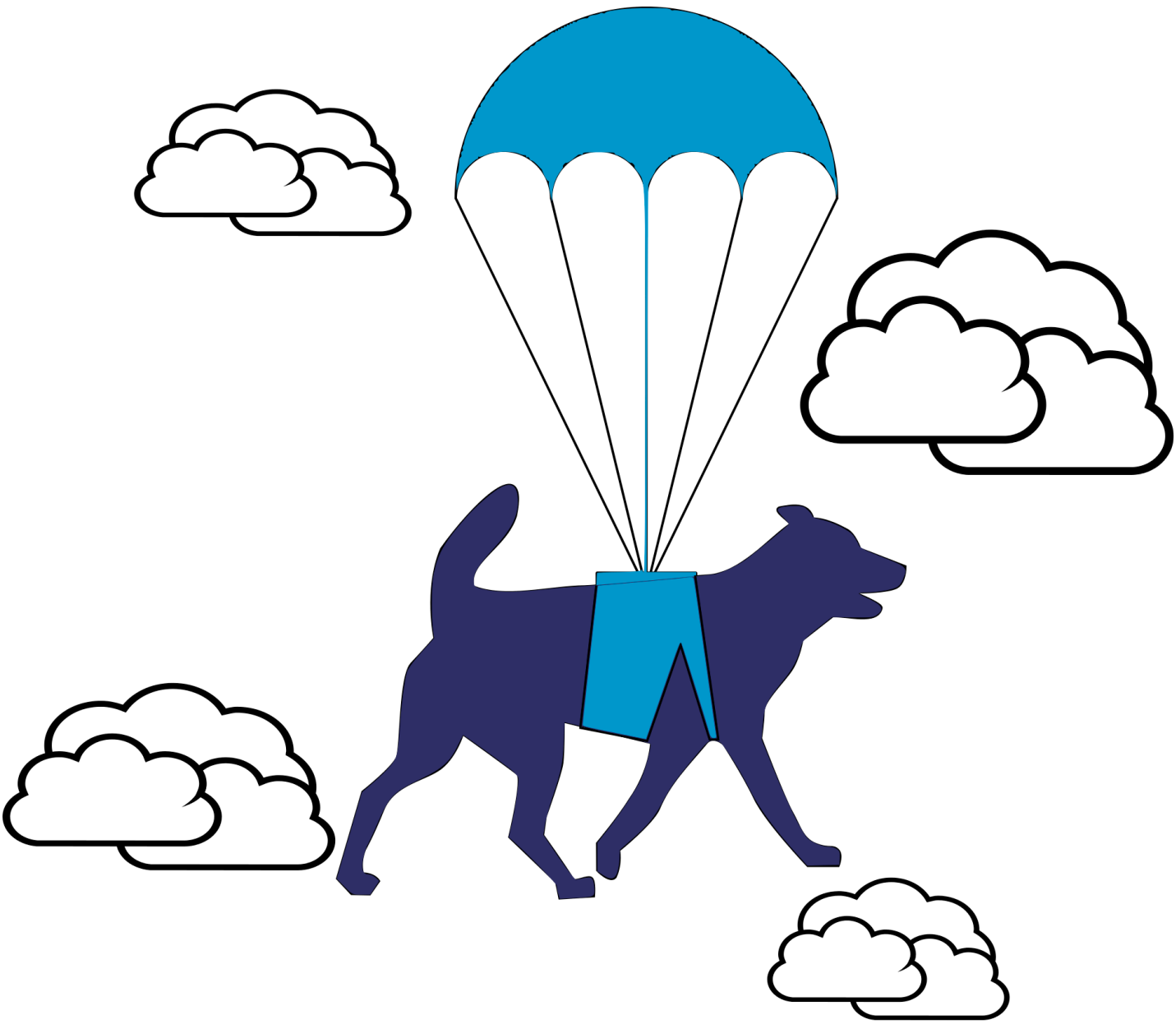
# Pålitliga IT-plattformar - Kopplingar mellan Försvarsmaktens behov och litteraturen

MARTIN KARRESAND



FOI-R--3903--SE
ISSN 1650-1942 Juni 2014

Martin Karresand

# Pålitliga IT-plattformar – Kopplingar mellan Försvarsmaktens behov och litteraturen

Bild/cover: Martin Karresand

| | |
|---|---|
| Titel | Pålitliga IT-plattformar – Kopplingar mellan Försvarsmaktens behov och litteraturen |
| Title | Trustworthy IT Platforms – Connections between needs of the Swedish Defence Forces and the literature |
| Rapportnummer | FOI-R--3903--SE |
| Månad | Juni |
| Utgivningsår | 2014 |
| Antal sidor | 50 |
| ISSN | ISSN-1650-1942 |
| Uppdragsgivare | Försvarsmakten |
| Projektnummer | E36057 |
| Godkänd av | Christian Jönsson |
| Ansvarig avdelning | Informations- och aerosystem |
| Forskningsområde | Informationssäkerhet och kommunikation |

FOI Totalförsvarets forskningsinstitut

## Sammanfattning

Den här rapporten redogör för de kopplingar (matchningar) som har identifierats mellan en litteraturstudie och en inventering av Försvarsmaktens behov rörande pålitliga IT-system, båda producerade av FOI. Kopplingarna har identifierats genom att klassificera behoven i sju kategorier i två steg. Först har behovens förklarande texter lästs igenom och alla relevanta kategorier har kopplats till respektive behov. I steg två har nyckelfraser från de förklarande texterna kategoriserats i en kategori per fras. Sedan har resultaten från de två stegen sammanställts.
I rapporten konstateras att det finns sju kopplingar (av 52 möjliga) mellan behov och litteratur, men att den tidigare litteraturstudiens omfattning är för snäv och att den därför skulle behöva breddas. För att studera förekomsten av vetenskapliga publikationer utanför litteraturstudiens avgränsningsområde har en begränsad litteraturstudie genomförts inom ramen för den här rapporten. Den nya litteraturstudien visar att det även för de första stegen i systemutvecklingsprocessen regelbundet publiceras vetenskapliga artiklar och att det därför kan antas att det är ett levande forskningsområde, vilket därför mycket väl kan inkluderas i basen för FM:s systemutvecklingskompetens. Om även artiklarna från det utökade forskningsområdet inkluderas i matchningsunderlaget stiger antalet kopplingar till 19.

## Nyckelord

pålitliga, IT-system, behovsanalys, litteraturstudie

## Abstract

This report presents the connections (matches) that have been identified between a literature review and an inventory of the needs of the Swedish Armed Forces regarding trustworthy IT systems, both produced at FOI. The connections have been identified by classification of the needs into seven categories in a two-step process. First the gist of the needs has been extracted and all relevant categories have been connected to each need. In the second step key phrases from the descriptions of the needs have been extracted and categorised into one category per phrase. Then the results from the two steps have been brought together.

The report concludes that there are seven connections (out of 52 possible) between the needs and the literature, but that the scope of the literature review is too narrow and needs to be expanded. To investigate the existence of scientific publications outside of the scope of the literature review a limited literature review has been done within this report. The new literature review shows a continuous publication frequency for the first steps of the system development process. If also the new publications are included in the basis of the work the number of connections increase to 19.

## Keywords

trustworthy, IT system, needs inventory, literature review

# Figurer



# Tabeller

# Innehåll

# 1 Inledning

Försvarsmakten har uttryckt en vilja och ett behov av att gå mot logisk separation istället för fysisk när det gäller att hålla isär olika säkerhetsnivåer i sina IT-system. Detta kräver att de enheter som upprätthåller separationen går att lita på. Som ett steg på vägen har FOI fått uppdraget att matcha den befintliga forskningen inom området pålitliga IT-plattformar mot de behov som Försvarsmakten har och därigenom identifiera var det kan finnas färdiga lösningar, respektive var forskningsinsatser krävs för att uppnå målet.

Den här rapporten presenterar en analys av innehållet i FOI-rapporterna ”Pålitliga IT-system i Försvarsmakten”[1] och ”Litteraturstudie av tekniker för pålitliga IT-plattformar” [2]. Analysen har gjorts för att se om det finns en matchning mellan behov och tillgängliga tekniker och att också, i förekommande fall, identifiera områden där det finns brist på tekniker som fyller behoven. För att kunna göra detta användes sju kategorier som täcker in området pålitliga IT-plattformar. De sju kategorierna består av fyra stycken som definierats i litteraturstudien, samt tre nya som definieras i den här rapporten. Behoven har sedan kopplats till kategorierna, för att på så sätt kunna visa var det finns matchningar, respektive brister på tillgängliga tekniker, vilket således pekar ut framtida forskningsbehov. I resten av rapporten kommer termen *koppling* användas för att beteckna en matchning mellan behov och teknik.

För att fylla ut en lucka i den ursprungliga litteraturstudiens omfattning har en begränsad litteraturstudie gjorts i samband med att den här rapporten skrevs. Resultatet av den presenteras i ett eget avsnitt. Den är inte tänkt att vara heltäckande på något sätt, endast visa på förekomst av forskning inom det område som den ursprungliga litteraturstudien inte täcker, nämligen de första stegen i systemutvecklingsprocessen.

## 1.1 Bakgrund

I projektplanen för FOI-projektet ”Pålitliga IT-plattformar” förklaras bakgrunden till projektet vara att ”Försvarsmakten har en vilja och ett behov av att gå mot logisk separation istället för fysisk när det gäller att hålla isär olika säkerhetsnivåer i sina IT-system. Detta kräver att de enheter som upprätthåller separationen går att lita på”. En del av projektet omfattar en studie av kopplingar mellan faktiska behov inom Försvarsmakten och forskningen kring lösningar på dessa inom området pålitliga IT-plattformar.

I projektet har det tidigare skrivits två rapporter, resultatet av en behovsinventering [1] och en litteraturstudie [2]. Litteraturstudien är koncentrerad till artiklar och publikationer om pålitlighet i ett systems livcykel, från programmeringssteget till laddning av den kompilerade binärkoden vid exekvering i hårdvara. Rapporten är tekniskt inriktad och täcker inte in steget mellan behovsanalys och systemdesign. Likaså medför den begränsade omfattningen att parametrar som *förmågan* att bland annat utföra de nödvändiga stegen från behovsanalys till installation, där systemets arkitektur *utformas*, samt hur *driften* av systemet hanteras saknas.

Behovsinventeringen har ett stort fokus på de delar av systemutvecklingsprocessen som inte avhandlas in i litteraturstudien. En förklaring till detta kan vara att de respondenter som ingick i studien kan ha haft andra arbetsuppgifter och därmed annat fokus.

Indelningen av texten i behovsinventeringsrapporten är gjord utifrån grupperingar av de behov som hittats, där författarna strukturerat behoven i grup-

per efter inbördes likhet iterativt tills alla behov tilldelats en grupp. Metoden kan i datavetenskapliga termer närmast beskrivas som en *Nearest-Neighbour*-klusteralgoritm. En dylik grupp av behov kallas i den här rapporten för *behovsgrupp*. Det finns inte någon garanti för att mängden av behovsgrupper är heltäckande och det har heller inte varit avsikten.

I den ursprungliga litteraturstudien används fyra kategorier för att klassificera de artiklar som studien omfattar. Kategorierna omfattar flödet från design till körande kod i en generell programutvecklingsmodell och består av följande steg [2, sid. 11] (listan har här kompletterats med de kategorinamn som används i den här rapporten):

**Programmera** Mellan specifikation och källkod (F1) måste det säkerställas att källkoden uppfyller specifikationen. [2, sid. 11]

**Kompilera** Mellan källkod och binärkod (F2) måste det säkerställas att binärkoden är en korrekt avbildning av källkoden. [2, sid. 11]

**Installera** Mellan binärkod och körklar kod (F3) måste det säkerställas att det som laddas in i IT-systemet är en oförvanskad version av binärkoden. [2, sid. 11]

**Ladda** Mellan körklar kod och körande kod (F4) måste det vid uppstart säkerställas att den körklara koden inte har påverkats sedan den installerades i IT-systemet. [2, sid. 11]

Definitionen av vad som i den här rapporten kallas *installera* är lite olyckligt formulerad i och med användningen av orden ”laddas in” som synonym för installeras i den ursprungliga litteraturstudien. Detta är korrigerat i senare versioner av resultatrapporteringen från projektet. Valet av termen installera ligger i linje med vad som beslutats inom projektet sedan tryckningen av litteraturstudien.

