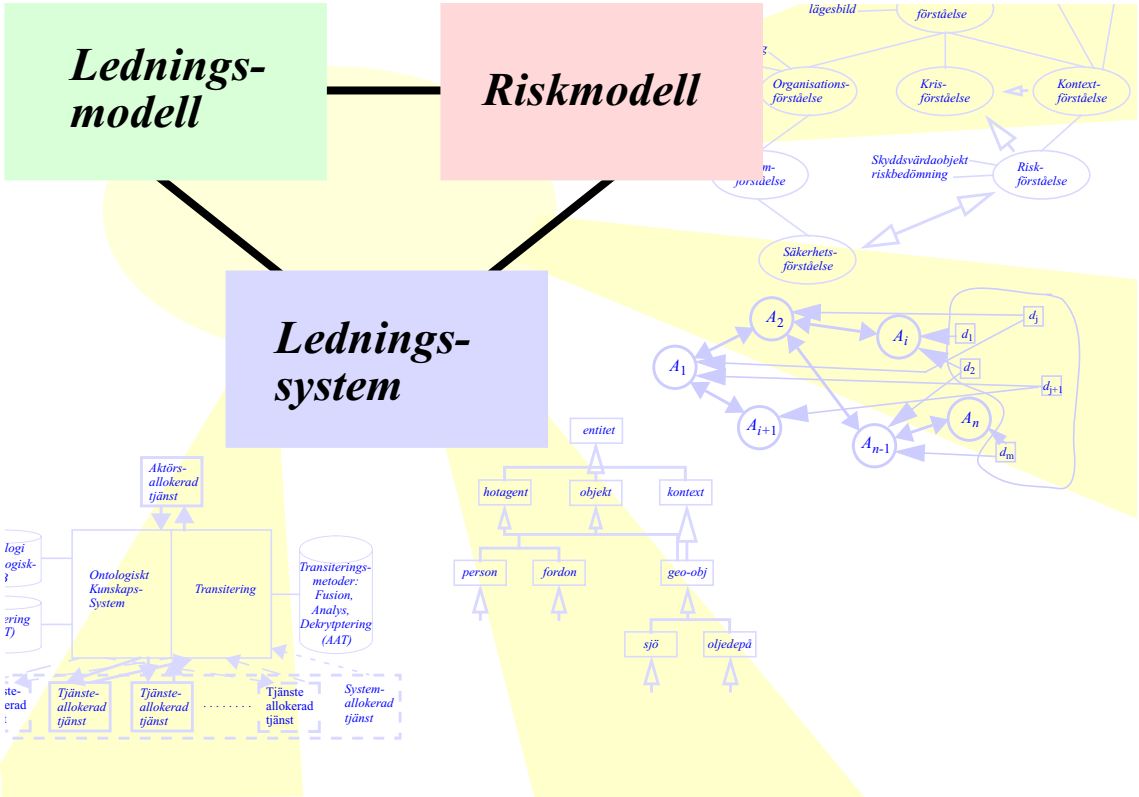
FOI-R--1569--SE
Januari 2005
ISSN 1650-1942

Metodrapport

Erland Jungert, Niklas Hallberg, Amund Hunstad

Arkitektur för tjänstebaserade krisledningssystem med preventiva och operativa förmågor



Ledningssystem
SE-581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystem
Box 1165
581 11 Linköping

FOI-R--1569--SE

Januari 2005

ISSN 1650-1942

Metodrapport

Erland Jungert, Niklas Hallberg, Amund Hunstad

Arkitektur för tjänstebaserade krisledningssystem med preventiva och operativa förmågor

Innehållsförteckning

Sammanfattning

Denna rapport presenterar ett förslag till arkitektur för krisledningssystem. Mera precist har målsättningen med studien som ligger till grund för rapporten varit att studera hur en tjänstebaserad arkitektur kan användas för att utveckla krisledningssystem med preventiv och operativ förmåga.

Rapporten är uppdelad i två huvuddelar. Del 1 behandlar på ett allmänt plan olika aspekter av krisledningssystem, med hänsyn till ledningsaspekter, situationsförståelse, ledningsmodell, tjänstekonceptet, beslutsstödshjälpmedel, lägesbild, ontologier, applikationsdatabas, informationsinsamling, nätverk och informationssäkerhet. Vidare diskuteras implementationsrelaterade begrepp som datakällor, simulering och agentbaserad systemlösning. Del 2 har en mer teknisk prägel och behandlar strukturen i ledningsmodellen med avseende på hur allokering av tjänster på olika nivåer kan ske. Vidare behandlas hur *interoperabilitet* kan förverkligas. Det vill säga hur godtyckliga tjänster, t ex sensortjänster, skall knytas till användarnära tjänster i olika beslutsstöd. I del 2 presenteras även den vidarutveckling av riskmodellen som genomförts. Slutligen diskuteras olika tekniska aspekter av IT/systemsäkerhet i krishanteringssystemet.

Den genomförda studien visar på ett antal centrala aspekter av krishanteringssystems arkitektur, vilka främst grundar sig på ledningsstrukturen. Två väsentliga aspekter för ledningsstrukturen som har identifierats är informationsflödet och beslutsfattandet. Modellen för hur beslutsfattandet sker har konsekvenser, inte bara på informationsflödet utan också, på organisationsstrukturen. Flera olika typer av organisationsstrukturer är tänkbara för krishantering, men dessa måste kunna svara upp mot kravet att hantera behov som inte alltid är förutsägbara. Bland de organisationsstrukturer som för närvarande står i fokus hör nätverksorganisationer. Dessa nätverksorganisationer består av noder som tar (1) emot information och uppgifter, (2) övervakar händelser, (3) bearbetar uppgifter, observationer och information, (5) utför uppgifter samt (6) skickar vidare information till andra noder. Information som skickas vidare kan utgöra en nedbrytning av uppgifter som andra noder skall utföra. Detta medför att varje nod har som ansvar att (i) övervaka externa händelser, (ii) ta beslut, (iii) genomföra uppgifter och (iv) kommunicera information och uppgifter.

För att i nätverksorganisationer kunna svara mot de krav som ställs på krisledningssystem ställs krav på flexibilitet och att olika aktörers arbetsplatser kan anpassas till en mängd olika *roller*, vilka medverkande aktörer måste kunna ta. Traditionella programstrukturer visar sig i sådan fall vara olämpliga och i stället har begreppet *tjänst* introducerats. En tjänst är en abstraktion av hur producenter kan åstadkomma nytta för konsumenter utan att i detalj beskriva hur detta kan realiseras. Nyttan åstadkoms genom att en producent levererar en prestation och prestationen ger en effekt hos/för en konsument. Tjänster kan beskrivas oberoende av hur de implementeras manuellt, tekniskt, eller genom kombinationer av dessa. En tjänstedefinition beskriver enbart hur konsumenter gör för att få tillgång till tjänsten och vad som produceras. Tjänster har specificerade egenskaper och med stöd av dessa kan konsumenter välja vilken realisering som fungera bäst för dem. Därmed utgör tjänsten en fasad mot producenten utifrån konsumenters perspektiv. Konsumenterna behöver inte ha kännedom om vilka producenter som tillhandhåller olika tjänster, utan kan söka efter tjänsterna som passar bäst. Tjänster kan vara synkrona och asynkrona. Synkrona tjänster ger konsumenter effekt direkt. Asynkrona tjänster kan ses som prenumerationstjänster, vilka beställs och därefter levereras fortlöpande tills dess att tjänsten avbeställs. Tjänstebegreppet utgör en hörnsten i den arkitektur som föreslås, där olika beslutsstödtjänster spelar en central roll tillsammans med tjänster för datainhämtning och kommunikation.

En central aspekt i tjänstekonceptet är tjänsters förmåga att *allokera* andra tjänster på lägre nivå. En svårighet i att göra detta effektivt och praktiskt användbart är att tjänsterna på lägre nivå måste kunna allokeras automatiskt. Ytterligare en viktig fördel som vill erhållas med tjänstekoncept är interoperabilitet, vilket ses som möjligheten att koppla samman olika tjänster på ett generellt sätt och där eventuella tekniska begränsningar har eliminerats. Interoperabilitet är ofta ett centralt krav som föranlett valet av tjänstebaserade ledningssystem. I det förslag som presenteras i denna rapport skapas interoperabilitet mellan olika tjänster med ett ontologiskt kunskapssystem, en s k *allokeringsbrygga*.

Framtida ledningssystem för krishantering kommer, med hänsyn till deras nätverksberoende, att ha högt ställda säkerhetskrav. Vid utveckling och underhåll av dessa system måste klassiska informationssäkerhetskrav beaktas som omfattar problem rörande sekretess, tillgänglighet och korrekthet. Speciellt eftersom systemen kommer att vara komplexa och svårare att kontrollera i dessa avseenden. Genom att basera krishanteringen på väl definierade roller, bearbetningsregler

och taktiska bedömningar blir det möjligt att uppfylla förekommande säkerhetskrav. Detta kräver dock att säkerhetsaspekterna beaktas tidigt i utvecklingen av dessa system och att omfattande dialog förs med användargrupper. I anslutning till utveckling av nätverksbaserade ledningssystem för krishantering kommer ett stort antal centrala forskningsfrågor att behöva studeras noggrant, vilka kan relateras till den krävande miljö som operativ krishantering ställs inför. I förlängningen kommer också frågor relaterade till skydd av enskilda individer och deras personliga integritet att ställa krav på både fortsatt forskning och politiska ställningstaganden.

En central del, i framförallt den preventiva delen av, krishantering är förmågan att bedöma sannolikheten för att olika former av hot realiseras och incidenter sker. Det vill säga, riskbedömning i framtida ledningssystem kommer att vara en viktig funktion. För att skapa en förståelse av vad riskbedömning innebär skapades en riskmodell innefattande hotagenter, hot, risker, konsekvenser, motåtgärder samt hur dessa förhåller sig till varandra. Denna riskmodell kan utnyttjas för att bedöma behovet av att preventivt hantera risker, genom att beskriva skyddsvärda objekt, vilka hot de är utsatta för, vilken risk dessa hot utgör samt vilka konsekvenser realiseringen av ett hot skulle innebära. I riskmodellen tas hänsyn till hur förebyggande åtgärder påverkar risken för att ett hot realiseras samt hur åtgärder minskar konsekvenserna av ett realiserat hot. I denna studie vidareutvecklas den riskmodell som presenterades i förstudien till detta arbete. Modellen delas upp i en datamodell som kan ligga till grund för en implementering i en databas, en ontologi som beskriver de olika koncepten i datamodell samt tre aktivitetsmodeller som beskriver hur arbetet genomförs för att exempelvis bedöma en risk. Riskmodellen är långt utvecklad men ytterligare forskning krävs och då främst för att implementera modellen och utvärdera den.

Det är av avgörande betydelse att vid krishantering ha god förståelsen för situationen, för att kunna fatta korrekta beslut om åtgärder. Denna förståelsen för vad som händer behöver vara gemensam för dem som deltar i krisarbetet. I detta ingår kännedom om miljön, krisen, vilka åtgärder som genomförs och planeras att genomföras samt vilka hot som föreligger. Lika viktigt som det är att ha förståelse för situationen är det att ha förståelse för den organisation som skall hantera krissituationen. Att ha organisatorisk förståelse (eng: organizational awareness) innebär att ha kännedom om vilka resurser som finns tillgängliga och hur dessa relaterar till varandra. Bristande organisatorisk förståelse medför ineffektiv krishantering, då de tillgängliga resurserna

inte utnyttjas optimalt. Svårigheten att överblicka insatsorganisationen blir betydligt större då denna sätts samman av enheter från olika organisationer. Detta innebär också att det kan uppstå oklarheter i hur insatser leds och koordineras. *Situationsförståelse* i ledningssammanhang kan således tolkas som aktörernas förståelse av olika sidor av krishanteringssystemet, organisationen för krishantering och det aktuella läget i vad avser förståelse och bedömning av pågående kris, dvs krisförståelse. En central fråga är hur ledningssystem skall tillhandahålla insatskoordinatorer automatiskt stöd för detta så att dessa kan leda verksamheten på ett adekvat sätt och samtidigt delge situationsförståelse till övriga aktörer, som ofta tillhör olika organisationer med olika mål och resursbehov. Kunskap om detta område och framförallt hur detta skall lösas är dålig och berör i grunden ledningsproblematiken. Fortsatt forskning omkring detta rekommenderas.

I den studie som genomförts har vissa avgränsningar varit nödvändiga att göra. I arbetet beaktas inte de juridiska och etiska aspekter som bland annat följer av ökad övervakning, samkörning av dataregister och nyttjande av gemensam lägesbild. Inte heller gemomförs någon empirisk studie av behov av en ledningsfunktion. Detta på grund av omfattningen på projektet och att dess syfte är att påvisa de tekniska möjligheterna utan restriktioner. Inte heller beaktas de närliggande aspekterna människa-systemintegration (MSI) och systemtilltro, även detta som en konsekvens av projektets begränsade omfattning.

Av förklarliga skäl kan inte några slutsatser dras på hur de förslag som presenteras i denna rapport skulle påverkas av, eller ha påverkat skeendet i Sydostasien om ett krisledningssystem funnits tillgängligt. Dock, kan det konstateras att av central betydelse för all krishantering är att den måste baseras på god krisförståelse och att väl fungerande ledningssystem måste ge stöd för detta.

Syftet med denna rapport är att ge en bild av vilka aspekter som påverkar utformningen av ledningssystem för preventiv och operativ krishantering samt att lägga grunden för utveckling av krisledningssystem genom att presentera grunderna i en arkitektur för nätverksbaserat ledningssystem för krishantering. Emellertid kan detta inte ses som en slutgiltig och färdigt utvecklad lösning för utveckling av krisledningssystem. Fortsatt arbete måste till för att i slutändan nå fram till adekvata ledningssystem som kan användas för krishantering.

Del 1

Övergripande metoder och tekniker för tjänstebaserade ledningssystem - avgränsningar och avvägningar

1. Inledning

Samhällen har genom historien drabbats av kriser och svåra påfrestningar av olika former, men en tidigare relativt förutsägbara hotbild med givna motmedel har ersatts av en alltmer komplex hotbild [1]. Förmågan att effektivt och med för allmänheten accepterade medel kunna förebygga och hantera svåra påfrestningar är nödvändig för samhällens fortlevnad. Detta är speciellt angeläget i tider då naturkatastrofer och terrorism blir allt vanligare, samtidigt som det är viktigt att värna om levnadsstandard och den öppenhet som vårt samhälle i så hög grad bygger på. Begreppet krishantering avser i denna rapport att förebygga och hantera svåra påfrestningar.

