på nivå 4 är tekniska säkerhetsmål (nivå 4) samt befintliga nivå 5-granskningar.

Efter arbetet med Säkerhetsmålsättningen enligt *avsnitt 5.3* gäller ett av följande alternativ:

a. Säkerhetsmålsättningarna från nivå 5 är kompatibla. Informationsklassningen för nivå 4-systemet är samma som för nivå 5-systemen eller lägre.
b. Säkerhetsmålsättningarna har stor diskrepans p g a att klassningen av systemet är högre än klassningen av delsystemet.

5.5.1.1 Alternativ A

För alternativ A gäller:

- Granskningar från nivå 5 går att återanvända.
- Eventuell diskrepans i identifierade brister pga av ändrad kravbild till följd av lägre informationsklassning för ett av nivå 5-systemen.
- Tillkommande säkerhetsmål/krav måste granskas.

CC-evaluerade produkter är svåra att återanvända. Undantag kan vara väldefinierade produkter. Generellt gäller att desto mer funktionalitet i en CC-evaluerad produkt desto svårare att återanvända. TOE (Target of Evaluation) är avgörande när det gäller att bedöma huruvida det går att återanvända CC-evalueringen eller inte.

5.5.1.2 Alternativ B

För alternativ B gäller:

- Om granskningarna från nivå 5 ska återanvändas måste en närmre analys göras så att krav och utlåtanden fortfarande är aktuella.
- En helt ny granskning utifrån nivå 4-Säkerhetsmålsättningen utförs.
- Granskningen är omfattande i jämförelse med alternativ A.
- Brister på delsystemen kan tillkomma p g a av att de inte kravställts för denna nivå från början.

5.5.1.3 Output

- Bristförteckning, se *avsnitt 5.5.2* nedan.
- Krav på användning, se *avsnitt 5.5.3* nedan.

5.5.2 Identifierade brister

Om alternativ a enligt ovan gäller så erhålles följande för brister på nivå 4:

$\sum$ Brister $_{\text{nivå 4}}$ = $\sum$ Brister $_{\text{nivå 5}}$ + ev $\sum$ Brister $_{\text{nivå 4}}$ – ev Brister $_{\text{nivå5}}$ som nedklassats.

Om alternativ b enligt ovan gäller så erhålles följande för brister på nivå 4:

$\sum$ Brister $_{\text{nivå 4}}$ = $\sum$ Brister $_{\text{nivå 5}}$ + nya brister $_{\text{nivå 5}}$ + $\sum$ Brister $_{\text{nivå 4}}$.

Identifierade brister måste hanteras, vilket kan ske enligt något av följande alternativ:

a. Krav på användning (dvs restriktioner) eller alternativa åtgärder. En åtgärd kan finnas kopplad till krav på användning, se *avsnitt 5.5.3* nedan.
b. Åtgärdsplan alternativt tidsbegränsat godkännande (Risk Management).

5.5.3 Krav på användning/alternativa åtgärder

Vid granskning av främst icketekniska säkerhetsmål framkommer ”krav på användning”. Denna typ av krav kan också uppkomma från ej uppfyllda tekniska säkerhetsmål (vilka då blir godkända genom krav på användning). På samma sätt kan krav på användning uppkomma från delvis uppfyllda tekniska säkerhetsmål.

Resultatet av ovanstående arbete illustreras med följande summering:

$\sum$ Krav på användning $_{\text{nivå 4}}$ = $\sum$ Krav på användning $_{\text{nivå 5}}$ + ev $\sum$ Krav på användning $_{\text{nivå 4}}$.

Hänsyn måste tas till motstridiga krav. Avstämning görs mot identifierade brister *avsnitt 5.5.2* ovan.

5.5.4 Testfall/-plan/-utfall

Ingångsvärden för tester på nivå 4 är tekniska säkerhetsmål på nivå 4 samt tester från nivå 5. De tester som utförts på nivå 5 används tillsammans med ytterligare tester som måste utföras på nivå 4.

För tester på nivå 5-system gäller generellt att nivå 5-system är testade för att de gör det de ska (d v s funktionella tester). Nivå 5-Säkerhetsmålsättningen tillsammans med övriga funktionskrav används som underlag för testningen.

Här är det viktigt att komma ihåg att leverantören (av nivå 5-system) inte har någon skyldighet att uppfylla krav som inte finns med i den kontraktuella konstruktionsspecifikationen.

För tester på nivå 4-system gäller generellt att nivå 4-system måste testas för att tillse funktion och säkerhet då de sätts samman, dvs verifiering och validering.

Testmiljöerna måste innehålla ett prototypsystem i fullständig version som är så snarlik det slutliga systemet som möjligt.

Testning sker mot nivå 4-Säkerhetsmålsättning. I detta fall är det inte säkert att det finns en specifik nivå 4 kravspecifikation att testa mot. Nivå 4-Säkerhetsmålsättning används då för framtagning av testspecifikation vilken motsvarar samtliga tekniska krav på denna nivå.

5.5.4.1 Olika typer av tester

- Funktionella tester
  - görs mot kravspecifikation
  - utförs av leverantören eller integratören
  - utfall från nivå 5-tester går att återanvända förutsatt att säkerhetsmålen fortfarande gäller.
- Validering
  - ”uppfyller system X verksamhetens krav?”
  - utförs av användare (eller dess representant)
  - måste göras för hela systemet på nivå 4
  - kan inte återanvända nivå 5-testning eftersom det inte är säkert att systemet gör vad det på nivå 4 för att det gör på ett visst sätt på nivå 5.

- Verifiering
  - ”gör system X det den ska?”
  - utförs av oberoende testare, integratör, användare och/eller leverantör
  - snarlikt funktionella tester
  - kan inte återanvända nivå 5-testning eftersom det inte är säkert att systemet gör vad det ska på nivå 4 för att det gör på ett visst sätt på nivå 5.
- Evaluering
  - uppfyllnad av säkerhetsmål
  - utförs av oberoende granskare
  - snarlik funktionella krav
  - se granskning ovan *avsnitt 5.5.1*
- Negativ testning
  - ”gör den något den inte ska göra?”
  - utförs av leverantör, användare eller oberoende granskare (beroende på assuranskrav)
  - måste göras för hela systemet på nivå 4 eftersom det inte är säkert att systemet inte gör något det inte ska på nivå 4 för att det inte gör det på nivå 5.
- Penetrationstester
  - intrångsförsök
  - utförs av oberoende granskare (beroende på assuranskrav)
  - måste göras på nivå 4 eftersom det tillkommer nya gränsytor, nya sätt att angripa systemet.