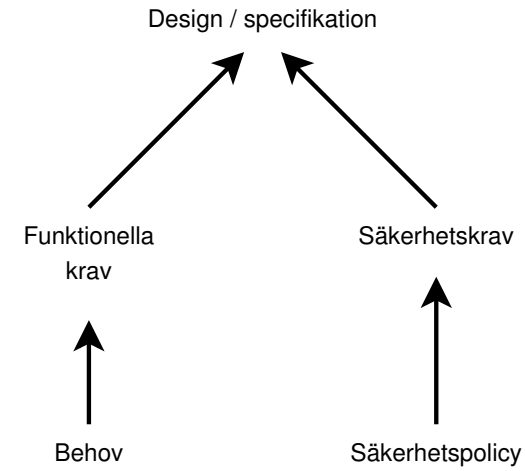
Anledningen till att litteraturstudien inte omfattar mer av ett IT-systems livscykel än dessa fyra faser är ett medvetet val från författarnas sida. Till grund för beslutet låg den ohanterliga mängd publikationer som blivit resultatet av en heltäckande studie. Genom att begränsa omfattningen på det sätt som gjorts har författarna lyckats hitta en balans mellan kvantitet och kvalitet och gjort det för kärnan av systemutvecklingsprocessen.

De tre nya kategorier som adderats till de fyra ursprungliga från litteraturstudien består av;

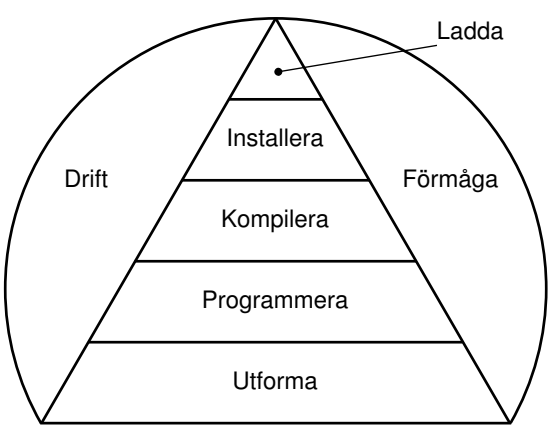
**Utforma** som omfattar kontroll av att de krav som ställs på systemets arkitektur och design också överförs korrekt till denna, så att systemets pålitlighet inte sänks. Kategorin är tänkt att täcka in de första stegen i systemutvecklingsprocessen (se Figur 1.1), vilka inte i egentlig mening täcks av kategorin *programmera*.

**Förmåga** som omfattar kontroll av att den kunskap som ligger till grund för kravställning, design med mera inom för systemet relevanta områden är tillräcklig för att upprätthålla systemets pålitlighet. I den här kategorin hamnar till exempel behov av expertstöd inom olika områden.

**Drift** som omfattar kontroll av att driften (patchning, uppdatering, administration, rutiner, strategier med mera) sker på ett sätt som inte sänker systemets pålitlighet. I den här kategorin hamnar till exempel behov av att regelverk följs, att det finns tillräckliga resurser under systemets livscykel och eventuella krav på utvecklingsmiljön. Likaså ingår behov av effektivare processer och snabbare flöden.




Figur 1.1: Den del av utvecklingsprocessen som saknar kategori i litteraturstudien och som i den här rapporten omfattas av den nya kategorin *utforma*.




Figur 1.2: Den tredelade kategorimodell som används i den här rapporten.

De nya kategorierna har använts för att bättre visa på de kopplingar som finns från behovsanalysen till den forskning inom pålitliga system som pågår, även om den litteraturstudie som gjorts inte omfattar de nya kategorierna.

I Figur 1.2 visas den tredelade kategorimodell som används i den här rapporten. De två kategorierna *drift* och *förmåga* griper över hela livscykeln för ett system. Den tredje delen av modellen, teknisk utveckling, omfattar den nya kategorin *utforma*, samt *programmera*, *kompilera*, *installera* och *ladda*, som härstammar från litteraturstudien.

Pyramidformen i Figur 1.2 är tänkt att visa hur antalet frihetsgrader vid systemutvecklingen minskar ju längre processen framskrider. Vid utformningen av systemets design finns ett stort antal möjliga lösningar, som minskar något när de ska omsättas i programform. Det finns sedan ytterligare några färre möjliga alternativ för hur den kompilerade koden kommer att se ut, eftersom en kompilator ofta optimerar och standardiserar koden. Därefter kan systemet installeras på en begränsad mängd hårdvara, som sedan kör något av några få operativsystem, som hanterar laddningen av den körbara koden.

De båda tidigare rapporterna i projektet täcker tillsammans in mer eller mindre hela systemutvecklingsområdet och de utmaningar som finns vid ut-

veckling av pålitliga system. De kan med fördel läsas tillsammans och ger i så fall en god förståelse för vilka behov som finns inom Försvarsmakten av tillgång till pålitliga system, samt vad forskarvärlden hittills har kommit fram till för att möta de krav på pålitlighet som finns under den senare delen av ett systems utvecklingsprocess.

## 1.2 Metod

Det här avsnittet beskriver de metoder som använts för att hitta kopplingarna mellan litteraturstudien och behovsinventeringsrapporten. Även principen för den begränsade litteraturstudien som gjorts inom ramen för den här rapporten redovisas.

### 1.2.1 Kopplingsanalys

I och med att de två tidigare rapporter som ligger till grund för den här rapporten är skrivna ur två olika perspektiv, har den här rapporten fått anta ett perspektiv däremellan. Tyngdpunkten har dock hamnat åt det filosofiska hållet på grund av att behovsinventeringen har analyserats vidare och därmed den här rapporten till viss del blivit en fortsättning på inventeringen.

Vidarebearbetningen av behovsinventeringen har utförts i form av kodning av innehållet. Detta har gjorts genom att behovsinventeringens resultatdel har lästs igenom upprepade gånger med målet att sammanfatta de identifierade behoven. Därefter har de tre sammanfattande kategorier[1] som utkristalliserat sig återförts på texten vid en ny genomläsning för att testa deras relevans. De avvikelser som då hittats har använts för att korrigera kategorierna och förloppet har sedan upprepats tills inga fler avvikelser hittats. De tre kategorierna redovisas i Avsnitt 1.

Den metod som använts för analysen av de behov som presenteras i behovsinventeringen [1] går ut på att först skapa en helhetsbild av behovsgruppen och sedan leta efter enskilda nyckelord och -fraser för att få med detaljerna för respektive behov. Dessa två steg kan närmare beskrivas som

1. en analys av de enskilda behoven på övergripande nivå för att få med textens kontext i analysen och på så sätt täcka in de utfyllande förklaringar som finns kring behovet. Varje behov kan ingå i flera kategorier.

2. En extrahering och analys av de viktigaste fraserna för respektive behov. Detta steg är tänkt att frambringa kärnan i varje behovsbeskrivning och filtrera bort eventuellt ovidkommande utfyllnad i beskrivningarna. Varje fras kan bara ingå i en kategori.

De två analysstegen redovisas först var för sig och sammanställs sedan på slutet av varje delavsnitt.

Anledningen till att den tvådelade metoden valdes var en önskan om att ge en så objektiv kategorisering som möjligt. De två stegen är tänkta att komplettera varandra och släcka ut varandras brister. Steg 1 ger en allomfattande analys av de presenterade behoven, men blir lätt för generell, det vill säga mer eller mindre alla kategorier kan kopplas till respektive behov, om inte direkt så i alla fall indirekt. Steg 2 är tänkt att motverka denna generaliseringsrisk i och med att bara en kategori får väljas för respektive nyckelfras. Nackdelen med detta är att i vissa fall är flera kategorier nödvändiga för en korrekt kategorisering, något som nu inte går. Kategoriseringen i detta steg riskerar därför att bli snedfördelad.

[1] *Utforma*, *drift* och *förmåga*.

I och med att resultatet för de två analysstegen redovisas separat kan läsaren själv bilda sig en uppfattning om hur respektive behovsgrupp ska kategoriseras och vilka kopplingar som (eventuellt) finns mellan behov och litteratur. Den efterföljande sammanställningen kan sedan användas som referens.

### 1.2.2 Begränsad litteraturstudie

Den begränsade litteraturstudie som har gjorts inom ramen för den här rapporten är uppbyggd kring en sammanställning av konferensbidrag från tre konferenser. De valdes ut genom en sökning i förlagen Elseviers och Springers publikationsdatabaser efter ordet ”trust”. De träffar som erhölls skummades igenom för att hitta eventuella gemensamma nämnare. Det visade sig att en stor del av dem härstammade från tre konferenser som sträckte sig minst fem år bakåt i tiden och vars proceedings publicerats i serien ”Lecture Notes in Computer Science” hos Springer Verlag. De tre konferenser som valdes var

- The International Conference on Autonomic and Trusted Computing (ATC)
- The International Conference on Trust and Trustworthy Computing (TRUST)
- The International Symposium on Trustworthy Global Computing (TGC)

Användningen av Springers goda publicistiska renommé och det faktum att konferenserna är väl etablerade får fungera som garanti för att artikelurvalet är representativt för forskningsfronten inom området pålitliga IT-system.

Ur de tre valda konferenserna plockades artiklar med titlar som pekade på arkitektur och design fram. Sedan lästes sammanfattningarna och i vissa fall valda delar av texten för att avgöra om de var möjliga att kategorisera som *utforma*. De som kvarstod inkluderades slutligen i den här rapporten i form av korta sammanfattningar av innehållet.

# 2 Kopplingsanalysresultat

I det här kapitlet redovisas resultatet av kopplingsanalysen. De två stegen i analysen redovisas separat och sammanfattas sedan i slutet av varje delavsnitt. Det första steget redovisas i form av en tabell med efterföljande kommentarer. Det andra steget redovisas i form av en graf med efterföljande kommentarer.

Strukturen på avsnittet är en kopia av den struktur som används i behovsinventeringsrapporten. Det gör att det i två avsnitt finns delavsnitt med behovredovisningar. Vid analysen har en linjär modell använts, det vill säga delavsnitten har lyfts upp en nivå och betraktats som egna fristående behovsgrupper. Avsikten är att underlätta läsningen och ge en högre detaljgrad.

Det finns bara sju tydliga kopplingar mellan rapporterna, vilket främst beror på att utfallen skiljer sig markant åt. Litteraturstudien utfördes innan behovsinventeringen och kunde därför inte baseras på utfallet från den senare. Författarna tvingades därför själva uppskatta behovsområdet. Följden blev att litteraturstudien fick ett strikt programvarutekniska perspektiv och behovsinventeringen istället fick ett perspektiv som blev vridet åt (system)-användarhållet. Likaså valde författarna av litteraturstudien att definiera termen ”system” som synonym för programvara, medan den i inventeringen till slut kom att användas som synonym för ett komplett system, innefattande användare, administratörer, regelverk, samt hård- och programvara.

## 2.1 Heltäckande IT-säkerhetslösning

Under den här rubriken har de behov som berör en helhetssyn på IT-säkerhetsfrågorna när nya IT-system utvecklas för Försvarsmakten samlats. I Tabell 2.1 redovisas resultatet av analyssteg 1.

Det finns tre behov som har klara kopplingar till litteraturen som presenteras i [2], enligt det första steget i analysen. Skälet till kopplingarna är att gruppen behandlar heltäckande lösningar och de kan därför också omfatta alla de sju kategorier som används i den här rapporten. Utöver de kopplingar som finns mellan behov och litteratur finns en i stort sett jämn fördelning mellan kategorierna *utforma*, *förmåga* och *drift*. Återigen kan behovsgruppens fokus på heltäckande lösningar användas som förklaring av analysstegets resultat.