Krishantering kommer i allt högre utsträckning att vara verksamhet som plötsligt kan ställas inför helt nya hot eller att hot realiseras. Detta kommer att ställa stora krav på krishanteringssystem när det gäller förmåga att anpassas till aktuell situation. Av ekonomiska skäl, måste den vara effektiv, vilket åstadkoms genom att effektivt utnyttja enbart de resurser som behövs. Dessa resurser bör vara sådan att de även används då ej svåra påfrestningar råder, för att få kostnadseffektivitet men också rutin på att använda dessa. Integration av olika resurser bör baseras på deras funktionalitet och yttre egenskaper, snarare än teknisk realisering. Inom krishanteringsområdet finns behov av att synkronisera, koordinera och samordna vitt skilda verksamheter. Detta för att erhålla verksamhet och system som är flexibla nog att anpassas till de krav som ställs från omgivningen, och samtidigt baseras på samverkan mellan ett antal organisationer. För att kunna åstadkomma detta måste krishanteringssystem baseras på en adekvat arkitektur [2].

I det arbete som beskrivs i denna rapport har en arkitektur för tjänstebaserade krisledningssystem med preventiva och operativa förmågor tagits fram. Arbetet skall ses som ett initialt, av flera, steg som måste tas för att samhället skall erhålla en ledningsfunktion som medför en effektivt preventiv och operativ krishantering. Denna ledningsfunktion skall medge att samhällets resurser effektivt kan användas för att motverka att krissituationer uppstår, samt om krisen är ett faktum att tillgängliga resurser effektivt sätts in för att hanterar krisen och lindra dess konsekvensers. Visionen är att krishantering i första hand baseras på möjligheten att flexibelt kunna allokera och nyttja resurser i normala verksamheter, men vid behov komplettera med extraordinära insatser.

Effektiv och adekvat krishantering bygger i hög grad på effektiv ledning. För att åstadkomma effektiv ledning av krishantering är det nödvändigt att ledningsfunktionen tydliggörs och utvecklas [3], [4]. Men för att skapa en adekvat ledningsfunktion, med tillhörande tekniskt stöd, krävs djup insikt i hur framtida krishantering kommer att bedrivas, vilka krav som kommer att ställas, vilka förutsättningar som kommer att gälla och vilka typer av resurser som kommer att finnas tillgängliga. Men det är också viktigt att påvisa vilka tekniska möjligheter som finns att stödja krishantering och därigenom se nya möjligheter. Det finns näst in till oändliga möjligheter att stödja såväl ledning som samverkan med olika former av informationsteknik.

För att erhålla ett effektivt stöd för ledning och samverkan krävs informationssystem som är anpassad till dess användares och verksamhetens behov av stöd, samtidigt som de är anpassningsbar till förändrade förutsättningar. Vid utveckling av tekniska system är det således viktigt att ha en förståelse för vilka behoven är så att välgrundade val gällande teknik kan göras. Vid ledning gäller generellt att det finns behov av att kunna (1) inhämta information, (2) fatta beslut om åtgärder, (3) genomföra dessa, ofta i samverkan med andra organisationer och (4) utvärdera genomförd insats. Samverkan bygger på förmågan att kunna (1) utbyta information och (2) koordinera verksamhet.

Under senare år har stora satsningar genomförts för att bygga informationsinfrastrukturer såväl för fast kommunikation (bredband) som för mobil kommunikation (3G). Det har dock visat sig vara otillräckligt att enbart tillhandahålla informationsinfrastrukturer för att erhålla nytta av dessa och skapa tillväxt i samhället. Samtidigt ger dessa informationsinfrastrukturer en teknisk plattform för att effektivisera verksamhet och skapa förutsättningar för samverkan mellan olika organisationer.

Utvecklingen av informationssystem som stöd för ledning av krishantering måste baseras på en holistisk och koherent systemutvecklingsprocess, som utgår från verksamheten samt verksamhetens och dess aktörers behov och därefter omvandlar dessa till krav på ledningsfunktionen och på det tekniska stödet. I denna process finns ett flertal aspekter som måste beaktas; till dessa hör verksamhetsanalys, arkitekturegenskaper, kravhantering, mänskliga faktorer, IT-säkerhet etc.

Att utnyttja arkitekturer för att beskriva befintliga och tänkta system ger förutsättningar för (1) helhetssyn, (2) interoperabilitet och (3) möjlighet att studera detaljer av system utan att behöva ta del av det som för tillfället anses som oväsentligt. När det gäller helhetssyn ger exempelvis konceptet *System-av-system* möjlighet att betrakta systems enskilda och avgränsade delar från olika abstraktionsnivåer. Interoperabilitet erhålls genom att system på olika nivåer har väldefinierade gränssnitt. Dessa gränssnitt isolerar också funktionalitet och yttre egenskaper från den faktiska realiseringen. Ett exempel på sådana gränssitt är tjänstekonceptbaserade gränssnitt.

En annan mycket viktig aspekt som måste beaktas vid utveckling av ledningsfunktion för krishantering är IT-säkerhet. IT-säkerhet beaktas ofta alldeles för sent i utvecklingsarbetet, vilket leder till att *illa anpassade lösningar* måste forceras in i system. Detta resulterar i försämrad effektivitet, med avseende på såväl säkerhet som funktionalitet, och i värsta fall att system överhuvudtaget inte kan tas i drift på grund av bristande säkerhet.

1.1 Mål

Målet med arbetet som beskrivs i denna rapport är *en arkitektur för tjänstebaserade krisledningssystem* med preventiv och operativ förmåga.

1.2 Syfte

Syftet med arbetet är att skapa en tjänstebaserad arkitektur som kan användas för att utveckla krisledningssystem med preventiva och operativa förmågor.

1.3 Avgränsningar

Inom ramen för detta arbete beaktas inte de juridiska och etiska aspekter som bland annat följer av ökad övervakning, samkörning av dataregister och nyttjande av gemensam lägesbild. Inte heller gemomförs någon empirisk studie av behov av en ledningsfunktion. Detta på grund av omfattningen på projektet och att dess syfte är att påvisa de tekniska möjligheterna utan restriktioner. Inte heller beaktas de närliggande aspekterna människa system integration (MSI) och systemtilltro, även detta som en konsekvens av projektets begränsade omfattning.

1.4 Kopplingar till förstudien

Arbetet i detta projekt baseras i hög utsträckning på det arbete som genomfördes inom Förstudie avseende förslag till integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering [3]. Detta projekt skall ses som en fördjupning av förstudien inom områdena ledningsmodellen, riskmodellen och IT-säkerhet som är de områden det är av intresse att gå vidare med. Emellertid är dock de underliggande frågeställningana de samma.

2. Bakgrund

Inom förstudien [3] togs ett förslag fram till en integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering. Fundamentala antaganden som gjordes inför vidare forskningsverksamhet var bland annat:

- För att en ledningsfunktion skall vara nyttig bör den kunna användas även då kris inte råder.
- Av denna anledning måste ledningsfunktionen kunna anpassas till den dagliga verksamheten.
- Ledningsfunktionen måste ha kapacitet för hantering av extraordinära händelser.
- Människan måste spela en central roll i ledningsfunktionen.

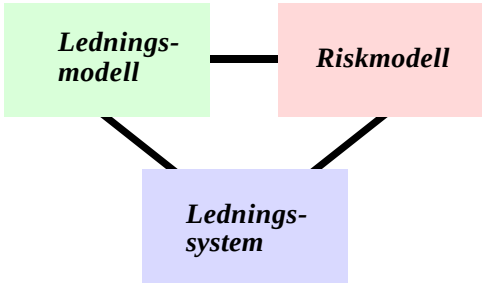
För att säkra anpassning till daglig verksamhet bedömde förstudien nedan listade områden, som lämpade:

- Registrering och övervakning av sjukdomar (t ex virussjukdomar).
- Miljöfaktorer (t ex luftkvaliteten).
- Transporter av farligt gods; kontroll och övervakning.
- Kriminella aktiviteter.
- Bränder.

De ovan nämnda områden har potential både enskilt och i kombination med någon av de övriga att kunna utvecklas till olika typer av kriser. Tillämpningsmöjligheter för polis, räddningsverk och olika kommunala instanser existerar i rik omfattning, i vardag såväl som då svåra påfrestningar råder.

Vidare ansågs i förstudien att det var av vikt att i anslutning till bekämpning av kriser i ett operativt sammanhang också studera preventiva aspekter. Detta kan göras som en del av övervakningsprocesser för skyddsvärda objekt, som t ex:

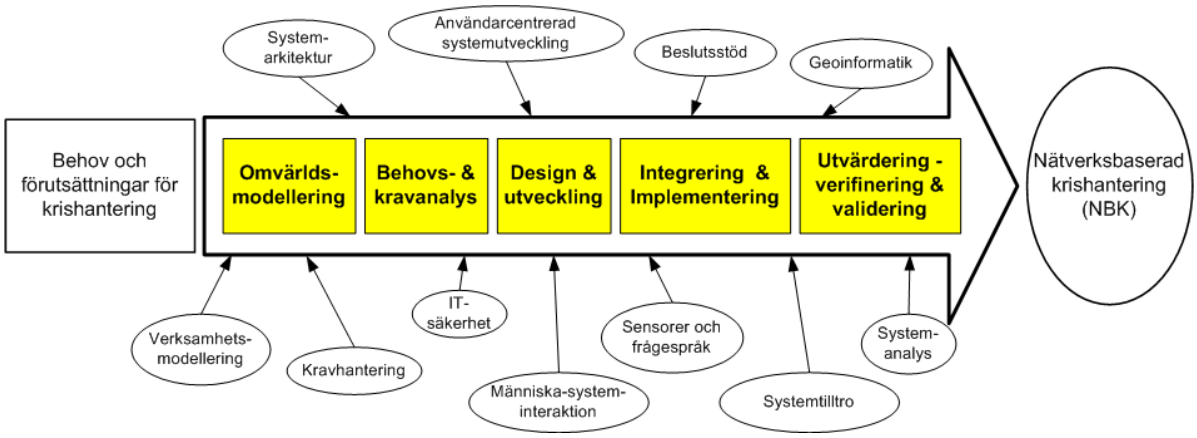
- Flygplatser (extern och/eller intern övervakning).
- Hamnar (extern och/eller intern övervakning).
- Kärnkraftverk (extern övervakning).
- Infrastrukturer, t ex för el-överföring.



Figur 1. Illustration av sambanden mellan ledningsmodell, riskmodell och ledningssystem.

Dessa antaganden och slutsatser gör förstudien efter

- en *analys av tänkbara generella hotbilder* mot samhället och viktiga samhällsfunktioner. Hot kan grovt indelas i hot utgående som resultat av mänskligt agerande (antagonistiska respektive icke-antagonistiska hot) och hot som resultat av ej mänskligt agerande (tekniska fel, tillverkningsfel, naturrelaterade händelser och brister i andra system och beroenden av dessa)
- en observation av att insatsledning vid *krishantering kräver kraftfullt ledningsstöd*, vilket förslagsvis kan baseras på resultat ur forskning kring aktionsstyrning [5],
- framtagande av ett *ledningsramverk* där ett ledningssystem baserar sig på en ledningsmodell respektive en riskmodell, som illustreras av figur 1 och figur 2.
- *identifierande av centrala forskningsområden*, enligt figur 2 som berörs av problematiken kring utvecklingen av ledningssystem för krishantering.



Figur 2. Illustration av systemutvecklingsprocessen.

2.1 Regional samverkan

eNavet [6], GOTSAM [7] och CeSam-C är exempel på svenska satsningar där man på olika sätt studerar integration av vardaglig verksamhet med verksamhet som behövs under svåra påfrestningar, det vill säga krishantering. Bärande i dessa satsningar är vikten av samverkan mellan olika myndigheter och andra aktörer.

eNavet är ett samarbete mellan Linköpings kommun, Tekniska Verken och SAAB med fokus på teknik för hantering av gemensam lägesbild och integrering av detta i ledningsteknik och ledningsfunktioner. Detta skall vara tillämpligt i såväl vardagliga situationer som mera krisbetonade; som exempel på scenarion har man inom eNavet utgått från ett par fallstudier med olika inriktning. Det första scenariot utgörs av en tankbil som transporterar ammoniak och som välter i en rondell utanför Linköping, i lägesbilden illustreras spridningsrisker och därpå följande konsekvenskedjor. Det andra scenariot fokuserar på mera vardagligt användande av eNavets potential för samordning av olika insatser inom ett lokalsamhälles ökande behov av äldreomsorg. Detta blir av särskild vikt i och med den ökade satsningen på vård av äldre i hemmet.

eNavet avses att även fungera i ett antal andra sammanhang än vad dessa senarioexempel illustrerar, men åtminstone indikerar deras olika karaktär att det existerar en betydande bredd på det spektrum inom vilket eNavets lägesbildsteknik med kringfunktioner kan användas.

Inom GOTSAM studeras delvis liknande problem och behov, men utgående ifrån de förutsättningar, begränsningar och möjligheter ett ösamhälle som Gotland ger. Det utsatta läget Gotland har som ö nödvändiggör ett effektivt och tätt samarbete mellan öns olika krisaktörer för att kunna hantera allvarliga olyckor och andra typer av svår påfrestningar. Det är av stor vikt att undvika dubbelarbete och samtidigt ha överblick av olycks- och krissituationer samt att snabbt kunna sätta in rätt resurser. Följande gotländska myndigheter deltar i projektet: Länsstyrelsen, Gotlands Kommun, polisen, försvarsmakten, kustbevakningen och sjöfartsverket.

Inom Uppsala läns samverkansorganisation CeSam-C (Central samordning inom C-län) samordnas polis, räddningstjänst, försvarsmakten, länsstyrelsen, SOS Alarm, Radio Uppland och landstinget [8], [9]. Länets status som kärnkraftslän är en av flera orsaker till CeSam-C:s tillblivelse. Under början av 1990-talet initierades ett arbete med att effektivisera samordning mellan länets kommunala räddningstjänster och samverkan med Försvarsmakten. År 2000 formaliserades arbetet inom CeSam-C.