I det andra analyssteget används nyckelfraser från behovsinventeringen, vilka i den här behovsgruppen ligger på en högre systemnivå än de andra grupperna. Gruppnamnet indikerar att behoven handlar om överblick och helhetssyn, vilket i behovsinventeringsrapporten bland annat beskrivs som ett

> behov av att ta hänsyn till samtliga delområden vid bedömning av vilken IT-säkerhetslösning som krävs. [1, sid. 14]

Det kan också handla om att

> säkerställa att alla relevanta tillkommande funktionella IT-säkerhetskrav kommer med i arbetet [1, sid. 14]

och att inte betrakta systemen som en uppsättning delar som kan behandlas separat, utan att

> istället hantera systemen i sin helhet. [1, sid. 14]

Arbetet ska också vara kontinuerligt, det slutar inte bara för att utvecklingsfasen är över, utan

Tabell 2.1: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen heltäckande IT-säkerhetslösningar.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Bedöm IT-säkerhet ur en samlad bild utifrån samtliga delområden | U | | | | | F | |
| Få med alla relevanta tillkommande funktionella IT-säkerhetskrav | U | | | | | F | D |
| Se till lösningen på en högre nivå | U | P | K | I | L | F | D |
| Ha god metodmässig hantering under systemets hela livscykel | | | | | | | D |
| Säkerställ en känd användningssituation | U | | | | | | |
| Ta hänsyn till den mänskliga faktorn | | | | | | | D |
| Genomför säkerhetsgranskning väl och vid önskad tidpunkt | U | P | K | I | L | F | D |
| Ha hög kvalitet i arbetet | U | P | K | I | L | F | D |

> [d]et finns behov av att under hela systemets livscykel metodmässigt hantera systemet på ett effektivt sätt som bidrar till tillit, [1, sid. 15]

en sak som också gäller beaktande av användargränssnitt och regler för hur systemet ska användas, för

> [o]m användarna inte kan utföra sina uppgifter tillfredsställande tenderar de att ta genvägar, vilket ger en okänd användningssituation och därmed minskad pålitlighet. [1, sid. 15]

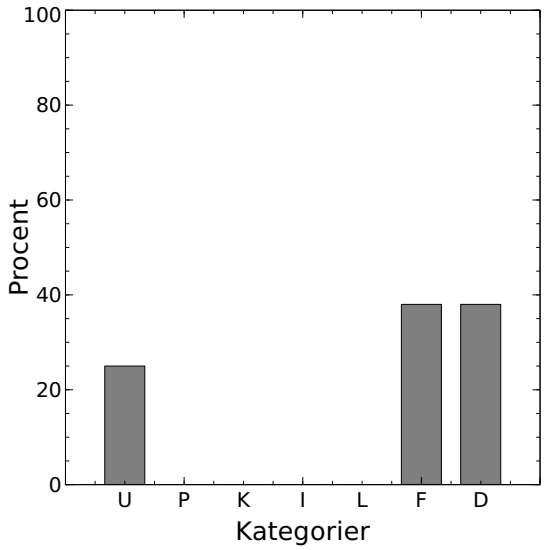
Enligt behovsinventeringen är det också viktigt att hantera säkerhetshoten från all personal som är inblandad i utvecklingen av systemen redan från allra första början och sedan också när systemet är på plats och ska administreras. Det uttrycks som ett

> behov av att ha säkra rutiner för att hantera systemadministratörer och deras höga behörigheter i IT-systemen. [1, sid. 15]

Ett sätt att lösa hanteringen av hot redan från början av systemutvecklingsprojekten föreslås i behovsinventeringen vara att genomföra

> säkerhetsgranskningar av oberoende part, som tar hänsyn till IT-systemets kontext och som säkerhetsställer att IT-systemets säkerhetsegenskaper motsvarar kraven. [1, sid. 15]

Alla de punkter som berörts kan sammanfattas med att för att uppnå pålitlighet i (Försvarsmaktens) IT-system måste säkerhetsarbetet genomsyra all relaterad




Figur 2.1: Den procentuella fördelningen mellan kategorierna för behovsgruppen Heltäckande IT-säkerhet efter det andra steget i analysen.

verksamhet, det vill säga vara heltäckande. I behovsinventeringen uttrycks det så här:

> För att nå pålitliga IT-system krävs det hög kvalitet i säkerhetsarbetet, vilket omfattar alla utförda uppgifter, alla resultat som producerats, i alla faser och från alla involverade aktörer. [1, sid. 16]

Den kategorimässiga tyngdpunkten för den här behovsgruppen ligger efter analyssteg 2 på *drift* och *förmåga*, men även till viss del *utforma*, vilket visas i Figur 2.1. Anledningen till fördelningen är att alla behov i gruppen har starkt fokus på mer allmängiltiga situationer. Framför allt handlar det om att upprätthålla tillräcklig kvalitet och att ta höjd för eventuella användarmisstag. Det gör att de mer programnära delarna *programmering*, *kompilering*, *installation* och *laddning* hamnar något i skymundan. Tre av behoven har dock kopplingar till alla de kategorier som används i den här rapporten.

Sammantaget innebär de två delresultaten av analysen att *drift*, *förmåga* och med något mindre tyngd även *utforma* blir huvudkategorier för behovsgruppen. Dock har fortfarande kategorierna *programmering*, *kompilering*, *installation* och *laddning* sådan tyngd att de inte kan bortses från.

## 2.2 Säkerhetskedjan

Den här behovsgruppen är en variation på Avsnitt 2.1, betoningen ligger dock lite mer åt det handfasta hållet, med behov av administrativa regler och verifiering av systemutvecklingsstegen.

Analyssteg 1 (se Tabell 2.2) visar att ett behov, ”Bevisa ett IT-systems funktioner och IT-säkerhet”, har en koppling till de vetenskapliga artiklar som presenterades i litteraturstudien [2]. Behovet har en nästan heltäckande kategorisering, det som saknas är en koppling till *förmåga*. Övriga behov i gruppen klassades enbart som tillhörande en kategori, *drift*. Snedfördelningen beror på att de övriga behoven inte hade ett lika direkt och tydligt uttalat krav på ett systems funktioner och IT-säkerhet som ”Bevisa ett IT-systems funktioner och IT-säkerhet”.

Tabell 2.2: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen säkerhetskedjan.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Arbeta enligt beskrivna regler | | | | | | | D |
| Kostnadseffektivt hantera stor mängd kod | | | | | | | D |
| Skapa en säker utvecklingsmiljö | | | | | | | D |
| Bevisa ett IT-systems funktioner och IT-säkerhet | U | P | K | I | L | | D |

Behovsgruppen benämns ”Säkerhetskedjan” i behovsinventeringen och fokus ligger på

> att ha administrativa regler för att undvika påverkan från antagonister under utveckling. [1, sid. 16]

Behovsinventeringen tar bland annat upp

> behov av att kostnadseffektivt kunna granska stor mängd kod, samt behov av att ha IT-system med god insynsmöjlighet [1, sid. 16]

som exempel på hur pålitligheten i systemet ska kunna säkras. De behövs även

> bra källkodshantering och change management [1, sid. 16]

enligt respondenterna. Ytterligare ett behov med bäring på utvecklingsfasen är

> att få effektivare granskningsförfarande och ökad pålitlighet hos lösningar, [1, sid. 17]

vilket också tas upp i inledningen till kapitlet i behovsinventeringen. Där står det att

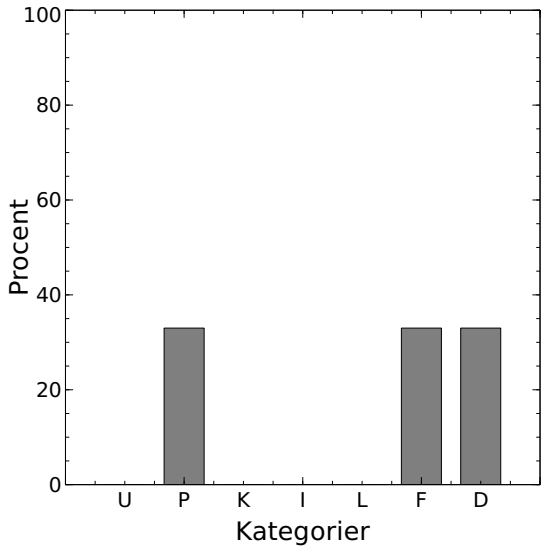
> [d]et finns behov av att undvika påverkan av antagonister under varje fas i säkerhetskedjan, det vill säga från det att programmeringen startar till att det körande programmet har laddats i datorn. [1, sid. 16]

Dock konstateras att behovet främst gäller existens av

> administrativa regler [1, sid. 16]

och verifiering av alla steg i systemutvecklingskedjan.

Behovet ”arbeta enligt beskrivna regler” har en tydlig koppling mellan behov och den forskning som presenteras i litteraturstudien. Det talas bland annat om skydd mot insiderhot under utvecklingsfasen och behov av bevis på att utvecklingen har skett i enlighet med de regler som det också finns behov av. Det gör att gruppen som sådan har kopplingar till alla kategorier i rapporten. Dock betonas särskilt behovet av administrativa regler, vilket gör att *driften* blir extra viktig, tillsammans med *förmåga* eftersom det talades om granskning




Figur 2.2: Den procentuella fördelningen mellan kategorierna för behovsgruppen Säkerhetskedjan efter det andra steget i analysen.

Tabell 2.3: Tabellen visar de kopplingar som som hittats mellan behov och litteratur för kravställning i utvecklingsarbetet.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Kravställning i utvecklingsarbetet | U | | | | | F | D |

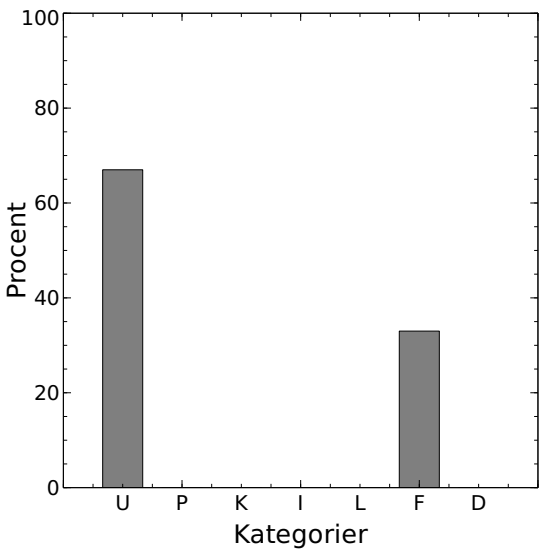
av bland annat kod. I och med att steg 2 i analysen innebar att endast en kategori fick användas per citat valdes *programmering* som representant för behovet av att ”undvika påverkan” och därför syns inte de andra däri ingående kategorierna i Figur 2.2.

Sammanställs analysstegen tonar det fram en kategorisering med tyngdpunkten på *drift*, men som också har en klar koppling till de kategorier som presenteras i litteraturstudien. I steg 2 finns ett inslag av *förmåga*, något som inte finns i steg 1. Skillnaden beror på att när behoven i gruppen detaljstuderades i steg 2 tolkades delar av innehållet annorlunda än i steg 1 i och med att steg 1 är kontextberoende, vilket steg 2 inte är.

## 2.3 Kravställning i utvecklingsarbetet

Kravställning i utvecklingsarbetet är en övergripande behovsgrupp, som saknar specifika behovsdefinitioner. Dessa redovisas istället i egna underavsnitt. Vid analysen har dock underavsnitten betraktats som egna behovsgrupper på samma nivå som den övergripande behovsgruppen, det vill säga ett linjärt angreppssätt har använts.

Den här behovsgruppen består bara av ett behov och ska därför kanske inte kallas grupp i egentlig mening. Kategoriseringen för det enda behovet blev i analyssteg 1 (se Tabell 2.3) en lika fördelning mellan *utforma*, *förmåga* och




Figur 2.3: Den procentuella fördelningen mellan kategorierna för behovsgruppen Kravställning i utvecklingsarbetet efter det andra steget i analysen.

*drift*. Tyngdpunkten ligger dock åt *utforma*-hållet, det syns bara inte i och med att dataunderlaget är för litet.

Analysen av behovsgruppen har gjorts utifrån det faktum att behovsinventeringen pekar på ett

> stort antal behov som relaterar till att säkerställa att de system som tas fram både har tillräckligt IT-säkerhet och är användbara. [1, sid. 17]

Inventeringen för också fram

> behov gällande att ta fram verksamhetsregler i samspel mellan verksamhetens behov och teknikens möjligheter. [1, sid. 17]

Även Försvarsmaktens

> behov av möjlighet att påverka informationshanteringen genom att få ställa kraven [1, sid. 17]

har använts vid kategoriseringen.

Resultatet av analyssteg 2 (se Figur 2.3) visar att *utforma* är den viktigare kategorin, men att det även finns ett visst behov av *förmåga*. Det senare främst beroende på behovet av att få ställa krav.

När analysstegen sammanställs syns en tydlig övervikt för *utforma* och det finns därför en implicit koppling till en del av litteraturstudiens artiklar, i och med att kategorin *programmera* där i praktiken även omfattar delar av systemutvecklingsstegen innan den faktiska programmeringen. Det finns dock även att inslag av *förmåga* och *drift*.

### 2.3.1 Stöd för att ta reda på vilka säkerhetsegenskaper som krävs för ett specifikt IT-system

Den här behovsgruppen fokuserar på kunskap och omfattar tre behov, som har störst inslag av *förmåga*, följt *utforma* och till sist *drift*. Anledningen till

Tabell 2.4: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen säkerhetsegenskaper för ett specifikt IT-system.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Designprinciper för IT-system | U | | | | | F | |
| Beskrivning av det önskvärda resultatet och hur man kommer dit | | | | | | F | D |
| Säkerställ att tänkt lösning uppfyller kraven | U | | | | | F | |

att tyngdpunkten ligger på *förmåga* är att, som namnet ”Stöd för att ta reda på vilka säkerhetsegenskaper som krävs för ett specifikt IT-system” antyder handlar det om kunskap och förmåga. Det behövs ”[s]töd för att ta reda på”, vilket tydligt visar på att behovet handlar om *förmåga*.

Analysresultatet för steg 2 grundar sig på att det i behovsinventeringen framkommer att det behövs

> stöd och riktlinjer för hur ett tillräckligt säkert IT-system bör byggas arkitektuellt [1, sid. 17]

och även för ett ”metodstöd för IT-säkerhet” [1, sid. 17] bestående av mer än bara checklistor. Metodstödet ska också vara

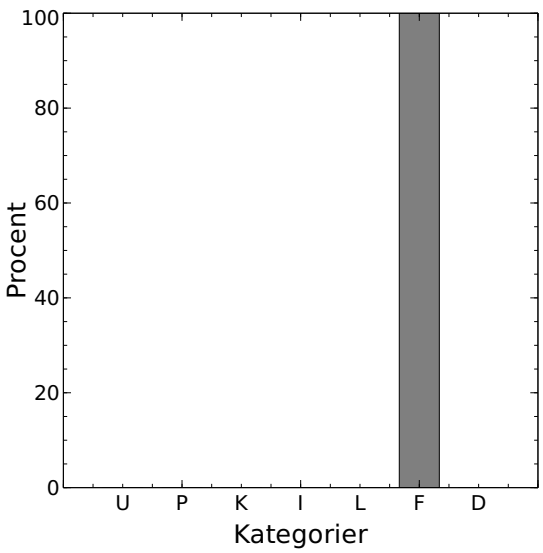
> ständigt aktuellt och uppdaterat utifrån kunskaper och erfarenheter[,] [1, sid. 18]

samt visa på nyttan av ordning och reda i alla led av systemutvecklingen. Stödet ska även beskriva hur detta ska uppnås. Metodstödet utgör ett regelverk som stöttar utvecklingsorganisationen, men det framförs också i behovsinventeringsrapporten att det även finns ett behov av mer praktisk hjälp i form av att

> säkerhetsexpertis kommer in redan från början i projekten, så att behov av IT-säkerhet och motsvarande krav identifieras från start[.] [1, sid. 18]

Ur dessa citat framträder ett övergripande behov av nödvändig och tillräcklig *förmåga* att genomföra systemutvecklingsprojekt med sådan kvalitet att resultatet blir pålitligt, vilket visas i Figur 2.4. Det talas också om behov av att få detta förmågestöd tidigt i processen och därför skulle också *utforma* kunna ingå. Denna kategori har trots det inte tagits med på grund av att behovet är av ”säkerhetsexpertis kommer in redan från början i projekten”, vilket har tolkats som extern expertis och Försvarsmakten således inte har något egentligt behov av egen kompetens inom området.

Sammanvägningen av resultaten för de två analysstegen visar att den här behovsgruppen inte har några kopplingar till litteraturstudiens kategorier, utan i praktiken endast innehåller behov av *förmåga*.




Figur 2.4: Den procentuella fördelningen mellan kategorierna för behovsgruppen Stöd för att ta reda på vilka säkerhetsegenskaper som krävs för ett specifikt IT-system efter det andra steget i analysen.

Tabell 2.5: Tabellen visar de kopplingar som som hittats mellan behov och litteratur för förmågan att utföra kravställning i utvecklingsarbetet.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Stöd för kravställning i utvecklingsarbetet | | | | | | F | |

### 2.3.2 Stöd för hur krav ska ställas för att få önskade säkerhetsegenskaper för ett specifikt IT-system

Den här behovgruppen är inriktad på *förmåga* att ställa krav. De krav som ställs ”behöver resultera i en vederhäftig säkerhetsmålsättning.” [1, sid. 18] Resultatet av analyssteg 1 kan ses i Tabell 2.5

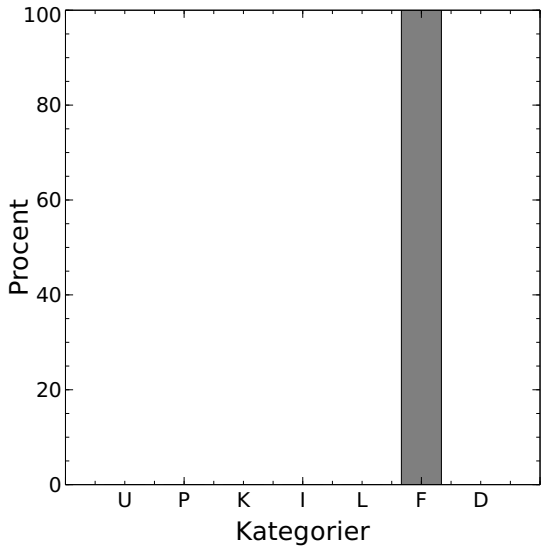
Gruppen innehåller endast ett uttryckt behov, vilket klassas som *förmåga*. Gruppen är mycket specifikt definierad och redan namnet på gruppen, ”Stöd för hur krav ska ställas för att få önskade säkerhetsegenskaper för ett specifikt IT-system”, indikerar att det handlar om *förmåga*.

Resultatet av analyssteg 2 är helt baserat på det behov av

> stöd för att veta hur och vilka krav som ska ställas för att få önskade IT-säkerhetsegenskaper, det vill säga eliminering av tolkningsutrymmet i regelverket för IT-säkerhetskrav[,] [1, sid. 18]

som beskrivs i behovsinventeringsrapporten. I och med att det är ett behov av stöd blir kategoriseringen *förmåga*, även om stödet handlar om utformning av system. Resultatet av analyssteg 2 visas i Figur 2.5.

Resultatet för den här behovsgruppen är entydigt *förmåga* för båda analysstegen och kopplingar till litteraturstudien saknas således.




Figur 2.5: Den procentuella fördelningen mellan kategorierna för behovsgruppen Stöd för hur krav ska ställas för att få önskade säkerhetsegenskaper för ett specifikt IT-system efter det andra steget i analysen.

Tabell 2.6: Tabellen visar de kopplingar som som hittats mellan behov och litteratur för behovet av stöd för kunskap om vilka lösningar som motsvarar uppställda krav på säkerhetsegenskaper.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Stöd för kunskap om lösningar i utvecklingsarbetet | U | | | | | F | |

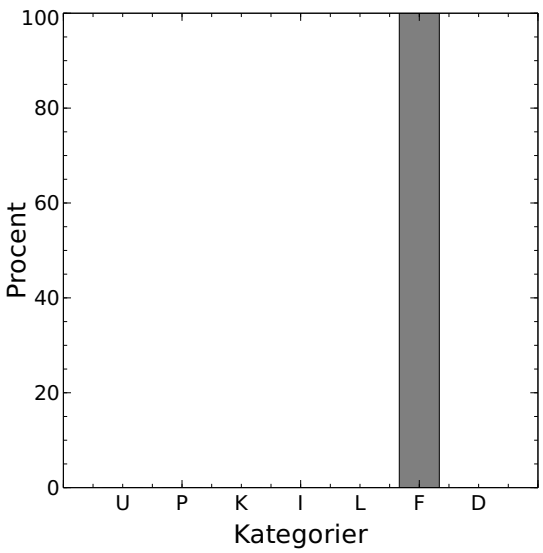
### 2.3.3 Stöd för att veta vilka lösningar som motsvarar uppställda krav på säkerhetsegenskaper

Behovsgruppen i fråga tar upp kunskap och *förmåga* och i det här fallet blev resultatet av analyssteg 1 en kategorisering som *utforma* och *förmåga*. Eftersom det bara finns ett behov i den här gruppen går det inte att peka på någon huvudkategori för steg 1. Däremot visar namnet på gruppen att det främst handlar om *förmåga* genom användningen av ordet ”veta”. Resultatet för analyssteg 1 redovisas i Tabell 2.6.

Analyssteg 2 för behovsgruppen använder det faktum att det finns ett behov av att

> vid framtagning av IT-system ha stöd för att veta vilka lösningar (i form av produkter, designval etc.) som motsvarar uppställda krav på IT-säkerhetsegenskaper och därmed ger en godkänd säkerhetslösning. [1, sid. 18]

Detta gör att behovsgruppen kategoriseras som *förmåga*, vilket kan ses i Figur 2.6. Även *utforma* skulle kunna fungera som kategorisering eftersom stödbehovet bland annat rör designval. Användningen av ordet ”stöd” pekar dock




Figur 2.6: Den procentuella fördelningen mellan kategorierna för behovsgruppen Stöd för att veta vilka lösningar som motsvarar uppställda krav på säkerhetsegenskaper efter det andra steget i analysen.

Tabell 2.7: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen användbarhet.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Ha en samlad bild av krav och behov innan lösningen tas fram | U | | | | | | D |
| Ha kunskap om systemets användning och syfte i verksamheten | | | | | | F | D |

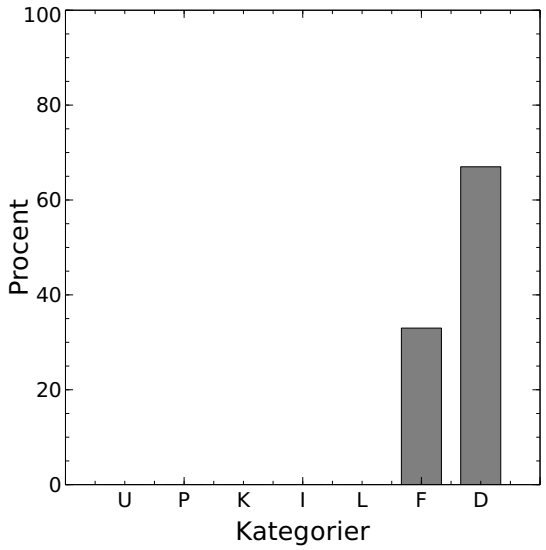
på ett förmågebehov.

Både analyssteg 1 och 2 pekar på *förmåga*, steg 1 har även *utforma* med som kategori. Det gör att behovsgruppen vid sammanställningen får en stark övervikt av *förmåga* och dessutom saknar kopplingar till den vetenskapliga litteratur som studerats i [2].

### 2.3.4 Användbarhet

Ingen kedja är starkare än dess svagaste länk, så även användarsidan måste tas i beaktande vid systemutvecklingen. Det gör att behovsgruppen ”Användbarhet” fokuserar på användarna och betydelsen för systemets pålitlighet av att de kan använda systemet. Därför ligger tyngdpunkten för resultatet av analyssteg 1 framförallt på *drift*, med ett inslag av *utforma* och *förmåga*. Resultatet kan beskådas i Tabell 2.7.

Det redogörs i behovsinventeringen för behov av att ”identifiera funktionella krav” [1, sid. 19], men även om ”drift- och förvaltningsrelaterade behov” [1,




Figur 2.7: Den procentuella fördelningen mellan kategorierna för behovsgruppen Användbarhet efter det andra steget i analysen.

sid. 19]. Även det faktum att det framförs behov av

> kunskap om hur systemet ska användas, och dess syfte i verksamheten [1, sid. 19]

bidrar till valet av *drift* som huvudkategori för behovsgruppen och referensen till ”kunskap” ses som en tydlig indikator på *förmåga*, vilket visas i Figur 2.7. Dock skulle behovet av kravidentifiering också kunna ge en kategorisering som *utforma*, men eftersom behovet begränsas till funktionella krav omfattas endast en del av systemdesignen och kategorins relevans minskar så pass att den kan bortses ifrån utan nämnvärd påverkan av resultatet.

I och med att det andra analyssteget kategoriserades som till två tredjedelar *drift* och en tredjedel *förmåga* har sammanställningen av behovsgruppen av förklarliga skäl en stor övervikt åt drifthållet. Inte heller den här gruppen uppvisar några kopplingar till litteraturstudiens kategorier.

## 2.4 Effektiva utvecklingsprojekt

Det första analyssteget för behovsgruppen ”Effektiva utvecklingsprojekt” har en tydlig koppling till litteraturstudiens kategorier. Dock är huvudkategorin för analyssteg 1 (se Tabell 2.8) för den här behovsgruppen *drift*. Behovet som ger upphov till kopplingen är ”Värdera pålitlighet vid upphandling” och det handlar egentligen om framför allt *förmåga*, men denna är tätt knuten till bland annat det kategorispann som behandlas i litteraturstudien.