2.2 Svensk forskning

Bland andra svenska forskningssatsningar bör nämnas verksamheten inom Centrum för riskanalys och riskmanagement (LUCRAM) vid Lunds Universitets [10] och speciellt deras ramforskningsprogram Framework programme for Risk and Vulnerability Analysis (FRIVA).

FRIVA består av följande delprojekt (DP):

- DP2: Metoder för risk- och sårbarhetsanalys
- DP3: Metodutveckling
- DP4: Krishantering och social sårbarhetsanalys
- DP5: Proaktiv krishantering och säkerhetskultur på myndighetsnivå
- DP6: Kommunal och regional sårbarhetshantering
- DP7: Sårbarhetsanalys av storskalig infrastruktur: el- och vattenförsörjning
- DP8: Sårbarhetsanalys av storskalig infrastruktur: tele- och IT-system
- DP9: Statistiska simulerings- och beräkningsmodeller för komplexa system

Inom DP2, Metoder för risk- och sårbarhetsanalys, är tanken att integrera resultat från övriga delprojekt och därigenom nå ett helhetsperspektiv på hur metoder för risk- och sårbarhetsanalys kan användas. Detta medför att DP2 har en samordnande roll i hela FRIVA-programmet. DP3-DP6 fokuserar på krishanteringens olika verksamhetsområden med avseende på teorier, koncept, modeller och begrepp. DP7-DP9 fokuserar på förbättringsarbete rörande de tekniska systemen. Särskild vikt läggs på förståelse och systematiskt analys av ömsesidigt beroende mellan olika tekniska infrastrukturer.

I förhållande till det ledningssystemperspektiv som denna rapport utgår från, är problemmässig närhet och anknytningar tydligast till det informationssystemperspektiv som DP7 har, även om ledningssystemaspekter verkar vara något mindre accentuerade. Vidare kan sannolikt forskningsresultat från DP2 och DP9 utgöra värdefulla bidrag till utveckling av ledningssystem. Resultat från övriga delprojekt är också av intresse vid arbetet med utveckling av arkitekturer för krisledningssystem, till exempel med avseende på hur de olika verksamhetsområdenas lednings- och beslutsstödsbehov ser ut, hur social sårbarhet kan uppstå och bör hanteras.

Generella aspekter på risk- och sårbarhetsanalysens roll lyfts fram i en forskningsrapport [11] framtagen inom LUCRAM. Särskild lyfts här fram även vikten av att ta hänsyn till myndig-heters riskhantering generellt, bland annat med avseende på aktiviteter som ligger inom myndighetens tillsynskontroll respektive aktiviteter som ligger utanför myndighetens kontroll men som samtidigt har potential att påverka myndighetens ansvarsområde.

Beredskap och krishantering i svenska kommuner är verksamhet som i betydlig grad bör ges möjlighet att påverka ledningssystemutveckling, och lämpligen med anknytning till arkitekturavvägningar kring ledningssystem. Inom projektet Beredskap och krishantering i svenska kommuner har forskare vid Försvarshögskolan i en serie rapporter publicerade av Krisberedskapsmyndigheten, studerat kommunala instansers erfarenheter av kriser och krishantering [12], [13], [14]. Dessutom studerades drivkrafter och motivationsfaktorer för arbete med säkerhets- och beredskapsfrågor. Den erfarenhet som har inhämtats via dessa studier bör ingå som påverkande faktorer vid vidare utveckling av krisledningssystem.

Erfarenheter så här långt av den svenska försvarsmaktens övergång till nätverksbaserat försvar och tjänstebaserade ledningssystem diskuteras i [15]. Erfarenheterna härifrån rörande behov av situationsmedvetande och tjänstebaserade system är i betydande grad även relevanta för civila behov.

Då informations- och IT-säkerhet är synnerligen kritiska faktorer för att kunna realisera krisledningssystem, bör även den verksamhet nämnas som planeras inom ett regionalt kompetenscentrum för informationssäkerhet i Linköping-Norrköpingsregionen. I denna centrumbildning planeras följande aktörer att bidra: Linköpings universitet, lokal industri, Landstinget i Östergötland och Totalförsvarets forskningsinstitut (FOI).

2.3 Internationell forskning

På EU-nivå har säkerhetsfrågor i vid mening blivit uppmärksammade i rapporten *Research for a Secure Europe*[16]. Globaliseringen medfört ett antal fördelar för EU:s utveckling, men även nya hot och risker. Sjukdomar sprids snabbare i och med att människor rör sig i allt högre utsträckning över allt större områden. Lokala konflikter kan ge kedjereaktioner globalt på grund av att ekonomiska system, transport- och kommunikationssystem är sammankopplade. Dessutom utgör terrorism, som med hjälp av Internet blivit en distribuerad verksamhet, ett hot som i ökande grad måste beaktas. Detta tillsammans med andra observationer, nödvändiggör betydande forskningsinsatser för att hantera de olika indikerade problemen. EU-rapporten poängterar teknologins roll som möjliggörare[1] för ett säkrare Europa. Rapporten observerar att detta kräver en industri som är nära utvecklings- och forskningsfronten, en stark kunskapsinfrastruktur samt en ändamålsenlig finansiering och optimal resursanvändning. Detta kräver dock förbättrat samarbete mellan EU:s medlemsländer och betydande forskningsinsatser. Dessa konstateranden utgör några av de skäl till att ett europeiskt säkerhetsforskningsprogram föreslås med start i 2007.

Motsvarande utveckling har, tillsammans med händelserna den 11 september 2001, resulterat i satsningarna i USA på ett samordnat departement, Department of Homeland Security [17]. Betydande forsknings- och utvecklingssatsningar finansieras från detta nya departementet, bland annat med relevans för krishantering och ledningssystemutveckling men detta finns i betydande

1. ”Force-enabler”

grad belyst i många andra sammanhang och av denna anledning diskuteras detta inte vidare i detta arbete. Detta hänger också samman med de generella begränsningarna i detta arbete.

Komplexiteten i verksamheten krishantering speglar forskningen inom området. Teoribildningen inom området är inte entydig, men inslag i denna som bör ligga till grund för vidare arbete framgår av följande aspekter:

- Situations-, [18], och organisationsmedvetande, [19], är faktorer som ger strategiska fördelar vid hantering av krissituation, men även i ett mera vardagligt användande av ledningssystem. Att uppnå sådant medvetande måste vara resultatet av användningen av ledningssystemen, men själva medvetandet måste dock finnas hos användarna själva. Utöver situations- och organisationsmedvetande måste ett tydligt säkerhetsmedvetande finnas.
- Koordinering av aktiviteter och aktörer inom krishantering måste utformas på ett teoretisk välgrundat sätt. Den multidisciplinära karaktären på koordineringsproblematiken framgår av [24]. Shen och Shaw, [23], diskuterar vikten av att identifiera vad som behöver koordineras, vilka koordineringsmekanismer som krävs och hur informationsteknologi kan bidra med dessa mekanismer.
- Strikt hierarkiska organisationer har klara begränsningar vid krishantering. Dynamiska och självorganiserande organisationsmodeller med distribuerad auktoritet (heterarkier) ger andra möjligheter. Hur optimala strategier för informations- och ledningsflöden respektive kommunikation kan konstrueras diskuteras i [22].
- Självorganiserande system-av-system baserade på agentteknik har ett antal fördelar för bland annat krishantering, vilket diskuteras i [20] respektive [21].
- De ovan nämnda inslagen realiseras sannolikt i koalitioner med olika typer av krishanteringsaktörer, vilket vidare diskuteras i [24]. Agentteknik är en hörnsten i detta arbetet.

Vidare diskussion om dessa aspekter återkommer i senare delar av denna rapport.

3. Ledningsaspekter

När det gäller krishantering och riskhantering finns det ett flertal olika modeller som beskriver hur detta skall genomföras [11]. Generellt kan krishantering dock anses bestå i att (1) förebygga för att minska sannolikheten för att svåra påfrestningar inträffar, (2) förbereda genom att planera för insatser vid olika krissituationer, (3) akut avhjälpa för att möta de behov som uppstår vid en incident samt (4) avveckla och återuppbygga för att återföra samhället till ett normaltillstånd. I detta sammanhang syftar förebygga till att minska sannolikheten för att svåra påfrestningar inträffar, förbereda handlar om att planera insatser vid realisering av hot, akut avhjälpa syftar till att möta de behov som uppstår vid en incident och avveckla och återuppbygga syftar till att återföra samhället till ett normal tillstånd.

Framtida krishantering kommer att baseras på nära samverkan och informationsutbyte mellan olika heterogena organisationer. Dessa heterogena organisationer har sina egna mål som kan ses som delmål i att genomföra krishanteringen. En aspekt som är viktigt för att förbättra krishanteringen är att stärka samverkan mellan olika involverade organisationer, där delad situationsförståelse, interorganisatoriskt beslutsfattande och väl synkroniserade insatser är centralt [20]. När det gäller synkronisering eller koordinering av insatser finns ett antal beroenden som måste hanteras. Shen och Shaw [23] diskuterar tre olika typer av beroenden; (1) delning, (2) flöde och (3) passa. Delningsberoende uppstår när flera aktiviteter kräver samma resurs. Flödesberoendet uppstår när en aktivitet är beroende av att en annan aktivitets genomförts. Beroendet att passa uppstår då behovet integration och samverkan finns, det vill säga interoperabilitet. Dessa beroenden kan uppstå mellan aktörer, aktiviteter samt aktör och aktivitet. Exempelvis måste vissa aktivteter ske samtidigt eller i en specifik sekvens. Vissa aktörer blir tilldelade flera aktiviteter och måste välja vad som skall göras först. Det samma gäller med resurser som flera aktörer behöver men som finns i begränsat antal. För att hantera den dynamik och den mångfald av varianter kriser omfattar, krävs en modulär organisation som kan anpassas till den aktuella situationen [23]. Koordination av verksamheter inom en modulär organisation förutsätter en strukturering gällande beslutsfattande. När det gäller delningsberoende är någon form av interorganisatorisk resursfördelare nödvändig, exempelvis en *koordinator*. När det gäller flödesberoende så förordas planering, som stöd för realtidskommunikation gällande aktionsplaner, anmälan om aktiviteter och beordring av aktiviteter. För att hantera olika organisationers mål och för att undvika konflikter av aktiviteter krävs regelbundna möten.

Det finns flera olika typer av organisationsstrukturer som är tänkbara för krishantering, exempelvis hierarkiskt orienterade, processorienterade och heterarkiskt orienterade. Heterarki organisationer beskrivs oftast som en nätstruktur av samverkande noder. Vilken nod som leder och koordinerar en verksamhet är helt situationsberoende. Den organisationsstruktur som anses vara mest lämpligt krishantering är någon form av hybrid organisation, då dessa anses lämpliga att möta behov som inte alltid är förutsägbara. Nätverksorganisationer kan ses bestå av noder som tar (1) emot information och uppgifter, (2) övervakar händelser, (3) bearbetar uppgifter, observationer och information, (5) utför uppgifter samt (6) slutligen skickar vidare information. Informationen som skickas vidare kan utgöra en nedbrytning av uppgifter [22]. Detta medför att varje nod har som ansvar att (i) övervaka externa händelser, (ii) ta beslut, (iii) genomföra uppgifter och (iv) kommunicera information och uppgifter.

Att effektivt kunna samverka vid genomförandet av insatser kräver tillit övriga aktörer. Det kan vara svårt att skapa tilllit när samtliga aktörer är fysiskt lokaliserade på samma plats, än svårare är det då samverkan sker på distans via kommunikationsnätverk och då ledningen av insatsen tillhör en annan organisation, som blir fallet i nätverksbaserade organisationer [18]. Detta innebär att kravet på att bygga och säkerställa tillit för denna typ av organisation är av stor vikt.

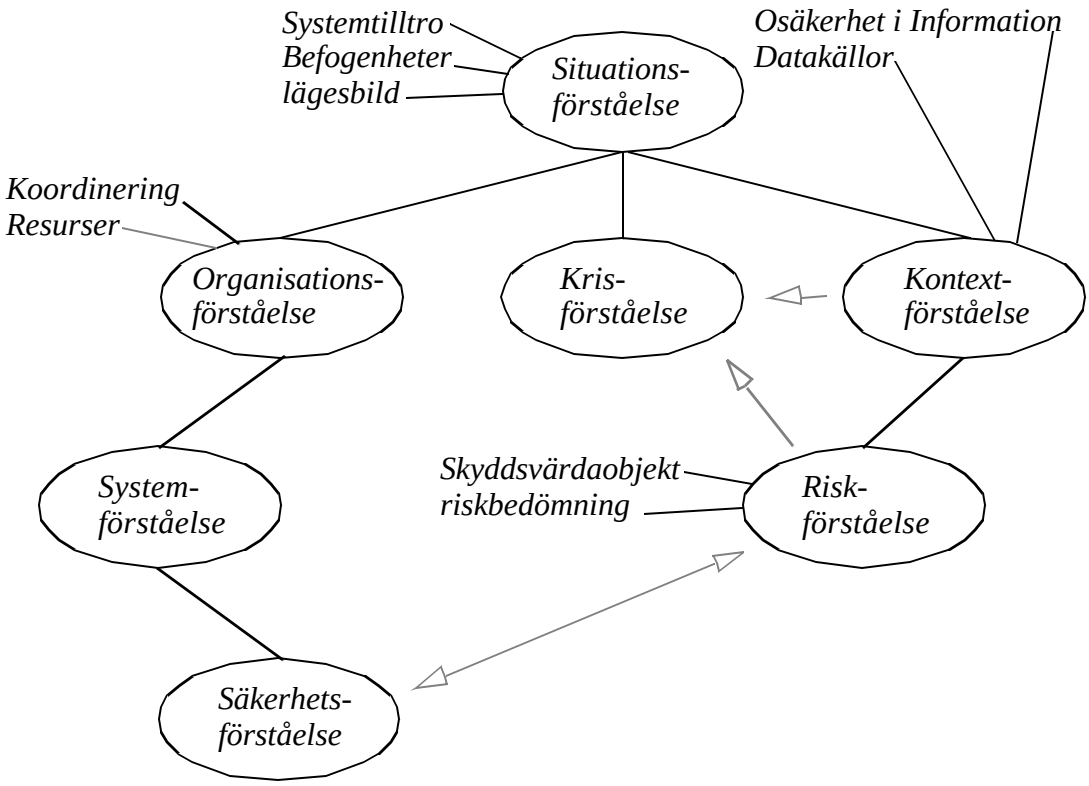
4. Förståelse för situationen

Att ha förståelse för situationen är centralt för att vid hantering krissituationer kunna ta korrekta beslut om åtgärder. Förståelsen för vad som händer behöver vara gemensam för samtliga aktörer som deltar i att hanterar krissituationen. I situationsförståelse ingår kännedom om miljön, krisen, åtgärder som genomförs, åtgärder som planeras att genomföras samt vilka hot som föreligger. Lika viktigt som det är att ha förståelse för situationen är det att ha förståelse för den organisation som skall hantera krissituationen, för att veta vilka resurser som finns tillgängliga.