I behovsgruppen ingår sju delar och de saker som i analyssteg 2 ledde fram till valet av de två huvudkategorierna *drift* och *förmåga*, vars inbördes fördelning kan beskådas i Figur 2.8, var att det framfördes behov av

> väl fungerande rutiner för att ständigt förbättra IT-säkerhetsarbetet [1, sid. 19]

tillsammans med ett behov av att ”ensa begreppsfloran inom IT-säkerhetsområdet i Försvarsmakten” [1, sid. 19] för att minska antalet missförstånd. Likaså föreslås att utvecklingsprocessen effektiviseras genom att det bara ska

Tabell 2.8: Tabellen visar de kopplingar som som hittats mellan behov och litteratur för effektiva utvecklingsprojekt.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Väl fungerande rutiner för förbättringshantering för IT-säkerhetsarbetet | | | | | | | D |
| Ensad begreppsflora inom Försvarsmakten gällande IT-säkerhet | | | | | | | D |
| Bara behöva granska en gång | | | | | | F | |
| En effektiv auktorisationsprocess | | | | | | | D |
| Granska direkt gentemot leverantörs produktbeskrivning | | | | | | | D |
| Ha långsiktiga strategier | | | | | | | D |
| Värdera pålitlighet vid upphandling | U | P | K | I | L | F | |

> behöva genomföra[s] granskning en gång [. . . ] på såväl enskilda komponenter och produkter som på hela plattformar. [1, sid. 19]

Det finns även behov av att ”förkorta auktorisationsprocessen genom att korta tiden för att ta beslut.” [1, sid. 20] Genom att föra över ansvaret för auktorisation av produkter på tillverkarna kan utvecklingstiden i vissa fall kortas ytterligare, enligt ett förslag i behovsinventeringen. Det som då krävs är en

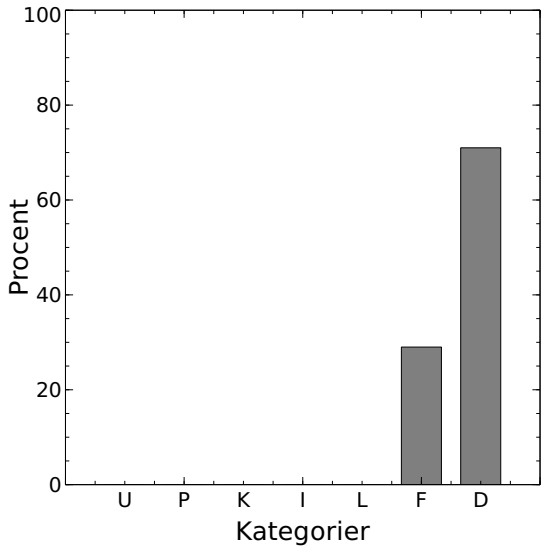
> beskrivning, riktad till tillverkare, av vad som krävs för att en programvara eller produkt ska bli godkänd, exempelvis att den måste ha en viss kontrollmekanism[,] [1, sid. 20]

vilket kan paras ihop med behovet att vid ”upphandling kunna värdera pålitlighetsfaktorer och få med dem i beslutsbilden[.]” [1, sid. 20] För att kunna genomföra detta på ett framgångsrikt sätt behövs, enligt vad som presenteras i behovsinventeringen,

> långsiktiga strategier både för IT och IT-säkerhet, med avseende på att kunna ta beslut om IT-system som bedöms vara pålitliga både i kortare och längre perspektiv. [1, sid. 20]

Analyssteg 2 för den här behovsgruppen har *drift* som huvudkategori, åtföljt av en liten del *förmåga*. Anledningen till denna kategorisering är att det uttrycktes behov av snabbare flöden, samt bättre strategier och rutiner.

Det är ett stort fokus på rutiner och regler i den här behovsgruppen, något som åtföljs av ett behov av att kunna värdera och formulera krav. Den sammanställda kategoriseringen, *drift*, av gruppen är därför enkel att göra. Det finns även en koppling till litteraturstudien via behovet av att kunna hantera upphandlingar på ett bättre sätt.




Figur 2.8: Den procentuella fördelningen mellan kategorierna för behovsgruppen Effektiva utvecklingsprojekt efter det andra steget i analysen.

Tabell 2.9: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen roller och ansvar i verksamheten.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Samarbeta mot en gemensam IT-säkerhetslösning | | | | | | | D |
| Ha kontinuitet i IT-säkerhetsarbetet | | | | | | F | D |
| Genomför uppgifter samvetsgrant | | | | | | F | D |

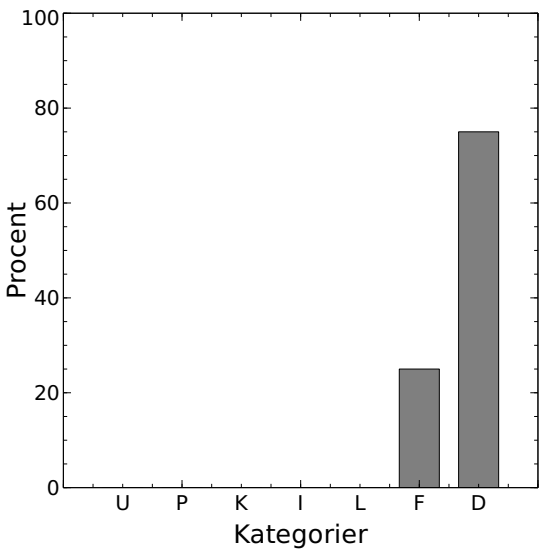
## 2.5 Roller och ansvar i verksamheten

För att möjliggöra utveckling av pålitliga system måste alla aspekter av utvecklingsprocessen beaktas. En viktig fråga är hur roller och ansvar fördelas i verksamheten. Detta framkom därför vid behovsinventeringen.

Resultatet av analyssteg 1 (se Tabell 2.9) har en viss övervikt av kategorin *drift*, men *förmåga* är nästan lika viktig. Eftersom behovsgruppen omfattar roller och ansvar är det naturligt att de kategorier som relaterar till användningen och driften av systemet ligger i fokus. Det gör också att eventuella behov från tidigare delar av systemets livscykel saknas. Det finns därför inte några kopplingar till litteraturstudien och dess kategorier i detta steg.

Grunden för analysens steg 2 kommer från redogörelsen i behovsinventeringsrapporten för det behov som finns av att

> förändra uppgifter och ansvar hos organisationsenheterna [...] för att tydliggöra ansvar och uppgifter, och undvika polarisering, internt och externt. [1, sid. 20]




Figur 2.9: Den procentuella fördelningen mellan kategorierna för behovsgruppen Roller och ansvar efter det andra steget i analysen.

Också behovet av ”kontinuitet i IT-säkerhetsarbetet i utvecklingsprocessen och förvaltningen” [1, sid. 21] tas upp i rapporten, som fortsätter med att konstatera att den tjänsterotation som förekommer inom Försvarsmakten ofta ger ett

> tapp i kunskap och erfarenhet, vilket ger ojämn nivå och ökar risken att uppgifter faller mellan stolarna. [1, sid. 21]

Det ställs också krav på att de olika uppgifter som är av vikt för utvecklingen av ett pålitligt system, såsom ”säkerhetsanalyser, ackrediteringar och andra uppgifter inom anskaffning[,] genomförs samvetsgrant” [1, sid. 21]. Det gör att analyssteg 2 får en liknande kategorisering som steg 1, med ett stort inslag av *drift* och en liten del *förmåga*, vilket visas i Figur 2.9.

Behoven inom den här gruppen handlar mycket om *driften* av utvecklingsprocessen och de färdiga systemen, vilken i sin tur är beroende av att *förmågan* att kunna genomföra den är tillräcklig. Gruppen kategoriseras därför också så vid sammanställningen. Denna kategorisering visar även på avsaknaden av en koppling till litteraturstudien.

## 2.6 Kompetens

Kompetens är tätt kopplat till *förmåga* och därför har också den här behovsgruppen en stor övervikt åt det hållet. Analyssteg 1 resulterar (se Tabell 2.10) i en kategorisering som *förmåga* med ett litet inslag av *drift*. Det lilla inslaget av *drift* beror på behovet av erfarenhet från tidigare verksamhet, något som kan ses som (dokumentation av) driften av systemet.

De behov av kompetens som framförs i behovsinventeringen är koncentrerade till utvecklings- och anskaffningsfasen av Försvarsmaktens system. Mer specifikt handlar det bland annat om ett

> behov av förståelse för hur IT-system fungerar i praktiken bland de personer som arbetar med säkerhetsmålsättningen. [1, sid. 21]

Tabell 2.10: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen kompetens.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Förståelse för hur IT-system fungerar i praktiken | | | | | | F | |
| Erforderlig kompetens hos de som granskar lösningar | | | | | | F | |
| Utnyttja erfarenheter och tidigare arbete och beslut | | | | | | F | D |

Nu är det inte bara bland dem det finns ett behov av *förmåga*[1]. Enligt behovsinventeringen finns det också ett

> behov av att de som granskar IT-säkerhetslösningar har erforderlig kompetens för att göra rätt bedömning och förstå de komplexa systemen. [1, sid. 21]

I Avsnitt 2.5 nämns att behovsinventeringen visat på behov av kontinuitet i roll- och ansvarsfördelningen för att minska risken för variationer i kompetensen hos organisationen. Detta behov återkommer i form av ett påpekande om att

> inom Försvarsmakten samla och utnyttja erfarenheter från tidigare anskaffningar, lösningar och beslut. [1, sid. 21]

Det är med andra ord inte svårt att se varför den här behovsgruppen vid analysen kategoriserades med en stor dominans av *förmåga* och en liten del *drift* (se Figur 2.10).

Resultatet av de två analysstegen liknar varandra, med en övervikt av *förmåga* och ett inslag av *drift*. Inte något av analysstegen visar på några kopplingar till litteraturstudiens kategorier.

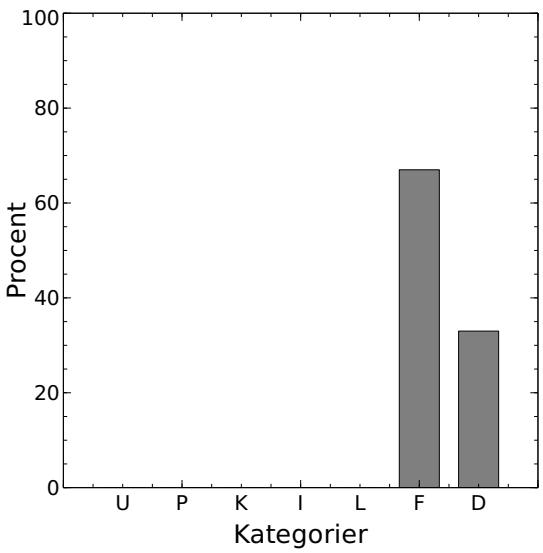
## 2.7 Kommersiella programvaror

Behovsgruppen för kommersiella programvaror omfattar de utmaningar som finns med att värdera pålitligheten hos programvaror och system där källkoden inte finns tillgänglig och därmed de första stegen i systemutvecklingskedjan ligger utanför Försvarsmaktens kontroll. Gruppen är svår att kategorisera, vilket avspeglar sig i det faktum att det ena av de två behoven kategoriseras som allt, utom *drift* och den andra som enbart *drift*. Resultatet av analyssteg 1 ses i Tabell 2.11.

Anledningen till att kategoriseringen i steg 1 skiljer sig så mycket åt mellan de två ingående behoven är att det ena tar upp frågan om effektiva evalueringsmetoder, något som kan ses som en del av den tekniska systemutvecklingen. Det andra behovet däremot behandlar modularisering av kommersiell programvara, vilket Försvarsmakten i realiteten bara kan påverka genom de rutiner som omgärdar systemet, det vill säga *drift*.

Analysresultatet för steg 2 baseras bland annat på det behov av ”kostnadseffektiva och bra evalueringsmetoder” [1, sid. 22] som framhålls i behovsinven-

[1] I behovsinventeringen används termen *kompetens* istället för *förmåga*.




Figur 2.10: Den procentuella fördelningen mellan kategorierna för behovsgruppen Kompetens efter det andra steget i analysen.

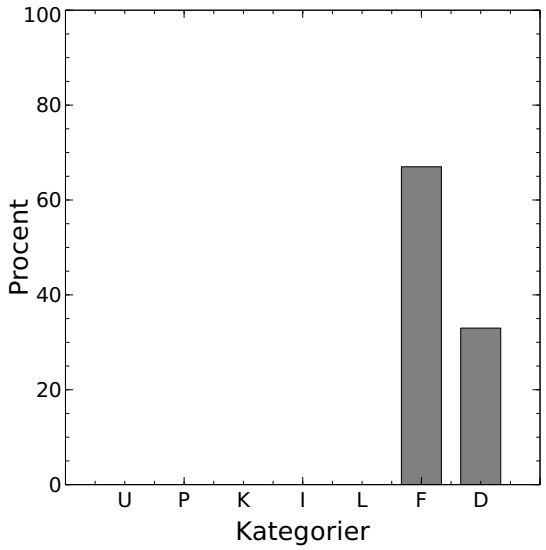
Tabell 2.11: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen kommersiella programvaror.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Kostnadseffektiv evalueringsmetod | U | P | K | I | L | F | |
| Modularisera kommersiella programvaror | | | | | | | D |

teringen. Även ett behov av extra uppmärksamhet vid ”utvärdering av kommersiella programvaror som marknadsförs som evaluerade” [1, sid. 22] tas upp. Det talas också om att det i vissa fall finns behov att ”få möjlighet att enbart anskaffa den del av programvaran som avses användas.” [1, sid. 22] I praktiken innebär det att Försvarsmakten vill få möjlighet att köpa system i modulär form, att kunna plocka russinen ur kakan, och på så sätt öka pålitligheten hos systemet i fråga.

Citaten från behovsinventeringen visar en övervikt av *förmåga* och *drift*, men också att övriga kategorier mycket väl kan vara relevanta på sekundär nivå. Analyssteg 2 fokuserar dock på att identifiera huvudkategorierna för behovsgruppen och bortser därför från eventuella sekundära kategoriseringar. Resultatet av analyssteget kan ses i Figur 2.11.

När resultaten från de två analysstegen sammanställs visar det sig att huvudkategorin blir *förmåga*, tätt följd av *drift*, men att där också finns en koppling till litteraturstudiens kategorier. Det går också att konstatera att kategoriseringen av den här behovsgruppen var svår att göra, något som de mycket spridda resultaten från de olika analysstegen visar.