4.1 Organisationsförståelse

Att ha organisatorisk förståelse (eng: organizational awareness) innebär kännedom om vilka resurser som finns tillgängliga och hur dessa relaterar till varandra [19]. Bristande organisatorisk förståelse leder till ineffektiv krishantering, då inte de egna resurserna utnyttjas optimal. Svårigheten med att överblicka insatsorganisationen blir betydligt större då denna sätts samman av team från olika organisationer. Detta innebär i sin tur även att det kan uppstå oklarheter i hur

insatsen leds och koordineras. Situationsförtåelse finns också belyst och definierat av Stanton et al. i [18]



Figur 3. Situationsförståelse, dess inre samband och relationer till yttre beroenden och villkor.

4.2 Situationsförståelse

Med utgångspunkt från vad som sagt om situations- och organisatoriskförståelse framstår det som nödvändigt att dela upp situationsförståelse i ett antal underbegrepp i enlighet med figur 3. Situationsförståelse påverkas av en mängd olika externa faktorer såsom aktörernas systemtilltro och deras befogenheter men också den aktuella lägesbilden som i sin tur beror av det MSI-stöd som finns tillgängligt. Den därefter följande nivån kan betecknas som en *ledningsnivå* som beror av förståelsen av organisationen, själva krisen och den kontext i vilken krisen pågår. Organisationsförståelsen påverkas av faktorer som koordinering av verksamheten men också av tillgängliga resurser. Kontextinformationen påverkas av osäkerheten i inkommande information men även av de datorkällor som måste finnas tillgängliga och som i de flesta fall kommer att utgöras av olika typer av sensorer som kommer att generera data som till viss del är osäker; därav problematiken kring osäkerhet gällande information. Till kontextförståelse kan på lägre nivå knytas riskförståelsen som är beroende de två faktorerna skyddsvärda objekt samt metoder

för riskbedömning, vilket diskuteras vidare i del 2 av rapport. Vidare på lägre nivå ingår systemförståelse som identifieras som en del av organisationsförståelsen. Systemförståelse utgör en överordnad del av säkerhetsförståelse. Till dessa olika nivåer kan också kopplas flera olika svagare samband såsom t ex riskförståelse och kontextförståelse påverkan på krisförståelse.

Med utgångspunkt från de olika typer/nivåer av förståelse, vilka var för sig utgör en del av situationsförståelsen, framgår att de var för sig relaterar sig till ledning vid krishantering och att de utgör mycket komplexa samband som inte till alla delar är kända. Därför är det angeläget att studera dessa samband och relationer till ledningsproblematiken för att öka kunskapen om och förmågan till ledning i anslutning till utveckling av ledningssystem för krishantering, dvs alla dessa aspekter måste ses som en del av systemarkitekturen.

5. Ledningsmodell

Ledningsmodellen som utvecklades under förstudien avsåg att omfatta tekniker för datainsamling för att preventivt och operativt upptäcka, identifiera, bedöma och hantera olika typer av hot [3]. Huvudsyftet med ledningsmodellen var att den skulle kunna ligga till grund för realisering av ledningssystem för preventiv och operativ ledning av krishantering. Grundläggande krav på ledningen, som hanteras i ledningsmodellen, utgörs av (1) övervakning av aktuella insatsmiljöer och hotagenter, (2) samverkan mellan olika aktörer, (3) koordinering av insatser samt (4) information till andra aktörer och allmänheten. Operativt skall ledningsmodellen stödja enskilda myndigheter att sätta in rätt insats vid rätt tillfälle så att olika kriser bekämpas på effektivaste sätt. I ledningsmodellen ingår ett operatörsstöd vars syfte är väsentligen att ge ett adekvat stöd för beslutsfattandet samt för kommunikation mellan olika användarkategorier. För att klara den funktionalitet som krävas i ett ledningssystem för krishantering, måste en riskmodell integreras med ledningsmodellen.

Således utgörs en del av målsättningen att vidareutveckla och fördjupa den ledningsmodell för preventiv och operativ krisledning som beskrivs i förstudien till detta arbete [3] och delvis i Jungert et al. [4]. Till detta kommer att modellen också skall vara anpassad till de ledningsaspekter som diskuterats i avsnitt 3 och som i flera avseende är baserade på aspekter som framförts av Levchuk et al. [22] och som grundar sig på en tämligen platt ledningsstruktur. Emellertid utgör en väsentlig del av Levchuks arbete ett försök att utveckla en flexibel struktur på automa-

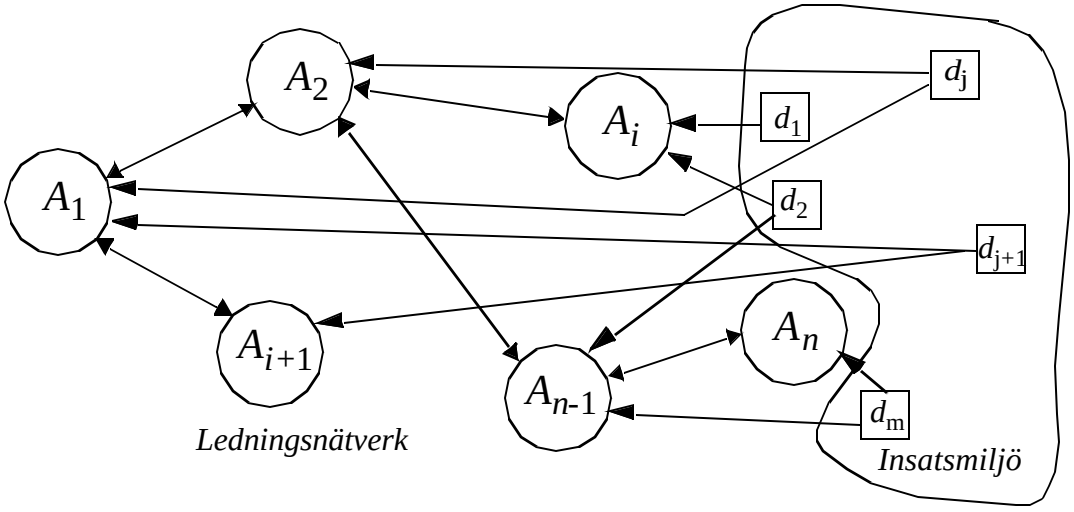
tiskt sätt, vilket inte görs i det arbete. Skälet till detta är att det med säkerhet kommer att leda till ett alltför komplext system. Det arbete som beskrivs i Levchuks arbete bör ses som ett experiment. Vidare diskuteras i Shen och Shaw [23] aspekter som har att göra med hur arbetsordningen skall fördelas, dvs koordineras, och vilka arbetsuppgifter som skall genomföras i en krissituation; detta har redan diskuterats i avsnitt 3. Stor del av grunden i Shen och Shaws arbete har hämtats från arbete om koordinering av Malone och Crowston [24]. Koordinering spelar en central roll vid ledning och har givetvis påverkat utformningen av arkitekturen också i detta arbete. Emellertid, grunden för denna ledningsmodell presenteras i detta arbete kallas ledningsarkitektur, vilket också diskuterats förstudien [3]. Ledningsarkitekturen påminner till viss del om den agentflödesmodell som beskrivs av Levchuk et al. [22]. Kännetecknande för ledningsarkitekturen är att den är tjänsteanpassad.

5.1 Applikationsstruktur

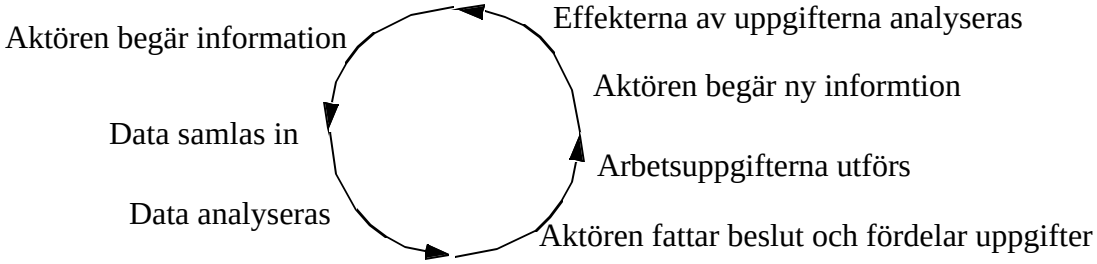
Ledningsmodellens grundläggande principer kan beskrivas i enlighet med figur 1. Principen utgörs av ett antal aktörsapplikationer vilka utgör arbetsplatser för ett antal aktörer. Dessa har till sitt förfogande ett antal tjänster som kan vara bestämda på förhand med avseende på aktörernas arbetsuppgifter eller vara bestämda av aktörena själv. Tjänster kan också bytas ut, tas bort eller så kan helt nya tjänster kopplas till. Varje aktör kan kommunicera med andra aktörer i det existerande nätverket genom olika kommunikationstjänster. Den information som överförs på detta vis kan vara efterfrågad men behöver inte vara det. Tillgängligt i nätverket skall också finnas en mängd datakällor, vilka inhämtar information från insatsmiljön eller från tillgängliga databaser. Alternativt kan sådan information vara av a priori-typ, till exempel kartor. Aktören skall kunna inhämta information från dessa datakällor genom att antingen prenumerera på informationen eller utnyttja tjänster som hämtar data från lämpliga datakällor. I de senare fallen kommer aktörena inte att behöva avgöra vilka datakällor som information inhämtas från.

Principerna för ledningsstrukturen, som utgörs av ett nätverk (figur 4). Figur 4 beskriver ett antal olika aktörsapplikationer som kommunicerar med varandra samt med olika datakällor. Denna ledningsstruktur kan förefalla vara helt platt men i praktiken kommer den inte att vara det, då någon form av koordinator kommer att behövas, vilket diskuteras vidare i avsnitt 5.2.

Ledningsmodellen kommer att fungera som en loop vilket framgår av figur 5. Denna loop kallas för beslutsloop och kan beskrivas enligt följande. En aktör begär att få ta del av information från insatsmiljön. Information samlas in med hjälp av t ex en eller flera sensorer, analyseras och returneras till aktören som på grundval av den erhållna informationen fattar beslut och beordrar dess genomförande. Därefter begär aktören information från samma område för att verifiera effekten av beslutet. På grundval av den nya informationen kan nya beslut fattas. Aktören fullbordar varv efter varv i beslutsloopen till dess arbetet har slutförts.



Figur 4. Strukturen i ledningsnätverket med dess aktörsapplikationer (A_i) och datakällor (d_j) med vars hjälp information hämtas från insatsmiljön.



Figur 5. Beslutsloopen i ledningsystemet.

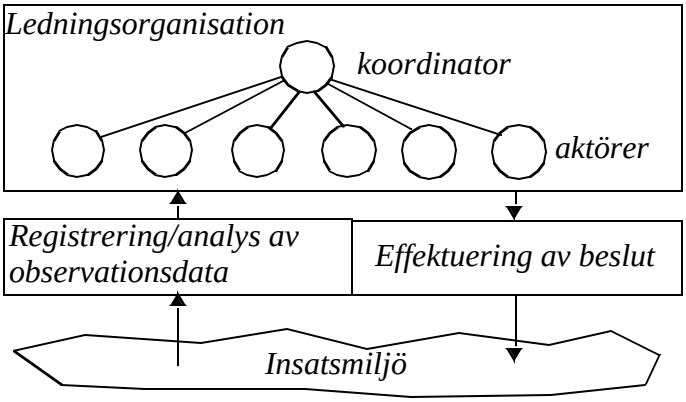
5.2 Ledningsarkitektur

Den flödesmodell som beskrivs av Levchuk et al. [22] leder fram till en i de flesta fall hierarkisk ledningsmodell även om den framställs som flexibel. Av denna anledning talas det om en *heterarkisk* (eng. heterarchical) modell som definieras som ett självorganiserande nätverk utan någon överordnad beslutsfattare. Det finns vidare en dubbelriktad relation mellan beslutsfattare

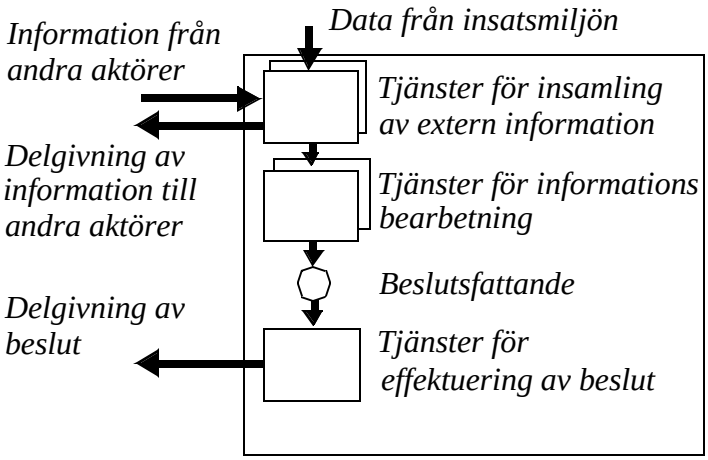
som bl a innebär att information kan överföras mellan dem i båda riktningarna. Trots detta ger arbetet intryck av att resultatet kommer att vara ganska hierarkiskt. I förslaget till ledningsmodell som beskrivs här kan modellen karaktäriseras som platt men med en något överordnad aktör med uppgift att koordinera den pågående verksamheten. Anledningen till att en sådan struktur har valts är att det inte är önskvärt med en strikt hierarkisk ledningsstruktur eftersom en sådan ofta blir rigid. En sådan struktur är inte önskvärd eftersom de kriser som ledningssystemet måste kunna hantera ofta är av skiftande karraktär. Vidare kommer i varje kris många olika myndigheter och organisationer att vara involverade. Dessa kommer i de flesta fall att ha sin egen beslutsordning och med sitt speciella ansvar, men också sina egna resurser för insamling av information. Till detta kommer också krav på utbyte av information mellan dessa aktörer. Exempel på myndigheter som kommer att vara involverade i denna typ av verksamhet är polis och räddningstjänst. Övergripande kan således ledningsstrukturen beskrivas enligt figur 6. I denna struktur kan *koordinatorn* ses som en aktör som övervakar det pågående händelseförloppet för att bl a tillse att ingen del av verksamheten faller mellan stolarna och att all nödvändig information finns tillgänglig för alla aktörer. Koordinatorn skall också kunna fatta övergripande beslut och kan därför likställas med en räddningsledare. Samtliga aktörer har till uppgift att samla in *relevant* information, sprida specifika information för stöd åt övriga aktörer, inklusive koordinatorn, samt att inom sitt problemområde fatta beslut och tillse att dessa effektueras. Till detta kommer också behovet av att samtliga aktörer vid behov måste kunna kommunicera med varandra.