Figur 2.11: Den procentuella fördelningen mellan kategorierna för behovsgruppen Kommersiella programvaror efter det andra steget i analysen.

Tabell 2.12: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen hantering av risker.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Anpassa IT-säkerhetskraven efter verksamhet och ekonomi | U | | | | | F | |
| Ha möjlighet att acceptera risker | | | | | | F | |

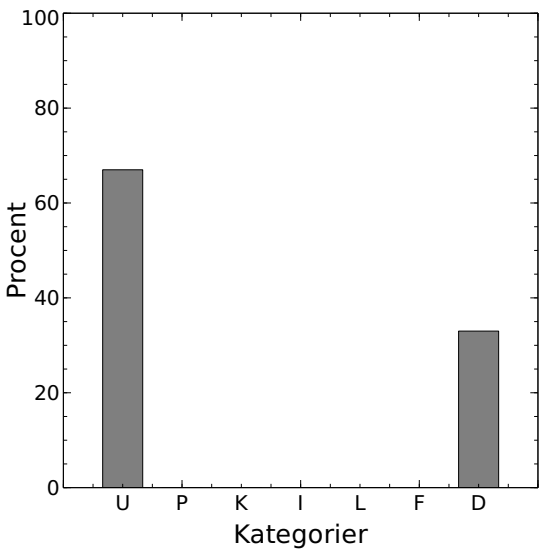
## 2.8 Hantering av risker

Den behovsgrupp som omfattar hantering av risker siktar in sig på att hitta balansen mellan IT-säkerhetskraven och systemets kontext. *Förmåga* är den mest framträdande kategorin för den här behovsgruppen visar resultatet efter analyssteg 1 (se Tabell 2.12). Det finns även en liten del *utforma*, som kommer från behovet av en verksamhetsanpassning av IT-säkerhetskraven för de system som utvecklas.

Det finns enligt behovsinventeringen behov av metoder för att hitta rätt nivå av IT-säkerhet i relation till kostnader och krav, det vill säga

> anpassa nivån för IT-säkerhetskraven så att de matchar de ekonomiska förutsättningarna och systemets kontext [1, sid. 22]

och ”kunna ta beslut gällande IT-säkerhetsegenskaper med hänsyn till användningssituation.” [1, sid. 22] Dessa behov kan tolkas som en önskan om att göra regelverken mindre strikta och mer dynamiska genom att kunna anpassas efter situation. Skulle det inträffa att en IT-säkerhetslösning inte skulle klara granskningen finns det behov av att




Figur 2.12: Den procentuella fördelningen mellan kategorierna för behovsgruppen Hantering av risker efter det andra steget i analysen.

> samtidigt få en konsekvensbedömning av användning i verksamheten, för att på så sätt få möjlighet att göra avvägda beslut om huruvida riskerna är accepterbara [1, sid. 23]

om systemet ändå skulle användas.

Resultatet av analyssteg 2 för den här behovsgruppen kan ses i Figur 2.12 och visar på en övervikt för *utformning*, vilket kommer sig av att behoven uttrycker önskemål om anpassningsmöjligheter för de IT-säkerhetskrav som ställs på systemet. Det finns också ett inslag av *drift* som kommer från behovet av konsekvensbedömning av eventuell användning av ett icke godkänt system.

Sammantaget ger de här behoven en övervikt åt kategorierna *utforma* och *förmåga*, eftersom det handlar om att ta beslut och anpassa systemets regler, processer och rutiner. Dock är den förklaringen inte begränsad till enbart dessa två kategorier, utan kan gott och väl omfatta även *utforma*, något som också visar sig i steg 2 av analysen. Några andra kategoriseringar har inte analysen gett, vilket innebär att den här behovsgruppen inte har några kopplingar till litteraturstudien.

## 2.9 Arkitektur

I det här avsnittet presenteras kategoriseringen av de olika behov relaterade till arkitektur som tas upp i behovsinventeringsrapporten. Vissa delavsnitt under rubriken ”Arkitektur” i behovsinventeringsrapporten innehåller endast text och redovisar inte explicit några behov. I de fallen har ändå en analys av texten gjorts. Precis som i avsnitt 2.3 har delavsnitten vid analysen betraktats som separata behovsgrupper på samma nivå som den övergripande behovsgruppen ”Arkitektur”.

### 2.9.1 Utformning av arkitekturen

Ledordet för behovsgruppen ”Utformning av arkitekturen” är tydlighet och då främst i samband med arkitekturspecifisering. Tydlighet ”ger mindre komplexitet, ökad möjlighet till överblickbarhet och förenklar IT-säkerhetslösningarna.” [1,

Tabell 2.13: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen utformning av arkitekturen.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Arkitekturell utformning | U | | | | | | |

sid. 23]

Den här behovsgruppens resultat efter analyssteg 1 (se Tabell 2.13) blir *utforma*, vilket är naturligt eftersom den omfattar utformning av ett systems arkitektur

I behovsinventeringsrapporten räknas ”verksamhetsarkitektur, applikationsarkitektur och teknisk arkitektur” [1, sid. 23] upp som de tre arkitekturer som avses. Där står också att det även finns

> behov av att ha bra dokumentation som kan fungera som en karta över lösningen för att effektivt minska de resurser som krävs för att få kunskap om och överblick över lösningen. [1, sid. 23]

Vid framtagning av dessa arkitekturer ska målet vara att ”lägga skyddet så nära informationen som möjligt, och ha IT-säkerhetsskydd i flera lager.” [1, sid. 23] Arkitekturerna behöver också vara så ensade som möjligt

> för att på så sätt öka effektiviteten och minska sårbarheten orsakad av de personberoenden som uppstår med många speciallösningar. [1, sid. 23]

Fokus ligger i de ovanstående citaten på *drift*, rubriken antyder dock en inriktning mot arkitektur och hur systemet ska *utformas*. Kategoriseringen av behovsgruppen efter steg 2 i analysen blir därför en viss övervikt för *drift*, med ett tydligt inslag av *utforma*. Detta kan ses i Figur 2.13.

Resultatet från steg 2 av analysen har ett större inslag av *drift* än *utforma* och skiljer sig därmed från resultatet av steg 1. Sammanvägningen av resultaten ger därför en lika fördelning mellan *utforma* och *drift*, dock utan några inslag av kategorierna från litteraturstudien.

### 2.9.2 Komponenter

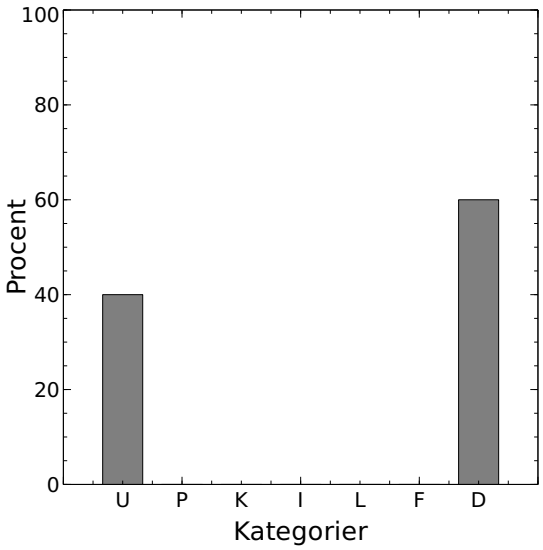
Den här behovsgruppen har endast ett behov, komponenttillgång, redovisat i behovsinventeringen. Kategoriseringen efter analyssteg 1 (se Tabell 2.14) blir därför *utforma*, eftersom komponenterna ska användas för att bygga (utforma) systemet.

Den här behovsgruppen omfattar förslag på att ha ett

> tillräckligt antal betrodda säkerhetskomponenter att välja mellan, tillgängliga vid det tillfälle de behövs och väl testade och fungerande redan från början. [1, sid. 24]

Komponenterna ska också vara kompatibla med varandra och ha bra gränssnitt mot omvärlden för att minska risken för felanvändning eller -funktion.

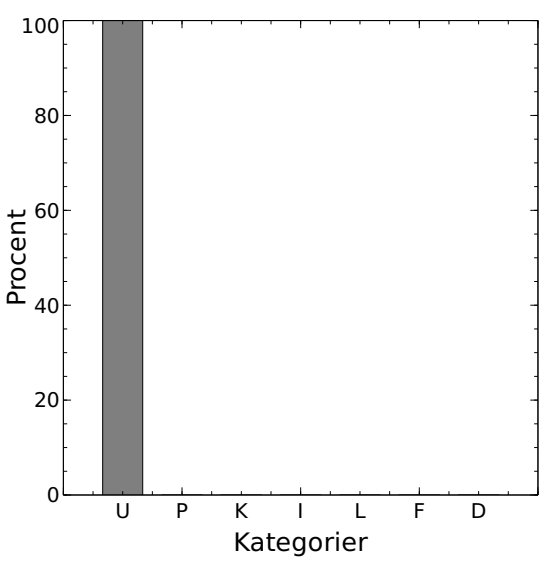
I och med att fokus ligger på (system)komponenter blir analysen i steg 2 enkel och resultatet *utforma*, vilket visas i Figur 2.14.




Figur 2.13: Den procentuella fördelningen mellan kategorierna för behovsgruppen Utformning av arkitekturen efter det andra steget i analysen.

Tabell 2.14: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen komponenter.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Tillgång till granskade och godkända komponenter | U | | | | | | |




Figur 2.14: Den procentuella fördelningen mellan kategorierna för behovsgruppen Komponenter efter det andra steget i analysen.

Tabell 2.15: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen komplexitet.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Hantera komplexitet | U | P | K | I | L | F | |

Sammanställningen av behovsgruppen är trivial i och med att det är en och samma kategori som blir resultatet av båda analysstegen. Det finns därför heller inte någon koppling till de kategorier som tas upp i litteraturstudien.

### 2.9.3 Komplexitet

Behovsgruppen som handlar om hantering av komplexitet återfinns under samma huvudrubrik som gruppen ”Komponenter”. De behov som identifierats leder vid analysen i steg 1 (se Tabell 2.15) till att det i första hand handlar om *förmåga*, men att behovet av tekniska lösningar också ger ett behov av *utforma*, *programmera* och *kompilera*, samt till viss del *installera* och *ladda*.

Beskrivningen av behovsgruppen i behovsinventeringen är mer än dubbelt så lång som genomsnittet av de övriga. Enligt behovsinventeringen är många av Försvarsmaktens system ”mycket komplexa” [1, sid. 24]. Det handlar då främst om

> en stor mängd verksamhetsregler, infrastruktur, informationsutbyte samt av att IT-säkerhetsbehovet är kontextberoende[,] [1, sid. 24]

där till exempel information kring en enskild soldats skobehov inte är hemligt, men antalet skor tillhörande ett kompani mycket väl kan vara det. En sänkning av komplexiteten hos systemen anges som ett delbehov.

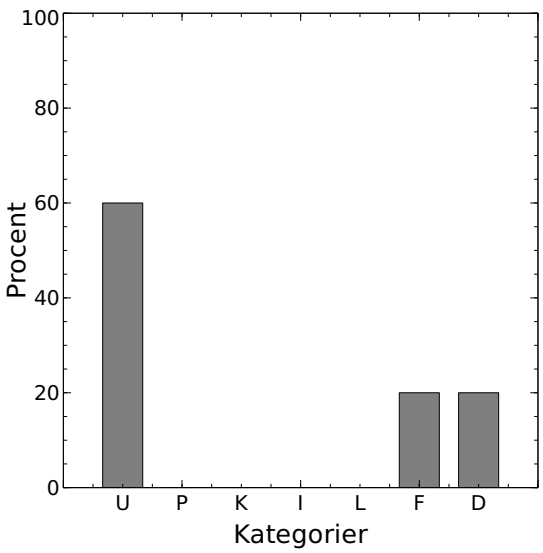
Det finns även en koppling tillbaka till behovsgruppen ”Komponenter” i form av ett

> behov av att minska komplexiteten genom att ha ett fåtal, generella, tekniska lösningar att välja mellan vid utformning av system. [1, sid. 24]

Detta behov beskrivs som sprunget ur de problem med för hög systemkomplexitet som finns, vilka gör det ”omöjligt att ta ett helhetsgrepp om lösningar vid deras utformning” [1, sid. 24]. Det finns därför ett behov av ”stöd för att på ett effektivt sätt arbeta sig fram stegvis till en bra och tillräckligt säker totallösning.” [1, sid. 24]

Huvudkategorin för ovanstående citat blir i analyssteg 2 (se Figur 2.15) *utforma*, men även *förmåga* och *drift* finns med till en viss del. Den främsta orsaken till kategoriseringens utseende är att fokus ligger på att minska komplexiteten i Försvarsmaktens system, vilket bäst görs så tidigt som möjligt i utvecklingsprocessen. Dessutom behöver både administrativa rutiner och kompetensen kring systemen ses över, därav förekomsten av *drift* och *förmåga*.