Av figur 66 framgår det övergripande sambandet mellan insatsmiljö och ledningsstruktur. Tanken är att samtliga aktörer skall kunna samla in information från insatsmiljön och dessutom kunna effektuera olika typer av beslut. Vidare skall den information som aktörerna med hjälp av olika typer av *tjänster* (avsnitt 7) samlar in via olika datakällor kunna delas mellan de olika aktörerna. Detta skall kunna ske på flera sätt och samtliga aktörer har ansvar för att detta sker. Antingen skall aktörerna kunna utnyttja samma datakällor eller så skall informationen kunna skickas vidare till antingen alla övriga aktörer eller till aktörer som har *abonnerat* på den aktuella informationen. Ett avsevärt problem i detta sammanhang är att tillse att samtliga aktörer får tillgång till en så komplett informationsmängd som möjligt och att informationsosäkerheten är minimerad. Emellertid måste de olika förmågorna hos varje enskild aktör liksom hos koordinatorn kunna beskrivas i enlighet med någon lämplig struktur. Det interna informationsflödet hos

varje enskild aktör kan beskrivas som den information som passerar noden, vilken utgör en del av ledningsarkitekturen. Strukturen hos en sådan aktörsnod som utgör en del av ledningsprocessmodellen finns åskådliggjord i figur 7. Tjänsterna kommer att vara beroende av varandra på olika nivåer, vilket kommer att diskuteras vidare i avsnitt 7. En viktig konsekvens av beroendet mellan de olika tjänstetyperna är att när en viss tjänst behöver tillgång till någon annan tjänst måste allokeringen av den nya tjänsten ske automatiskt utan inblandning av aktören. Primärt gäller detta de båda tjänstetyperna TAT och SyAT. Således måste det finnas stöd för detta i systemet. Hur allokeringen av tjänster på lägre nivå skall ske kommer att beskrivas i del 2.



Figur 6. Skiss över ledningsarkitekturen i krishanteringssystemet.



Figur 7. Informations och beslutsflödet i en aktörsnod i ledningsarkitekturen.

En frågeställning som inte kommer att diskuteras vidare i denna rapport hänför sig till att system måste bestå av ett antal olika aktörer med specifika roller som kommer att kunna definieras på förhand. Varje sådan roll kommer att behöva tillgång till ett antal tjänster. Vilka dessa tjänster är kommer inte att diskuteras vidare i denna rapport. Inte heller kommer någon diskussion att

ske avseende vilka dessa roller är. Skälet till detta är att de olika tjänsterna kommer att vara tillämpningsberoende, vilket inte påverkar principerna i ledningsmodellen. Av denna anledning är det nödvändigt att i ett senare skede studera de olika rollerna och deras behov av tjänster.

I detta sammanhang har en systemlösning diskuterats som bygger på användning av multipla tjänster i en nätverkslösning. Emellertid existerar också andra möjliga systemlösningar. Bland dessa kan speciellt nämnas lösningar som bygger på s k koalitionsformationer (coalition formations). Koalitionsansatser är ganska likartade när det gäller möjligheten att välja om ledningsstrukturen skall vara platt [25] eller mer hierarkisk [28]. Gemensamt för båda dessa ansatser är emellertid att de ofta bygger lösningsstrukturen på olika kunskapsbaserade modeller där multipla intelligenta agenter (avsnitt 17) utgör en central del.

6. Riskmodellering

Riskmodellering måste utgöra ett centralt concept i varje krisledningssystem. Det är också i sig ett omfattande forskningsområde. Emellertid kommer detta problemområde endast att behandlas ur en mer teknisk/logisk synvinkel i detta arbete, eftersom det naturligt knyter an till den generella arkitektur problematiken, vilket framgår av avsnitt 3, del 2.

7. Tjänstekonceptet

I detta kapitel beskrivs för begreppet *tjänst* och därefter konceptet tjänsteallokering.

7.1 Tjänster

Begreppet tjänst har ingen entydig definition och används inom ett flertal områden med vitt skilda betydelser [29]. Tjänst kan avse; (1) en befattning med formaliserade arbetsuppgifter och kvalifikationskrav, (2) utövandet av ett arbete och (3) en handling som är till nytta för någon annan. Även inom områden som systemarkitektur, informationssystem och informationsteknologi används begreppet tjänst flitigt och har blivit något av ett modeord, där i princip allt skall vara tjänstebaserat, utan att någon entydig definition antagits. Begreppet IT-tjänster har lanserats som "the typical outcome of people's activities using IT tools according to the precisely defined process." [30]. e-Service anser tjänster som är tillgängliga via nätverk, vanligen Internet [31]. I många fall anses tjänst inom IT området vara en funktion som tillhandhålls till en specificerad kvalité och kostnad [30]. Inom telekommunikationsområdet ses tjänst som kapaciteten

att utbyta information som tillhandahålls kunder av tjänsteleverantörer [32]. Begreppet tjänstekvalité (eng. Quality of Service, QoS) är relevant inom detta område. Tjänstekvalité utgörs av ett specificerat antal egenskaper hos tjänsten som är observerbara och som konsumenter av tjänsten kan bedöma [33].

Arkitekturen Service Oriented Architecture (SOA) har till syfte att skapa lösa kopplingar mellan mjuvarukomponenter. Det finns en stark koppling mellan konceptet Web-services och SOA. En tjänst i SOA definieras som "a unit of work done by a service provider to achieve desired end results for a service consumer." [34].

Inom den svenska Försvarsmakten togs en generell definition av begreppet *tjänst* fram avsett att kunna användas för att möjliggöra integration av olika system [35]. Enlig denna definition är en tjänst en abstraktion av hur en producent kan åstadkomma nytta för en konsument, utan att beskriva hur detta genomförs. Nytta åstadkoms genom att producenten levererar en prestation och prestationen ger en effekt hos/för konsumenten. Tjänster skall beskrivas oberoende av om de implementeras manuellt, tekniskt, eller genom kombinationer av dessa. Definitionen beskriver enbart hur konsumenten gör för att få tillgång till tjänsten och vad som produceras. Dessa tjänster har egenskaper och med stöd av dessa egenskaper kan en konsument välja vilken realisering som fungerar bäst. Därmed utgör tjänsten en fasad mot producenten utifrån konsumentens perspektiv. Konsumenten behöver inte ha kännedom om vilka producenter som tillhandhåller olika tjänster, utan kan söka efter de tjänster som passar bäst. Tjänster kan vara synkron, då konsumenten erhåller direkt effekt av tjänsten. Men tjänster kan även vara asynkrona, så kallade prenumerationstjänster vilka beställs och där leverans sker fortlöpande tills dess att prenumerationen avbeställs. Stödtjänster är tjänster som inte används direkt av verksamheten utan är tjänster av generell karaktär vilka har till uppgift att internt stödja systemelement.

Ett sätt att realisera tjänstebaserade informationssystem är att basera dessa på så kallade Web-services. Web-services är ett relativt nytt begrepp som för tillfället är mycket omskrivet och som så smått börjar mogna och komma till praktisk användning. Web-services är en tjänste- och komponentorienterad ansats för att ge tillgång till funktionalitet och information. Dessa tjänster skall vara tillgängliga för användare och andra applikationer [36]. Centrala begrepp inom koncept Web-services förklaras nedan:

- Elementary services är web-services som ger åtkomst av Internet baserade applikationer, utan att nyttja andra web-services.
- Composite services är web-services som är sammansatta av elementary services och andra composite services.
- Service container är web-services som innehåller ett flertal liknande web-services. Den ger dynamik då tjänsteproducenten kan välja vilken tjänstrealisering som skall nyttjas för att möta kundernas behov.

Att använda sig av tjänstebaserade arkitekturer där funktionalitet och förmågor beskrivs i form av tjänster, ger flera fördelar. En och samma tjänst kan implementeras på flera olika sätt. Möjligheten att kombinera flera olika tjänster för att erhålla en helt ny tjänst ger hög anpassningsförmåga och återanvändbarhet.

7.2 Tjänsteallokering

Tjänster kommer på olika sätt och på olika nivåer att vara allokerade till olika aktörer och deras arbetsmiljöer. Vilka tjänster som kommer att vara allokerade är avhängigt aktörernas roller och deras aktuella uppgifter. Vissa tjänster kommer aktörerna att kunna allokera eller avallokera på ett självständigt sätt allt eftersom behoven växlar. Tjänster av denna typ kallas *användarallokerade tjänster*. Till användarnas förfogande kommer också att finnas tjänster som är *obligatoriska*. Med obligatoriska tjänster avses tjänster som alltid är tillgängliga. Förnärvarande antas att det kommer att behövas två olika obligatoriska tjänster, nämligen för konsistent lägesbild (avsnitt 9) och för applikationsdatabasen (avsnitt 11). De obligatoriska och de användarallokerade tjänsterna utgör tillsammans den flexibelt anpassningsbara arbetsmiljö som står till aktörerna förfogande.

Till varje användarallokerad tjänst är det möjligt att knyta olika tjänster, så kallade *tjänsteallokerade tjänster,* som förser de användarallokerad tjänsterna med relevant information. Detta kommer att i viss utsträckning ske automatiskt. En tjänsteallokerad tjänst kan t ex vara en sensor för insamling och analys av sensordata. För bland annat sensortjänster gäller att dessa kan variera över tiden eftersom alla sensorer inte är användbara vid alla tider på dygnet eller under alla väderförhållanden.

Tilläggas bör att det finnas tillämpningar där tjänster är användarallokerad men där samma tjänster vid ett senare tillfälle är tjänsteallokerad. Exempel på detta är tjänster för visualisering. Eftersom tjänster kan klassas på olika sätt kräver detta att systemet måste kunna hantera detta på ett adekvat sätt. Detta kommer att hanteras med hjälp av det ontologiska kunskapssystemet som beskrivs i avsnitt 10.

Systemallokerade tjänster utgör en klass av tjänster som användaren inte har någon kontroll över. Dessa tjänster kommer i viss mån att också vara obligatoriska men kommer endast att arbeta på systemnivå. Denna typ tjänster kan speciellt utnyttjas som stöd för informationssäkerhet och beskrivs i avsnitt 14. Den enda direkta kontakt som användare kommer att ha med dessa tjänster består i meddelanden som tjänsterna sänder ut till användare. Dessa meddelanden kan vara t ex varning för intrång i systemet och att användarena måste vidta någon speciell åtgärd. Till dessa tjänster kan också hänföras stöd för åtkomstkontroll av externa data vilket innefattar kryptering, dekryptering, autenticering och auktorisering.

Beslutsstöd betecknas som tjänster även om alla tjänster inte på mostvarande sätt kan betecknas som beslutsstöd. Exempel på tjänster som är av typen beslutsstöd är geografiskt informationssystem medan exempel tjänst som inte är ett beslutsstöd är kommunikationssystem och sensorsystem.

En betydelsefull aspekt på hur tjänster på lägre nivå allokeras till de aktörsallokerade tjänsterna berör förmågan till interoperabiltitet dvs förmågan till integration av redan existerande tjänster såsom t ex sensorer. Den systemlösning som valts för allokering av sådana tjänster, där en så kallad allokeringsbrygga används, medger att godtyckliga tjänsteallokerade tjänster kan integreras till systemet, se del 2 avsnitt 1.4. Lösningen på detta problem är baserad på ontologier och speciellt anpassade regelbaserade kunskapsbaserade system, se avsnitt 10.

8. Beslutsstöd

Beslutsstöd syftar till att stödja användare i deras beslutsfattande, och inte att automatiskt fatta några beslut åt användarna. Beslutsstöd kan vara av en mängd olika typer av informationssystem. De kan vara relativt enkel till mycket komplexa. De mer komplexa beslutsstöden utgör system bestående av delsystem av enklare beslutsstöd. Svårigheten med dessa delsystem är att de

på ett kraftfullt sätt måste kunna utväxla information mellan sig. I detta förslag sker detta genom att informationen mellanlagras i en applikationsdatabas, som diskuteras i avsnitt 11.

I detta arbete görs inget anspråk på att ta fram en fullständig lista på nödvändiga typer av beslutsstöd som behövs vid krishantering. I detta avseende syftar arbetet endast till att utveckla en modell som är tillräckligt flexibel för att i form av tjänster kunna allokera alla de beslutsstöd som kommer att behövas. Däremot är det möjligt att peka på ett antal beslutsstöd som med säkerhet kommer att behöva finnas tillgängliga. Till dessa hör system för

- behandling av geodata (t ex GIS),
- databrytning (data mining),
- frågespråk,
- riskbedömning.

Att utveckla nya beslutsstöd kan leda till svårigheter av varierande slag beroende på systemens omfattning. I de fall redan tillgängliga redskap existerar kommer problemet att bli att bygga upp de delsystem som skall koppa ihop de olika tjänstemodulerna. Detta gäller för övrigt generellt för de tjänster som skall kopplas till ledningssystemet dvs det är ett allmängiltiga problem som i vissa fall kan vara komplexa.

9. Konsistent lägesbild

Med konsistent lägesbild menas lägesbild som med avseende på aktuell information är alltigenom överensstämmande med övriga aktörers motsvarande lägesbild. Gemensam lägesbild är ett snarlikt begrepp, som dock, avser att precisera samma information, vilken är tillgänglig för samtliga aktörer och presenteras på samma sätt. Olika aktörer har med sina respektive aktörsperspektiv och arbetssituation olika behov av information, vilka medför behov av olika lägesbilder. Till exempel har en insatsledning behov av mera övergripande lägesbilder, medan aktörer i fält har behov av mera detaljerad information, men inte samma behov av övergripande information.

Aktörer tolkar lägesbildsinformation på olika sätt, på grund av olika bakgrund, kunskap och andra förutsättningar. Detta ställer naturligtvis krav på lägesbildsutformningen för att undvika felaktiga tolkningar.

Utmaningen ligger här i att både lyckas hantera olika lägesbildsbehov och samtidigt uppnå en konsistent lägesbild. Det ligger även en dynamik i lägesbildsbehoven. Aktörers behov förändras med ändringar i miljön, interaktion med andra aktörer och att en eskalerande krissituation tvingar aktörer att agera i andra roller än de ursprungligen hade. Med olika typer av visualiseringsteknik måste lägesbilden åskådliggöra krisers utveckling och stödja bedömningar av vad som är lämpliga val av åtgärder och även stödja prediktion av krisers vidare utveckling och terminering. Detta kräver att risker modelleras på ett adekvat sätt.

I krissituationers omfattande dynamik kan en bland flera kopplingar observeras till tidigare resonemang om situationsförståelse och dess underbegrepp illustrerade i figur 3. Exempelvis modellerades lägesbilden som indata till situationsförståelsen. I praktiken är det en växelverkan, där situationsförståelsen visserligen baserar sig på lägesbildsinformation, men samtidigt påverkar även situationsförståelsen hur krav till lägesbildsutformning vidareutvecklas.

Situationsförståelsen är en synnerligen kritisk faktor för att lyckas hantera en aktuell krissituation. Detta gäller såväl enskilda aktörer som grupper av aktörer, vilket medför att det är viktigt att åstadkomma en tillräcklig grad av situationsförståelse. Detta ställer ytterligare krav på utformningen av lägesbilden, särskild med avseende på behov av koordinering. Olika perspektiv på koordinering vid krishantering, fredsinsatser och humanitära insatser, bland annat i koalitionsform, lyfts fram och diskuteras närmare i [23], [22] och [25].

Riskmodellen och lägesbilden måste integreras på ett sådant sätt att riskbedömningen understöds av lägesbilden. Om till exempel riskmodellen beskriver risker i termer av aktiviteter, hotagenter, skyddsvärda objekt och skyddsvärda objekts kontext, så måste lägesbilden på motsvarande sätt åskådliggöra dessa termer och deras inbördes relationer.

10. Ontologier

En ontologi utgörs av en kunskapsstruktur som logiskt beskriver olika objekt, deras egenskaper och deras relationer. Ontologier är oftast hierarkiska till sin struktur. En egenskap av speciellt intresse är förmågan att egenskaper på lägre nivå i hierarkin kan ärva egenskaper från högre nivå. Emellertid, en ontologi är inte enskilt användbar, den måste vara inplacerad i ett kunskapssammanhang. Oftast brukar ontologierna användas som underliggande struktur i kunskapsbaserade system. Detta gör det möjligt att använda ontologierna i olika tillämpningar tillsammans med frågesystem av olika slag.

I den ledningssystemmodell som utvecklats för krishantering kan ontologier utnyttjas i en mängd olika sammanhang och på olika nivåer i systemet och för specifika uppgifter. Av denna anledning finns det inte skäl att utveckla någon enskild ontologi utan det är möjligt att i detta sammanhang tala om multipla ontologier som kan vara distribuerade. Genom att distribuera dessa ontologier är det möjligt att dedicera dem till olika tjänster. Det är också möjligt att utnyttja dem för att knyta samman användarallokerade tjänster med tjänsteallokerade tjänster på ett effektivt och funktionellt sätt. Samma teknik har använts vid FOI för att allokera sensorer till ett frågespråk för data från multipla sensorer [37], [38]. Skillnade är att i ledningssystem modellen som diskuteras här kommer tekniken att generaliseras och explicit vara en del av den brygga som skall sammanbinda de olika tjänsterna. Denna teknik kommer att beskrivas ytterligare i del 2 av denna rapport.

Arbetet med att utveckla olika ontologier är i sig inte speciellt komplicerat. Däremot kommer det att krävas större arbetsinsatser för att få de ontologiska kunskapssystemen att fungera på ett tillfredsställande sätt.

11. Applikationsdatabas

Applikationsdatabasen som utgör en obligatorisk tjänst har till syfte att medge mellanlagring av all den information som en aktör har behov av och som denne samlar in för att kunna lösa alla sina arbetsuppgifter under den pågående krisen. Den lagrade informationen skall kunna användas både vids preventiva och operativa situationer. Den information som samlas in kommer dessutom att kunna användas efter krisen för analyser och diskussioner för att bedöma om genomförda aktiviter varit lämpliga och blivit korrekta utförda. Detta för att öka kompetensen hos

involverade aktörer, se också avsnitt 15 där träning och uppföljning diskuteras. En inte mindre central användning av applikationsdatabasen utgör uppgiften att leverera den information som behövs för presentation av en konsistent och relevant lägesbild. Lägesbilden finns diskuterad i avsnitt 9.

Problem som hänför sig till applikationsdatabasen och dess funtionalitet och som behöver penetreras ytterligare utgör behovet av att utveckla sökfunktioner för den information som behövs. Dessa sökfunktioner relaterar sig till de lagringsstrukturer som behövs för att göra applikationsdata tillgänglig. I vissa sammanhang kan de aktuella datavolymerna som skall lagras komma att bli mycket stora, vilket komplicerar problematiken ytterligare. Till detta kommer att kopplingen till lägesbilden också måste vara enkel.

12. Informationsinsamling

Informationsinsamling skall huvudsakligen kunna ske enligt följande två huvudprinciper:

- Produktion, prenumeration samt selektiv insamling av information genom frågor till applikationsdatabasen.
- Allokering av tjänster i form av olika datakällor, t ex sensorer, där relevant information inhämtas via frågor ställda direkt till datakällorna.

Dessa båda ansatser är relativt likartade. Skillnaden består väsentligen i att det första alternativet kommer att skicka information som inte till alla delar kommer att vara relevant. Detta kommer att kräva lagring av data som kanske inte kommer att behövas. I det andra fallet kommer bara efterfrågad information att skickas. I båda fallen kommer data att behöva fusioneras [39], dvs data som i stort beskriver samma information kommer att behöva integreras så att den kombinerade informationen som härigenom görs tillgänglig beskriver verkligheten på ett mer tillförlitligt sätt. Fusionen kan utföras som en internprocess i frågespråket [37], vilket har visat sig möjligt i försök som utförts vid FOI. Dessa experiment har genomförts med frågespråket ΣQL [40] och är speciellt utvecklat för att arbeta mot multipla heterogena sensordatakällor.

I moderna informationssystem, som speciellt skall behandla bildinformation från olika typer av sensorer, är det speciellt viktigt att inte bara bildinformationen finns tillgänglig utan även att

kontextuell information [41] om dessa bilder samlats in. Med kontextuell information avses sådan information som beskriver innehållet i bilden samt bland annat information om var och när bilden är tagen. Syftet med att samla in sådan kontextuell information är att förse informationssystemet, som kan vara ett ledningssystem, med metadata som kan användas för att förse en användare med ett bättre beslutsunderlag.

Forskningsproblem i anslutning till informationsinsamling berör till stora delar krav på utveckling av metoder för analys av sensordata, utveckling av metoder för sensordatafusion samt tekniker för allokering av olika typer av sensortjänster till frågespråket. Sådana tjänster kan variera med avseende på olika dynamiska händelseförlopp, men också med avseende på aspekter såsom ljusförhållanden, väderlek samt även tid och rum.

13. Nätverkskommunikation

Möjligheten att kommunicera är mycket central vid ledning. Om kommunikationsförmågan kraftigt begränsas eller helt förloras så förloras även förmågan att på distans överblicka och leda insatser. Kommunikationsnätet utgör infrastrukturer för att överföra information mellan olika enheter. Det finns i huvudsak två typer av kommunikationsnät, fasta och mobila. Båda typerna är av intresse från aspekten distribuerade ledning vid krishantering, efter som de erbjuder olika typer av funktionalitet. Utvecklingen av det mobila nätets kapacitet ökar dock ständigt, där dessa i allt högre utsträckning kan ersätta den funktionalitet som tidigare enbart kunde erhållas med fasta kommunikationsnätet. Dessutom förutsätter ledning av enheter ute på fältet, vid olycksplatser och inom riskområden tillgång till trådlösa kommunikationsnät eftersom mobilitet är av stor vikt i dessa situationer. Kommunikationsnät måste, förutom att tillhandahålla kapacitet för informationsöverföring, ha hög grad av tillgänglighet, tålighet samt säkerhet.

Eftersträvansvärt är att lyckas skapa så kallad sömlös kommunikation, vilket medför att användarna trots förändringar i näten har möjlighet att kommunicera oavsett vilken terminal de använder, vilket delnät de har tillgång till och vilken enhet de tillhör. Sömlös kommunikation är en framtidsvision som tros kunna lösas genom att få samtliga system att använda samma protokoll.

Protokoll är en uppsättning regler som styr format och syfte hos informationsenheter eller meddelanden som utbytes mellan lager på samma nivå men på en annan enhet. Protokollen används för att specificera och definierade tjänster. Det mest kända protokoll som används för kommunikation på Internet är TCP/IP (Transmission Control Protocol/Internet Protocol).

De system som byggts för att möjliggöra kommunikation mellan olika enheter består av så väl mjukvara som hårdvara. När det gäller mjukvarudelen används normalt en indelning i olika lager. Antalet lager och deras funktionalitet varierar från system till system. I alla system är däremot syftet hos lagren att utföra en tjänst åt ovanliggande lager. Därigenom kan man gömma för ovanstående lager hur en tjänst är implementerad. Denna princip används även här för de tjänsteallokerade tjänsterna dvs med hjälp av allokeringsbryggor, se avsnitt 2.3 del 2, styrda av ontologier, se avsnitt 2.5 del 2. Varje lager kommunicerar enligt bestämda regler med motsvarande lager hos andra enheter. En tjänst i detta sammanhang är en mängd operationer som ett lager erbjuder till lagret ovanför och nyttjar från lagret under. Därmed definieras tjänster inom området för nätverkskommunikation som de operationer som ett lager kan utföra åt sina användare. Tjänsterna beskriver inte hur de är implementerade. Gränssnittet mellan två lager kan ses som en tjänsteförmedlare och därmed blir det undre lagret en tjänsteproducent och det övre en tjänsteanvändare.

14. Informationssäkerhet

Under rubriken ”IT har nyckelroll i EU:s terrorkamp” diskuterades i en artikel i Ny Teknik [26] gemensamma europeiska databaser för ökad personkontroll, som ett led i bekämpningen av grov organiserad och gränsöverskridande brottslighet. Hur vi alla lämnar digitala spår efter oss i olika register vid handlande hos ICA-handlaren, vid användande av mobiltelefon etc, skisseras i [27]. Olika aktörer, från ICA-handlaren till polisen, kan vara intresserade av att följa och studera dessa spår. Frågor rörande personlig integritet är av vikt i sammanhanget, men måste vägas mot mål för verksamheten i vilken registreringen sker. Det måste även beaktas att insamlad information kan komma att användas i andra sammanhang än vad som första avsågs. Om exempelvis terrorbekämpning är målet, i vilken mån är det lämpligt att ta hänsyn till personlig integritet väger mindre tungt? Vilka verksamheter och aktörer bör, respektive bör inte, ha tillgång till denna typ av information? Vidare, vilka aktörer bör ha möjligheter att föra in registreringar i databaser respektive, ändra i redan existerande registreringar?

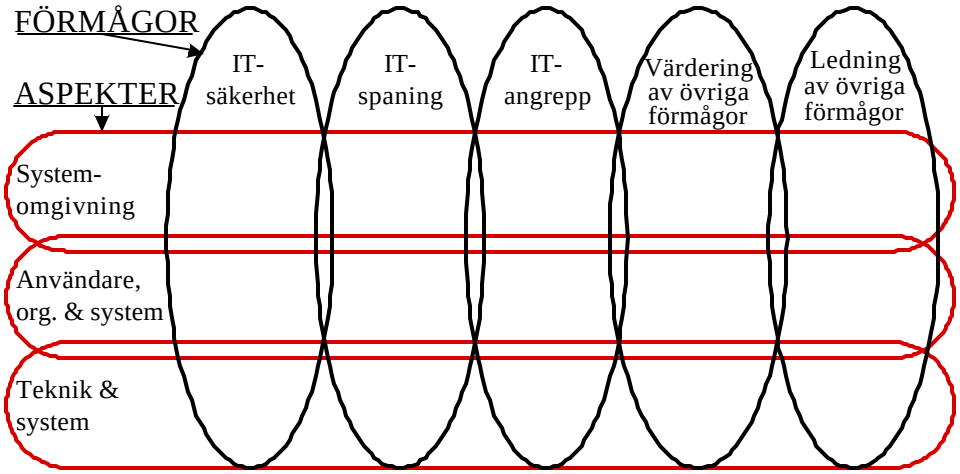
Utöver frågor rörande personlig integritet har vi härmed snabbt kommit över i frågor rörande sekretess, tillförlitlighet och tillgänglighet, vilka är de centrala problemområdena som informations- och IT-säkerheten normalt delas upp i. Informationssäkerhet avser information i alla dess former, medan IT-säkerhet endast avser information som hanteras av informationssystem (elektronisk information). Informations- och IT-säkerhetens centrala betydelse för lednings- och skyddsfunktioner diskuterades i förstudien [3]. Denna förstudie påpekade också behovet av att beakta frågor rörande driftssäkerhet[1], med andra ord säkerhetsfunktionalitet som normalt sett inte diskuteras i termer av informations- och IT-säkerhet. Fokus i detta avsnitt är dock på informations- och IT-säkerhet.