När resultaten för de båda analysstegen sammanställs är de i grund och botten lika, dock medför regeln om en och endast en kategori per fras i steg 2 att kategoriseringarna på pappret ser olika ut. I och med detta blir *utforma* den viktigaste kategorin, men i ett bredare perspektiv kan resultatet mycket väl snarare vara jämnt fördelat över *programmera*, *kompilera*, *installera*, *ladda*




Figur 2.15: Den procentuella fördelningen mellan kategorierna för behovsgruppen Komplexitet efter det andra steget i analysen.

Tabell 2.16: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen separation av information med olika sekretessgrad.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Separation av information med olika sekretessgrad | | | | | | | D |

och *utforma*. Därmed finns det också en tydlig koppling till litteraturstudien för den här behovsgruppen.

### 2.9.4 Separation

Behovsgruppen ”Separation” tar upp olika behov med bäring på den separation av information med olika sekretessklassning som ska göras enligt Försvarsmaktens regelverk. Gruppen saknar något explicit redovisat behov, men en analys har ändå gjorts och resultatet för analyssteg 1 redovisas i Tabell 2.16.

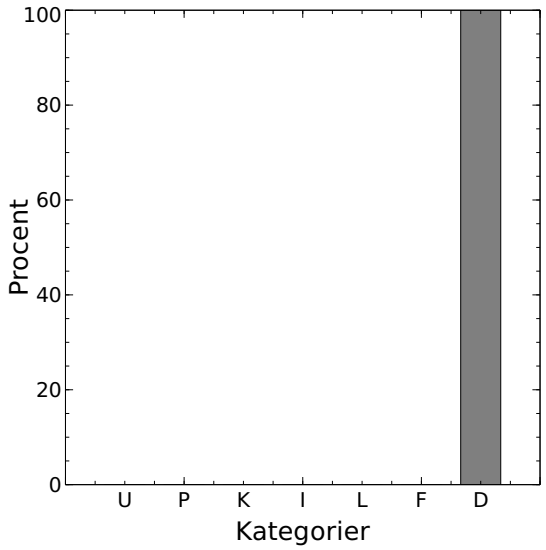
Gruppen innehåller endast ett behov och det kategoriseras som *drift* efter att analyssteg 1 har utförts. Den främsta anledningen till kategorivalet är att separation av sekretessgrader kräver ett korrekt administrativt regelverk i botten för att vara heltäckande.

Behoven i den här gruppen riktar sig mot att konstruera

> regler och tekniska system som effektivt stödjer användarnas arbete med information, när olika delar av information som bearbetas i samma arbetsmoment har olika sekretessnivå. [1, sid. 24]

Behovsinventeringsrapporten beskriver också ett behov av att

> i större utsträckning kunna lita på loggningsfunktioner, som skulle kunna larma om någon obehörig tar del av information i IT-




Figur 2.16: Den procentuella fördelningen mellan kategorierna för behovsgruppen Separation efter det andra steget i analysen.

Tabell 2.17: Tabellen visar kategoriseringen efter analyssteg 1 för behovsgruppen drift.

| Behov | Utfor. fas | Prog. fas | Komp. fas | Inst. fas | Ladd. fas | Förm. | Drift |
|---|---|---|---|---|---|---|---|
| Säkerställ funktionalitet och IT-säkerhet | | | | | | F | |
| Möjlighet att uppgradera system stegvis | | | | | | | D |
| Tydlig förvaltningsorganisation | U | | | | | | D |

systemet. [1, sid. 24]

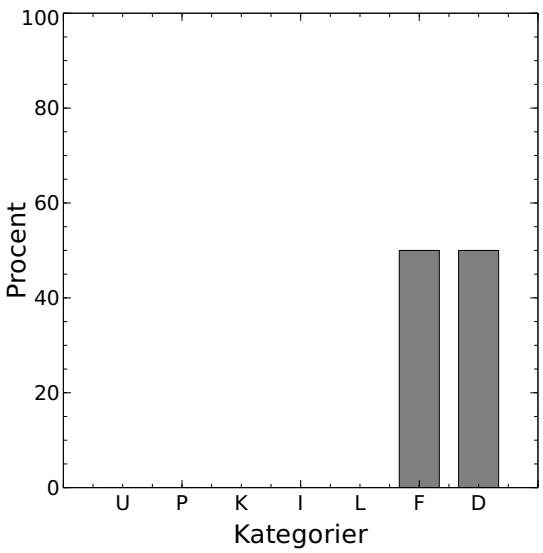
Resultatet av analysen i steg 2 blev en kategorisering av gruppen som *drift*. Både användarstödet och loggningsfunktionerna kan klassas som stödfunktioner utan direkt koppling till systemets (tekniska) bas. Kategoriseringsresultatet kan ses i Figur 2.16.

Sammantaget ger analysen av den här behovsgruppen en tydlig kategorisering som *drift*. Inga andra alternativa kategorier dök upp under analysen. Därför finns det heller inte några kopplingar till litteraturstudien i den här gruppen.

## 2.10 Drift

Den här behovsgruppen, kallad ”Drift”, skulle mycket väl även kunna kallas ”Tillgänglighet”. Det finns en tydligt vinkling i behovsbeskrivningarna mot tillgänglighet, till exempel talas det om att ”ha tillgång till redundanta IT-system för att kunna säkerställa tillgänglighet.” [1, sid. 25]

Resultatet för analyssteg 1 (se Tabell 2.17) visar att trots att namnet på behovsgruppen är ”Drift” och huvudkategorin också är densamma, så finns det




Figur 2.17: Den procentuella fördelningen mellan kategorierna för behovsgruppen Drift efter det andra steget i analysen.

fortfarande tydliga inslag av *utforma* och *förmåga*. Det är behovet av att kunna säkerställa IT-säkerhet som ställer krav på förmågan och behovet av en tydlig förvaltningsorganisation som kräver en korrekt utformning från början för att driften av systemet ska fungera.

Analysresultatet för steg 2 bygger på att det i behovsinventeringen framförs behov av att

> genom test och verifiering av systemen säkerställa att systemen gör sin uppgift som de ska. [1, sid. 25]

Det ska också vara modulärt uppbyggt eftersom det finns

> behov av att kunna uppgradera delkomponenter utan att behöva byta ut hela lösningen. [1, sid. 25]

Detta ska understödjas av organisationen runt systemen, som ”måste vara tydlig, med tydliga rollbeskrivningar, rolltilldelningar och ansvar.” [1, sid. 25] Organisationen ska kunna ”stödja i kravarbete och säkerställa att kravspecifikationen blir korrekt och tillgodoser behoven.” [1, sid. 25]

Sammantaget ger dessa uttalanden en kategorisering av resultatet en inriktning mot *drift* och *förmåga*, främst beroende på behovet av stöd i kravställningen av systemen. Titeln på behovsgruppen indikerar en ensidig användning av drift, men analyssteg 2 gav istället en jämnvikt mellan de två huvudkategorierna, vilket kan ses i Figur 2.17.

I och med att steg 2 av analysen är jämnt fördelad mellan *förmåga* och *drift*, samt att steg 1 har *drift* som huvudkategori, blir den sammanställda kategoriseringen av behovsgruppen *drift* med en stor andel *förmåga*. Trots att kategorin *utforma* finns med från analyssteg 1 saknas övriga kategorier i den tekniska delen av systemets utvecklingsprocess och det finns således inte några kopplingar till litteraturstudien från den här behovsgruppen.

Tabell 2.18: Tabellen visar de kopplingar som som hittats mellan behovsinventeringen och litteraturstudien. Varje behov redovisas tillsammans med det avsnittsnummer i den här rapporten som behovet tillhör. Kategorierna *utforma*, *programmera*, *kompilera*, *installera* och *ladda* är samlade under namnet *Tekn.* i tabellen.

| Behov | Kap. | Tekn. | Förm. | Drift |
|---|---|---|---|---|
| Se till lösningen på en högre nivå | 2.1 | T | F | D |
| Genomför säkerhetsgranskning väl och vid önskad tidpunkt | 2.1 | T | F | D |
| Ha hög kvalitet i arbetet | 2.1 | T | F | D |
| Bevisa ett IT-systems funktioner och IT-säkerhet | 2.2 | T | | D |
| Värdera pålitlighet vid upphandling | 2.4 | T | F | |
| Kostnadseffektiv evalueringsmetod | 2.7 | T | F | |
| Hantera komplexitet | 2.9.3 | T | F | |

## 2.11 Resultatsammanfattning

I det här avsnittet sammanfattas analysen av kopplingarna. För att underlätta förståelsen redovisas de sju behov som har kopplingar till forskningen som presenteras i litteraturstudien samlade i Tabell 2.18. För att öka läsbarheten har kategorierna *utforma*, *programmera*, *kompilera*, *installera* och *ladda* samlats under namnet *Tekn.* (Teknisk utveckling) i tabellen.

I varje enskilt fall omfattar kopplingar mellan de två FOI-rapporterna alla fyra kategorier från litteraturstudien. Det gör att kopplingarna är mycket tydliga. En anledning till den fullständiga täckningen av kategorierna är att de är svåra att separera i ett systems livscykel. Det går inte att hoppa över något steg i processen när ett systems pålitlighet ska säkerställas från ax till limpa.

De behov som inte har någon matchande kategori i den ursprungliga litteraturstudien faller alla istället inom de nya kategorierna som introducerades i den här rapporten. Delar av dem, 19 stycken, har kopplingar till *utforma* och täcks således av den nya, begränsade litteraturstudien. De 25 behov som enbart kategoriserats som *drift* eller *förmåga* kvarstår utan kopplingar. Det behöver dock inte innebära att det saknas vetenskaplig forskning som rör dem, bara att den forskningen inte kartlagts inom ramarna för det här projektet.

# 3 Litteraturstudie

Det här kapitlet innehåller en begränsad litteraturstudie riktad mot kategorin *utforma*. Begränsningen består i att endast några få tungviktiga konferenser inom området pålitliga IT-system användes som bas och att artiklarna inte har genomgått samma rigorösa urvals- och kategoriseringsprocess som i litteraturstudierapporten.

Proceedings från de tre konferenserna innehöll tillsammans 430 artiklar, varav 8 kvarstod när rensningen var avslutad. De utgör 1,9 % av de ursprungliga artiklarna och redovisas var för sig i egna underavsnitt.

## 3.1 Service Oriented Architectural Design

Bruni et al [3] beskriver Architectural Design Rewriting (ADR), vilket är ett språk för att formalisera utveckling och omkonfigurering av programvaruarkitekturer. Metoden ska ge garantier för att en programvara har konstruerats utifrån vissa kriterier och kunna hantera omkonfigurering med bibehållen korrekthet gentemot designen utan behov av extra formella bevis.

## 3.2 Verification of Model Transformations: A Case Study with BEPL

Baresi et al [4] har studerat om det går att göra verifierbara modelltransformeringar baserat på forskning redovisad i tidigare publikationer [5] av samma huvudförfattare. Författarna hänvisar även till en opublicerad teknisk rapport inom ämnet. Modellen, eller språket, är baserat på graftransformeringsteori rörande kritiska par och lokala sammanflöden (local confluence). Författarna visar att innehållet i de processer som används som exempel bevaras efter att de har genomgått en transformation.

## 3.3 Lockdown: Towards a Safe and Practical Architecture for Security Applications on Commodity Platforms

Vasudevan et al [6] har utformat en ny arkitektur för röd-gröna[1] system, där information med olika sekretessgrader ska separeras. Deras *Lockdown*-arkitektur använder sig av partitionering istället för virtualisering för att uppnå separationen. Enligt dem är fördelen att säkerheten ökar. Nackdelen är dock att bytet mellan miljöerna går långsamt; det tar mellan 13 och 31 sekunder vid deras tester.

## 3.4 Provably Correct Implementation of Services

Bruni et al [7] har konstruerat en tjänsteorienterad abstrakt maskin som är tänkt att överbrygga gapet mellan de existerande modeller för specifikation och analys av tjänstebaserade programvaror som finns och de faktiska programmeringsspråk som används. I maskinen kan modellerna testas utan att först behöva implementeras i något programmeringsspråk. Maskinen klarar av att hitta, koppla sig till och kommunicera med andra (nätverks)tjänster. På det här sättet säger sig författarna ha bevisat att för tre specifikationsmodeller, SL,

[1] Modellen verkar likna den röd-svarta systemmodellen. Den gröna sidan representerar väl skyddade och begränsade miljöer för säkerhetsklassade uppgifter. Den röda sidan representerar en snabb, generell och öppen miljö för allmänt bruk.

CaSPiS och Orc, är de föreslagna implementationerna operationellt korrekta.

## 3.5 A Generic and Modular System Architecture for Trustworthy, Autonomous Applications

Brancovici och Müller-Schloer [8] har skapat en allmängiltig systemarkitektur som hjälper till att systematisera designen av pålitliga tillämpningar. I arkitekturen ingår ett pålitlighetslager som garanterar funktionell stabilitet ur ett användarperspektiv. Hela arkitekturen är modulär och författarna uppmuntrar till modulär design, där uppdelningen sker utifrån komponenternas kognitiva funktion. Den i systemet inbyggda kunskapen är placerad i komponenterna, något som underlättar omkonfigurering av ett system som ska användas för andra ändamål.