De ovan snabbt skisserade frågorna rörande digitala spår och terrorbekämpning torde, med mindre justeringar, även vara aktuella rörande informations- och IT-säkerhet i andra krissituationer, som till exempel vid naturkatastrofer eller olyckor vid transport av farligt gods.

För att identifiera tjänster för informations- och IT-säkerhet i sådana sammanhang är det nödvändigt att komma vidare från säkerhetsgrundbegreppen sekretess, tillförlitlighet och tillgänglighet för att sätta dessa in i ett sammanhang. Sammanhanget beskriver vad som i aktuell typ av situation är i behov av att skyddas, vilka händelser som kan tänkas vara viktiga att upptäcka i omgivningen och hur reaktionen bör vara på dessa händelser. På liknande sätt, som tidigare har påpekats om nödvändigheten av att integrera riskmodellen och lägesbilden för bästa möjliga riskbedömning, är det också kritiskt att informations- och IT-säkerhetstjänster är väl integrerade med såväl riskmodellen som lägesbilden. Därigenom kan de tjänster som behövs och som ger bästa möjliga effekt identifieras i enlighet med riskmodellens analys. Detta måste åskådliggöras i lägesbilden för att slutligen ge olika aktörer en högkvalitativ säkerhets- och situationsförståelse för vidare analys, beslut och agerande.

1. I engelskspråklig litteratur används oftast termen *safety*.

:



Figur 8. Aspekter och förmågor rörande IT-försvar/skydd.

Säkerhet är, som observerad i [29] generellt mera av en egenskap än en funktion. Likaså observeras att bra säkerhet inte märks, den är transparent för användaren. Det är närmast tjänster som märks först när de fallerar eller medför extraarbete. För säkerhetsansvariga existerar dock andra behov av mera explicit tillgängliga säkerhetstjänster (säkerhetsfunktioner).

För att hitta passande informations- och IT-säkerhetstjänster föreslår [29] att dessa kan kategoriseras med hjälp av struktur i figur 8, som lyfter fram olika aspekter och förmågor rörande IT-försvar/skydd i vid mening.

En första grov indelning av tjänster, som torde behövas, redovisas av följande lista baserad på diskussion i [29][1]:

- Kommunikationssäkerhet

- Systemsäkerhet

* Identifiering och autenticering

* Åtkomstkontroll och auktorisering

1. Ytterligare referenser framgår av diskussionen i [29].

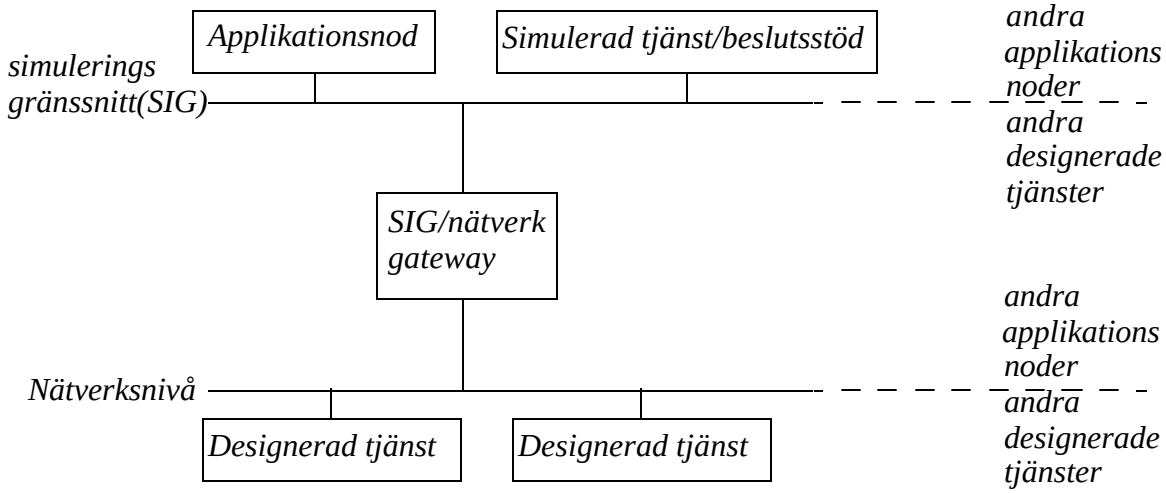
* Loggning

* Säker lagring

En närmare studie av vilka mera detaljerad specificerade tjänster som i krishantering behövs kan förslagsvis byggas upp med hjälp av distribuerade ontologier och den kunskapsrepresentation dessa stödjer. Dock bör dock noteras att säkerhetens natur av att mera vara en egenskap än en funktion/tjänst sannolikt gör identifierandet av lämpliga tjänster mera komplext.

15. Datakällor

Datakällorna som ingår i denna typ av ledningssystem utgörs främst av olika typer sensorer. Sensorer som förekommer kan vara av många olika slag. Vilka typer som kommer att vara aktuella beror på de tillämpningar som kommer att bli aktuella. För t ex olika typer av övervakningssituationer där människor kommer att vara i fokus kommer antagligen videokameror att vara speciellt användbara. För övervakning av trafiken vid hamnar och flygplatser kommer olika typer av sensornätverk att vara lämpliga. I framtida system kommer med säkerhet mobiltelefoner med högupplösande digitalkameror att vara användbara. I flera av dessa fall kommer dessa sensorer att kunna användas för såväl preventiva som för operativa aktiviteter.



Figur 9. En applikationsnod på nätverksnivå för simulering och för verklig drift av ledningssystemet.

Det måste också vara möjligt att använda även andra källor för datainsamling än sensorer. Bland annat måste det också vara möjligt att utnyttja skrivna och talade rapporter. Även indata från

andra modaliteter kan tänkas förekomma. Skillnaden mellan dessa typer av indata och indata från sensorer är väsentligen beroende av aktuella dataanalysmetoder.

Problem relaterade till olika förekommande datakällor beror väsentligen på t ex vilka sensorer som skall användas i de olika sammanhangen för att ge bästa möjliga information till de olika beslutsfattarna. Dessa problem måste behandlas enskilt för olika typer av tillämpningar.

16. Simulering

Krav på möjlighet att kunna simulera situationer som ger upphov till användning av ledningssystemet, grundar sig på behoven av att träna personal som kommer att vara engagerade i lösandet av olika kriser. Vidare föreligger också behov av att kunna analysera vad som hände under en given kris som kan vara antingen verklig eller simulerad. Av denna anledning kommer någon form av stöd för uppföljning att behöva utvecklas. Emellertid finns metoder och tekniker som är utvecklade för att kunna genomföra sådan verksamhet [42]. Vad avser metodik för simulering finns metoder och system utvecklade också för detta ändamål. Båda dessa tekniker kommer att kunna integreras på ett effektivt sätt i det ledningssystem som diskuteras här, även om i nuläget ingen av dessa utgör någon primär uppgift som skall belysas i detta sammanhang. Speciella lösningar för att överbrygga mellan en verklig nätverksbaserad miljö och en simulerad miljö kommer att behöva utvecklas. En lösning till detta problem framgår av figur 9. Av figuren framgår att i den nedre delen kan tjänster för verklig drift kopplas medan tjänster som skall simuleras kopplas till den övredelen som utgörs av simuleringsramverket. Mellan dessa båda nivåer kommer det att finnas en brygga som kopplar samman nätverk och simuleringsramverk för att göra det möjligt att bestämma vilken nivå som skall användas i ett visst sammanhang. Slutligen kan användare kopplas till vilken som helst av de båda angivna nivåerna genom att ansluta användarens applikationsnod. Genom denna lösning kommer det att vara möjligt att köra både renodlade simuleringar såväl som renodlade verkliga situationer samt även situationer som utgör kombinationer av dessa båda fall.

17. Agentbaserad systemlösning

Den typ av ledningssystem som diskuteras här kommer till sin inre struktur att vara komplex, vilket kommer att ställa speciella krav på den implementationsteknik som kommer att användas. Generellt gäller att om konventionella programmeringsmetoder används leder detta till att sys-

temet kommer att uppnå en sådan komplexitetsgrad att underhållskostnaderna för systemet kommer att bli enorma. Poängteras bör att normalt ligger underhållskostnaderna för programvarusystem på ungefär 60% av systemets totala kostnader, beräknat på dess livslängd. Av denna anledning är det angeläget att minimera inte bara utvecklingskostnader utan speciellt också underhållskostnader. Detta kan göras genom att välja systemlösningar som kan minska komplexiteten i systemet. En sådan ansats kan vara att utnyttja multipla intelligenta agenter [47]. Agenter i detta sammanhang utgörs av programvaruobjekt med viss autonomitet. Dessa kan skapas och avföras ur systemet allt efter behov och de är också mobila och kan därför röra sig i systemet enligt något på förhand bestämt mönster. Genom sin autonomitet blir det också möjligt för dem att kommunicera och förhandla med andra agenter. Eftersom agenterna kommer att utgöras av ett tämligen begränsat antal typer, där var och en har sina begränsade arbetsuppgifter kommer detta att leda till att kodningsarbetet för att beskriva deras förmågor och arbetsuppgifter blir relativt begränsat. Konsekvensen av detta är att man kan begränsa underhålls- och utvecklingskostnaderna med denna typ av systemlösning.

Referenser

[1] KBM (2003) Krishanteringssystemet, http://www.krisberedskapsmyndigheten.se/verksamhet/kommunal/kommunpaketet/krishanteringssystemet.pdf(2003-01-19).

[2] Rechtin, E. (1999) System architecting of organizations: Why Eagles can’t swim. CRC Press.

[3] Jungert, E., Derefelt, G., Hallberg, J., Hallberg, N., Hunstad, A., Thurén, R. et al., *Förstudie avseende förslag till integrerad lednings- och skyddsfunktion för preventiv och operativ krishantering*, FOI-rapport FOI-R--1183--SE, Februari 2004.

[4] Jungert, E., Derefelt, G., Hallberg, J., Hallberg, N., Hunstad, A., & Thurén, R. *Architecture-based Model for Preventive and Operative Crisis Management*, proceedings of the NATO SCI-158 symposium on Systems, Concepts and Integration Methods and Technologies for Defense against Terrorism , London, October 25-27, 2004.

[5] Worm, A. On Control and Interaction in Complex Distributed Systems and Environ ments, Linkoping Studies in Science and Technology, Dissertation No. 664, Linkoping University, Linkoping, Sweden, 2000.

[6] eNavet, http://www.linkoping.se/Organisation/Klk/Sakerhet/Navet/ProjektetNavet.htm, (2004-12-16).

[7] GOTSAM, http://www.gotsam.se/servlet/GetDoc?meta_id=1001, (2004-12-16).

[8] CeSam-C, http://www.c.lst.se/templates/KisPage.aspx?id=171, (2004-12-16).

[9] CeSam-C, http://www.c.lst.se/templates/newsPage.aspx?id=799, (2004-12-16).

[10] LUCRAM, http://www.lucram.lu.se.

[11] Abrahamsson, M. & Magnusson, S.E. Risk- och sårbarhetsanalyser Utgångspunkter för fortsatt arbete, KBM:s forskningsserie nr 2, Krisberedskapsmyndigheten 2004.

[12] Enander, A. & Hede, S. Förväntningar och erfarenheter hos aktörer Delrapport 1 från projektet Beredskap och krishantering isvenska kommuner, KBM:s forskningsserie nr 4, Krisberedskapsmyndigheten 2004.

[13] Lajksjö, Ö., Enander, A., & Hede, S. Drivkrafter för arbete med säkerhets- och beredskapsfrågor. Delrapport 2 från projektet Beredskap och krishantering i svenska kommuner, KBM:s forskningsserie nr 1, Krisberedskapsmyndigheten 2004.

[14] Enander, A., Hede, S., Lajksjö, Ö., Att stå i ”stormens öga” Delrapport 3 från projektet Beredskap och krishantering isvenska kommuner, KBM:s forskningsserie nr 1, Krisberedskapsmyndigheten 2004.

[15] Persson, P.-A., Towards an Understanding of the Service-Based Command System, In Proceedings of the 9th ICCRTS Command and Control Research and Technology Symposium, Monterey, California, USA, 2004.

[16] Research for a Secure Europe Report of the Group of Personalities in the field of Security Research, http://europa.eu.int/comm./research/security/.

[17] http://www.dhs.gov/dhspublic/theme_home2.jsp.

[18] Stanton, N.A., Chambers, P.R.G., Piggott, J., Situational awareness and safety, Safety Science 39, 2001, pp. 189-204.

[19] Oomes, A.H.J., Organizational awareness in crisis management, Proceedings ISCRAM2004, Brussels, May 3-4 2004.

[20] Burghardt, P., Combined Systems The Combined Systemns Point of View, Proceedings ISCRAM2004, Brussels, May 3-4 2004.

[21] Storms, P.P.A., Combined Systems A System of Systems Architecture, Proceedings ISCRAM2004, Brussels, May 3-4 2004.

[22] Levchuk, G.M., Yu, F., Levchuk, Y., Pattipati, K.R. *Networks of Decision-Making and Communicating Agents: A new Mothodology for Design and Evaluation of Organizational Strategies and Heterarchical Structures*, Proceedings of the ninth International Command and Control Research and Technological Symposium (ICCRTS), Copenhagen, Denmark, September 14-16, 2004.

[23] Shen, S.Y. and Shaw, M.J. *Managing Coordination in Emergency Response Systems with Information Technologies*, Proceedings of the tenth American Conference on Information Systems, New York, New York, August 2004, pp 2110-2120.

[24] Malone, T. W., Crowston, K., *The interdisciplinary Study of Coodination*, ACM Computing Survey, Vol 26, No 1, March 1994, pp 87-119.

[25] Pechoucek, M. Marik, V., Bárta, J., *A knowledge-Based Approach to Coalition Formation*, IEEE Intelligent Systems, May/June, 2002, pp 17-25.

[26] Kleja, M., *IT har nyckelroll i EUs terrorkamp*, Ny Teknik nr. 50, 8 december 2004.

[27] Andersson, S., *Många vill följa dina digitala spår*, Ny Teknik nr.24, 9 juni 2004.

[28] Marmelstein, R. E., *Force Templates: A blueprint for Coalition Interaction within an Infosphere*, IEEE Intelligent Systems, May/June, 2002, pp 36-41.