## 3.6 A Framework for Specifying and Managing Security Requirements in Collaborative Systems

Yau och Chen [9] tar sig an problemet med dåliga säkerhetskravspecifikationer. De hävdar att de flesta kravspecifikationer inom säkerhetsområdet är tvetydiga, missledande, dåligt sammanhållna och skrivna på en alldeles för hög nivå, så att nödvändiga detaljer saknas. De har därför utvecklat ett ramverk för att ta fram bra kravspecifikationer. Ramverket innehåller en ontologi med hierarkiskt ordnade säkerhetskrav, specifikationsprocess, regler och en algoritm för att renodla säkerhetskrav, samt en algoritm för att hitta oförenliga krav. Artikeln är en av flera artiklar som beskriver ramverket och just den här tar upp specifikation och renodling av säkerhetskrav.

## 3.7 A Methodology towards Usable Trust Management

Yan och Niemi [10] påpekar att i deras ögon saknas användbarhetsperspektivet hos de metoder för design av tillitshantering som för närvarande finns. De har därför utvecklat en metod för användardriven tillitsmodellering och -hantering som är tänkt att leda fram till lösningar som användarna har lättare att acceptera och förstå. Författarna ser två fördelar med sin metod, dels att den utgår från användarnas perspektiv, dels att den för samman fördelar från både det psykosociala forskningsfältet och det datavetenskapliga. I artikeln applicerar de metoden på ett system för anseendebaserad gradering av applikationer, ”appar”, för smarta mobiltelefoner. De har för avsikt att fortsätta testningen genom att utvidga området till olika internettjänster för dylika telefoner.

## 3.8 Systematic Security Assessment at an Early Processor Design Stage

Huang et al [11] har studerat säkerhetsevalueringsprocessen för hårdvarudesign och föreslår en systematisk modell för gradering av en designs säkerhetslösningar tidigt i utvecklingsprocessen. Metoden är baserad på frågeformulär i två detaljnivåer och graderar säkerhetsnivån för en hårdvarudesign i fyra nivåer; ingen, låg, medel och hög. Målet är att mäta en designs säkerhet genom att bedöma dess exponering[2] och risk[3]. Författarna har utvärderat modellen på ett antal nuvarande och framtida processoregenskaper och kommit fram till att

[2]Exponering (eng. *exposure*) definieras av artikelförfattarna som sannolikheten för att en funktion innehåller en svaghet. [11, sid. 158]

[3]Risk definieras av artikelförfattarna som kostnaden som är förknippad med ett angrepp via en eventuell svaghet. [11, sid. 158]

resultatet ligger i linje med de utvärderingsresultat som några av säkerhetsexperterna inom industrin har kommit fram till.

## 3.9 Litteraturstudiesammanfattning

De åtta artiklar som utgör litteraturstudien i den här rapporten belyser forskningen kring design och utformning av säkra och pålitliga system ur olika vinklar. Flera av dem är direkt inriktade mot en systematisering av utvecklingsprocessens tidigare steg och presenterar metoder som leder till verifierbara processteg. Även användarperspektivet tas upp i en artikel, liksom både hård- och mjukvaruutveckling.

Under förutsättning att urvalet av artiklar kan anses vara representativt för forskningsområdet kan det konstateras att ungefär 2 % av de artiklar som skrivs tar upp de tidigare stegen i systemutvecklingsprocessen. Det gör att de kopplingar som finns mellan behoven i behovsinventeringen och den nya kategorin *utforma* i den här rapporten också bidrar med en teoretisk grund i form av artiklar att bygga vidare på.

# 4 Diskussion

I många fall ligger de behov som redovisas i behovsanalysen långt ifrån det som den ursprungliga litteraturstudien tar upp. I sju fall, som redovisas i Avsnitt 2 och Tabell 2.18, finns det kopplingar mellan behov och litteratur.

De sju behov som kan kopplas till den första litteraturstudien har alla full utdelning på kategorierna som används i den studien. Anledningen är att de hänger tätt ihop och eventuellt att upplösningen på dem är för hög. Precis som kategorimodellen i Figur 1.2 visar faller antalet möjliga alternativ att skapa innehåll i kategorin ju högre upp i modellen kategorin återfinns. I och med att det finns färre parametrar att påverka, antalet frihetsgrader minskar, finns det också färre möjliga kopplingar till kategorin. Det gör att sannolikheten för att det ska finnas kopplingar till kategorin *ladda* är mindre än för kategorin *programmera*. De behov som uttrycks i behovsinventeringen är dock i de allra flesta fall alldeles för grova och inexakta för att någon av kategorierna ska kunna uteslutas. I ett fall framgår kopplingarna klart och tydligt genom att

> [d]et finns behov av att undvika påverkan av antagonister under varje fas i säkerhetskedjan, det vill säga från det att programmeringen startar till att det körande programmet har laddats i datorn [1, sid. 16]

och därmed omfattas alla fyra kategorierna från litteraturstudien.

Bortsett från kopplingen där kategorierna nämns vid namn i behovsbeskrivningen är skälet eller skälen till kopplingen svagare, men det eller de finns fortfarande där. Det handlar då om mer generella behov av kontroll av IT-säkerhetshot under utvecklingsprocessen. De har inkluderats under parollen ”hellre fria än fälla”. Det finns dock fortfarande substans i den kategorisering som gjorts, det är bara det att det inte förekommer några explicita nyckelord eller -fraser i texten, utan kategoriseringen bygger på implicita kopplingar.

Ett fenomen som är värt att diskutera är det faktum att resultaten mellan de två analysstegen i några fall skilde sig radikalt åt. Förklaringen är att stegen visserligen utgår från samma data, men från olika infallsvinklar. Steg 1 fokuserar på helheten och har som mål att få en så bra täckning som möjligt för texten vad gäller kategorisering. Både beskrivningen för och namnet på behovet beaktas och alla relevanta kategorier används, dock utan inbördes rangordning. I steg 2 används istället nyckelfraser från respektive behovsbeskrivning och en och endast en kategori utses som representant för frasen, vilket gör att det blir fokus på detaljer i ett försök att undvika påverkan från rubriker och utfyllande text. I de fall där skillnaden mellan resultaten för analysstegen var markant kan nyckelfraserna tolkas på ett annat sätt när de står ensamma, jämfört med när de sätts i ett sammanhang. Detta har kommenterats i samband med analyssammanställningen i de fall det varit aktuellt.

Kategorin *utforma* har ett stort antal ($\frac{19}{52} = 37\%$) kopplingar till behov. En utökad litteraturstudie som även inkluderar *utforma* skulle innebära att antalet kopplingar mellan behovsinventeringen och den vetenskapliga teorin nästan tredubblades. Det skulle heller inte skada att även studera eventuell forskning som rör *drift* och *förmåga*, eftersom det skulle innebära att ett helhetsgrepp togs på utmaningarna kring pålitliga IT-system.

Det var med anledning av den stora andelen *utforma* i matchningsresultatet som den begränsade litteraturstudien i samband med den här rapporten gjordes. Resultatet därifrån visar att det finns flera forskargrupper som ägnar sig åt

de tidigare stegen under systemutvecklingsprocessen. Bredden är relativt stor, åtminstone att döma av det begränsade urval som nu gjordes, frågan är om det är representativt för forskningsområdet som helhet? Vissa av de utvalda artiklarna har stor relevans för Försvarsmaktens systemutvecklingsprocess, medan andra inte är direkt tillämpbara, utan bör bearbetas och studeras vidare.

# 5 Slutsats

De slutsatser som går att dra utifrån resultatet av de två analysstegen är

- att det finns kopplingar mellan de behov som Försvarsmakten har enligt behovsinventeringen och den litteraturstudie som gjorts,
- att avståndet mellan de beskrivna behoven och litteraturen ofta är långt,
- att litteraturstudien bör utökas till att också omfatta vetenskapliga publikationer med bäring på kategorin *utforma*,
- att en fördjupning i den för kopplingarna relevanta litteraturen bör göras,
- att en utredning bör göras för att studera hur de lärdomar som litteraturfördjupningen ger ska återföras till Försvarsmakten på bästa sätt,
- att även kategorierna *förmåga* och *drift* bör beaktas och litteratursökas för att få ett livscykelperspektiv på utvecklingen av pålitliga IT-system och
- att definiera om begreppet ”pålitliga IT-system” så att det blir tydligare och bättre täcker alla nödvändiga aspekter för att uppnå pålitlighet under hela livscykeln.

Det är att rekommendera att en mer omfattande litteraturstudie görs med inriktning mot de nya kategorierna *utforma*, *drift* och *förmåga* för att komplettera den ursprungliga litteraturstudien. Genom att inkludera även andra artiklar av samma författare, samt de artiklar som refereras i respektive artikel, kan omfattningen av den här rapportens litteraturstudie snabbt utökas. Underlaget för att hitta direkta kopplingar mellan enskilda behov och litteraturen skulle då bli större och sannolikheten för att hitta kopplingar skulle således öka.

# Litteraturförteckning

[1] Nina Lewau och Jacob Löfvenberg. Pålitliga IT-system i Försvarsmakten – en behovsinventering. Teknisk rapport FOI-R–3799–SE, Informations- och aerosystem, 2014. Väntar på tryckning.

[2] Jacob Löfvenberg och Ioana Rohde. Litteraturstudie av tekniker för pålitliga IT-plattformar. Teknisk rapport FOI-R–3724–SE, Informations- och aerosystem, 2013.

[3] Roberto Bruni, Alberto Lluch Lafuente, Ugo Montanari och Emilio Tuosto. Service oriented architectural design. I: Gilles Barthe och Cédric Fournet, redaktörer, *Trustworthy Global Computing*, band 4912 av *Lecture Notes in Computer Science*, ss 186–203. Springer Berlin Heidelberg, 2008.

[4] Luciano Baresi, Karsten Ehrig och Reiko Heckel. Verification of model transformations: A case study with bpel. I: Ugo Montanari, Donald Sannella och Roberto Bruni, redaktörer, *Trustworthy Global Computing*, band 4661 av *Lecture Notes in Computer Science*, ss 183–199. Springer Berlin Heidelberg, 2007.

[5] Luciano Baresi, Andrea Maurino och Stefano Modafferi. Workflow partitioning in mobile information systems. I: Elaine Lawrence, Barbara Pernici och John Krogstie, redaktörer, *Mobile Information Systems*, band 158 av *IFIP International Federation for Information Processing*, ss 93–106. Springer US, 2005.

[6] Amit Vasudevan, Bryan Parno, Ning Qu, Virgil D. Gligor och Adrian Perrig. Lockdown: Towards a safe and practical architecture for security applications on commodity platforms. I: Stefan Katzenbeisser, Edgar Weippl, L. Jean Camp, Melanie Volkamer, Mike Reiter och Xinwen Zhang, redaktörer, *Trust and Trustworthy Computing*, band 7344 av *Lecture Notes in Computer Science*, ss 34–54. Springer Berlin Heidelberg, 2012.

[7] Roberto Bruni, Rocco Nicola, Michele Loreti och Leonardo Gaetano Mezzina. Provably correct implementations of services. I: Christos Kaklamanis och Flemming Nielson, redaktörer, *Trustworthy Global Computing*, band 5474 av *Lecture Notes in Computer Science*, ss 69–86. Springer Berlin Heidelberg, 2009.

[8] George Brancovici och Christian Müller-Schloer. A generic and modular system architecture for trustworthy, autonomous applications. I: Bin Xiao, Laurence T. Yang, Jianhua Ma, Christian Müller-Schloer och Yu Hua, redaktörer, *Autonomic and Trusted Computing*, band 4610 av *Lecture Notes in Computer Science*, ss 169–178. Springer Berlin Heidelberg, 2007.

[9] Stephen S. Yau och Zhaoji Chen. A framework for specifying and managing security requirements in collaborative systems. I: Laurence T. Yang, Hai Jin, Jianhua Ma och Theo Ungerer, redaktörer, *Autonomic and Trusted Computing*, band 4158 av *Lecture Notes in Computer Science*, ss 500–510. Springer Berlin Heidelberg, 2006.

[10] Zheng Yan och Valtteri Niemi. A methodology towards usable trust management. I: Juan González Nieto, Wolfgang Reif, Guojun Wang och

Jadwiga Indulska, redaktörer, *Autonomic and Trusted Computing*, band 5586 av *Lecture Notes in Computer Science*, ss 179–193. Springer Berlin Heidelberg, 2009.

[11] Ruirui Huang, David Grawrock, David C. Doughty och G. Edward Suh. Systematic security assessment at an early processor design stage. I: Jonathan M. McCune, Boris Balacheff, Adrian Perrig, Ahmad-Reza Sadeghi, Angela Sasse och Yolanta Beres, redaktörer, *Trust and Trustworthy Computing*, band 6740 av *Lecture Notes in Computer Science*, ss 154–171. Springer Berlin Heidelberg, 2011.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se