[29] Stenumgaard, P., Wenngren G., Tullberg H., Nilsson J., Grönkvist J., Cronström P., Lindström J., Hallberg J., Hallberg N., Grahn P., Andersson R. Tjänstebegreppets användning inom olika tillämpningsområden. Usage of the term "Tjänst" (Service) in different areas of application. Linköping, FOI 2004, (FOI-R--1211--SE).

[30] Rodosek, G.D. (2003)_A generic model for IT services and service management. IFIP/ IEEE Eighth International Symposium on Integrated Network Management, pp171 – 184.

[31] Rust, RT., & Kannan, PK. (2003) E-service: A new paradigm for business in the electronic environment. Communications of ACM June vol 46, issue 6.

[32] Gozdecki, J., Jajszczyk, A., & Stankiewicz, R. (2003) Quality of service terminology in IP networks. Communications Magazine, IEEE, vol 41,issue 3, pp 153 – 159.

[33] Lekkas, D.(2003) Establishing and managing trust within the public key infrastructure, Computer Communications vol 26, issue 16, pp 1815-1825.

[34] He, H. (2003) What is Service-Oriented Architecture? http://www.xml.com/pub/a/ws/ 2003/09/30/soa.html (2004-01-27).

[35] Jönsson, PG (2003) FMA AR Tjänstekonceptet M5, ver. 2.1, Funktion 09100:54976/02, FMV.

[36] Hu, J., & Grefen, P. (2003) Conceptual framework and architecture for service mediating workflow management, Information and Software Technology, vol 45, issue 13, pp 929-939.

[37] Horney, T., Jungert, E., Folkesson, M., *An Ontology Controlled Data Fusion Process for Query Language,* Proceedings of the International Conference on Information Fusion 2003 (Fusion'03), Cairns, Australia, July 8-11.

[38] Chang, S.-K., Costagliola, G., & Jungert, E. *Multi-sensor Information Fusion by query Refinement*, Recent Advances in Visual information Systems, Lecture Notes in Computer Science, 2314, Springer Verlag, 2002, pp 1-11.

[39] Hall, D.L., & Llinas, J. (Eds.)., *Handbook of Multisensor Data Fusion*, CRC Press, New York, 2001.

[40] Chang, S.-K., Costagliola, G., Jungert, E. and Orciuoli, F., *Querying Distributed Multimedia Databases and Data Sources for Sensor Data Fusion,* accepted for publication in the journal of IEEE transaction on Multimedia.

[41] Davis, M., King, S., Good, N., Sarvas, R., *From Context to Content: Leveraging Context to infer Multi Metadata*, Proceedings of the Multi Media conference (MM'04), New York, N.Y., October 10-16, 2004.

[42] Morin, M., Jenvald, J., & Thorstensson, M. (red.), *Utvecklingsmetoder för samhällsförsvar*, FOI, användarrapport, FOI-R--1064--SE, November 2003.

[43] Farkas, C. & Huhns, M. N. (2002) Making Agent Secure on the Semantic Web, *IEEE Internet Computing*, 6, 6, 76-79.

[44] Bengtsson, A., Hunstad, A., & Westerdahl, L. *Autonomitet i nätverksbaserade system*, FOI användarrapport, FOI-R—0695—SE, november 2002.

[45] Bengtsson, A. *Spårning vid samverkande Web Services*, FOI användarrapport, FOI-R--1399--SE, november 2004.

[46] Kagal, L., Finin, T., Paolucci, M., Srinivasan, N., Syacara, K., & Denker, G. (2004) Authorizationand Privacy for Semantic Web Services, *IEEE Intelligent Systems*, 19, 4, 50-56.

[47] Gerhard Weiss (ed.) *Multiagent Systems - A Modern Approach to Distributed Artificial Intelligence*, The MIT Press, Camebridge, Mass., 2000.

[48] Gollman, D., *Computer Scurity*, John Wiley & sons, New York, N. Y., 1999.

Del 2

Förslag till modellbaserad systemarkitektur

1. Inledning

I denna del av rapporten kommer grundprinciperna (ledningsmodellen, riskmodellen och informationssäkerhetsfrågorna) för ledningsarkitekturen att presenteras ur ett mer tekniknära perspektiv. Fokus kommer såsom redan framgått av del 1 att vara inriktat mot tjänstestrukturen och den nätverksbaserade hanteringen för att ge stöd för ledning med hjälp av bl a olika tjänstebaserade beslutsstöd. Av central betydelse är det stöd för riskhantering som också måste finnas. Avslutningsvis presenteras principerna för informationssäkerhet.

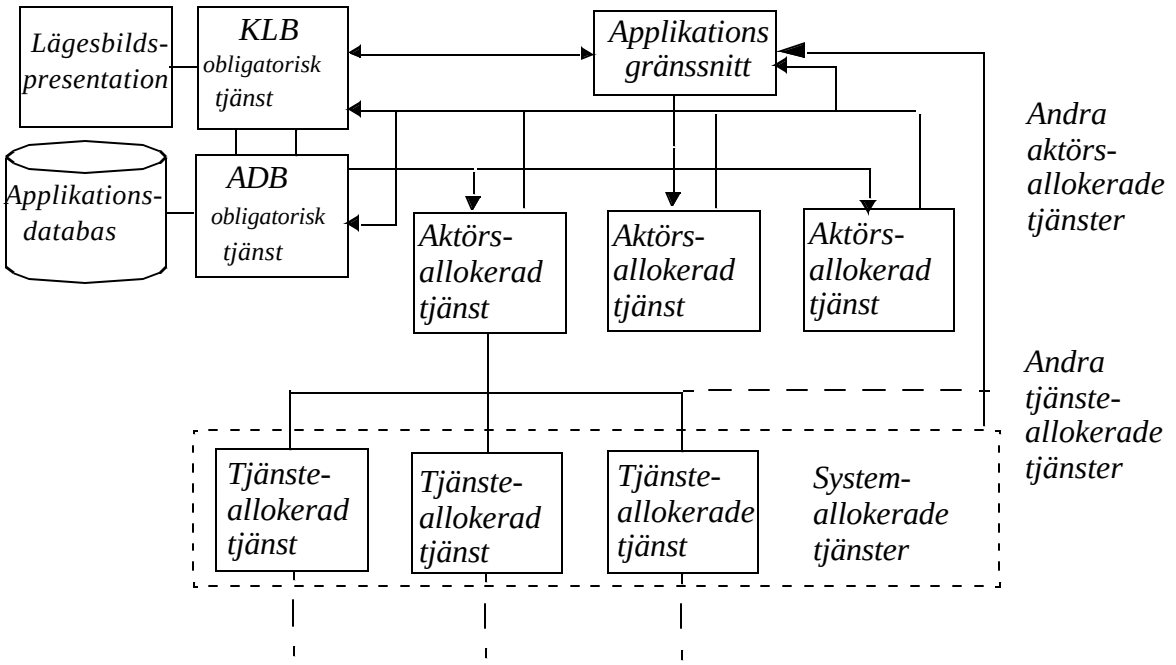
2. Ledningsmodellen

Detta kapitel är inriktat mot aktörsapplikationernas inre struktur samt deras användning som i praktiken styrs av de olika ontologierna och deras kunskapssystem. Generellt sett kan en aktörsapplikation definieras som en användarnod i ledningssystemets användar- och informationsnätverk. Varje sådan nod skapas efter de behov som en enskild aktör har med avseende på de tjänster som behöver knytas till applikationen. En sådan nod måste också omfatta en hög grad av flexibilitet och måste därför kunna förändras i takt med att behoven förändras, dvs med avseende på hur behoven av olika tjänster förändras över tiden. En del centrala delar kommer emellertid alltid att behövas; till dessa kan hänföras den konsistenta lägesbilden och aktörsdatabasen. Lägesbild och aktörsdatabas definieras som två obligatoriska tjänster. Till dessa kommer också systemallokerade tjänster, främst för informationssäkerhet att vara knutna.

Hur metodiken för hur tjänster allokerar andra tjänster är av speciellt intresse och ett inte helt trivialt problem. Lösningen på detta problem som föreslås är att låta ledningsarkitekturen bestå av olika bryggor, så kallade allokeringsbryggor, vilka vidare omfattar speciella ontologier och deras kunskapsbaserade system, som kommer att diskuteras i avsnitt 2.3 nedan. Dessa allokeringsbryggor utgör den centrala mekanismen för att åstadkomma interoperabilitet mellan tjänster.

Av central betydelse är de olika ontologier som måste finnas tillgängliga i systemet. Dessa har olika syften och är knutna till olika delar av systemet. Av denna anledning kallas dessa distribuerade ontologier och ontologiska kunskapssystem

.

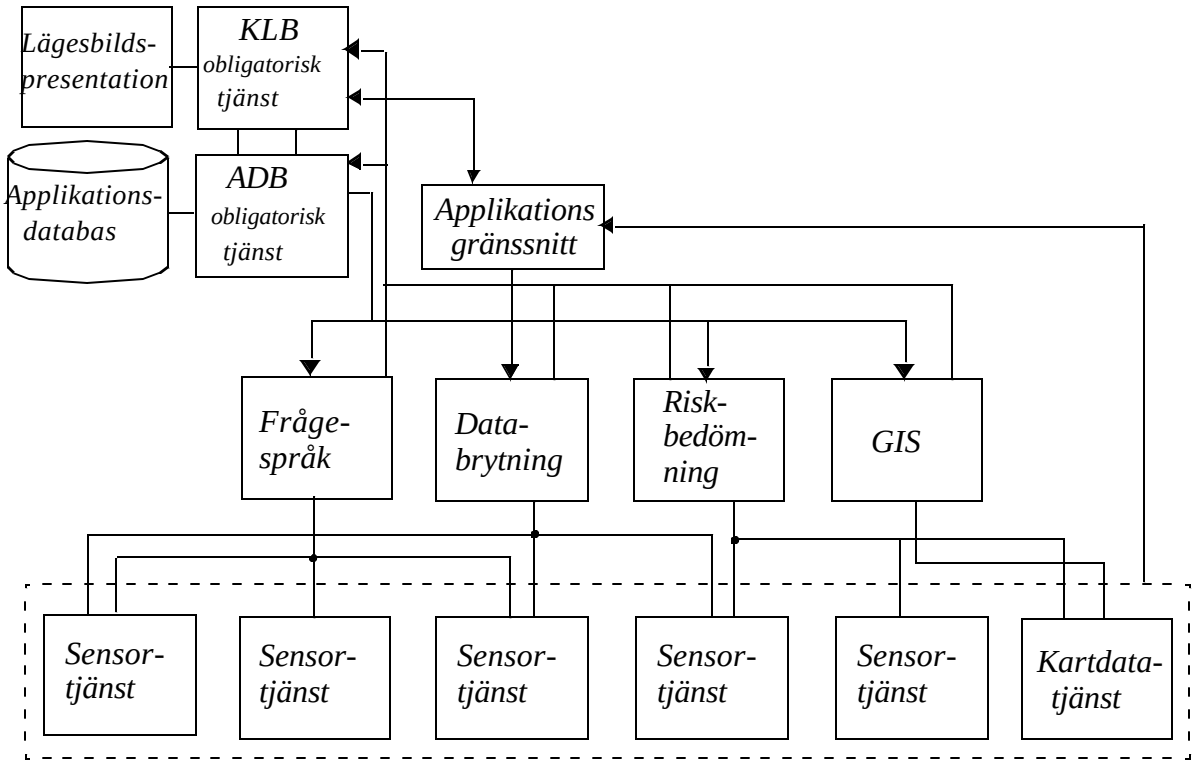


Figur 1. Aktörsapplikation/tjänstestruktur omfattande ett antal aktörsallokerade tjänster (AAT) med ett antal tjänsteallokerade tjänster (TAT) samt två obligatoriska tjänster.

2.1 Aktörsapplikationer

Aktörsapplikationer definieras som användarnoder i ett nätverk. Till dessa kommer att finnas användargränssnitt genom vilket användare (aktörer) interagerar med systemet. Användare kommer att ha en applikationsgenerator till sitt förfogande genom vilken de kan allokera de aktörstjänster som kommer att vara nödvändiga för att utföra de arbetsuppgifter som aktörerna har blivit ålagd. Arbetsuppgifterna kan vara antingen att genomföra preventiva åtgärder eller operativa insatser. I det första fallet är uppgiften att förhindra eller åtminstone minska riskerna för att krissituationer uppstår. I det senare fallet är uppgiften att bidra till att kriser slutförs. Mot denna bakgrund identifieras en tjänsteorienterad ledningsstruktur med vars hjälp de aktuella arbetsuppgifterna kan lösas (figur 1). Genom applikationsgränssnitt finns ett antal *aktörsallokerade tjänster* (AAT) tillgängliga, vilka aktören kan utnyttja för att lösa sina arbetsuppgifter. Till de flesta av dessa AAT finns en eller flera *tjänsteallokerade tjänster* (TAT) knutna på lägre nivå i strukturen. Dessa TAT:er kan vara distribuerade över nätet och av denna anledning måste de skyddas mot intrång och otillåten användning, vilket sker med hjälp av så kallade *systemallokerade tjänsterna* (SyAT). Eftersom allokering av de TAT i de flesta fall kommer att ske auto-

matiskt måste stöd för detta finnas. Detta, vilket inte är ett trivialt problem, diskuteras vidare i avsnitt 1.4 av del 2 och berör principerna för allokeringsbryggor. Undantag från den automatiska allokeringen av TAT måste naturligtvis tillåtas. Detta gäller speciellt i de fall då t ex aktörer begär att få allokera en speciell databas eller datakälla till sin aktörstjänst. Till aktörsapplikationerna hör också stöd för lägesbild samt en applikationsdatabas vilka båda är av obligatorisk typ och som således inte behöver allokeras. Figur 2 illustrerar en aktörsapplikation. I detta exempel finns fyra olika AAT, nämligen för frågespråk, databrytning, riskbedömning och GIS. Till frågespråket och databrytningssystemet finns tre underordnade sensortjänster, medan till riskbedömningstjänsten finns förutom två olika sensortjänster också en kartdatabas knuten. Kartdatabasen är, naturligt nog, även knuten till GIS-tjänsten. Med KLB avses konsistent lägesbild och med ADB avses ett system för hantering av applikationsdatabasen.



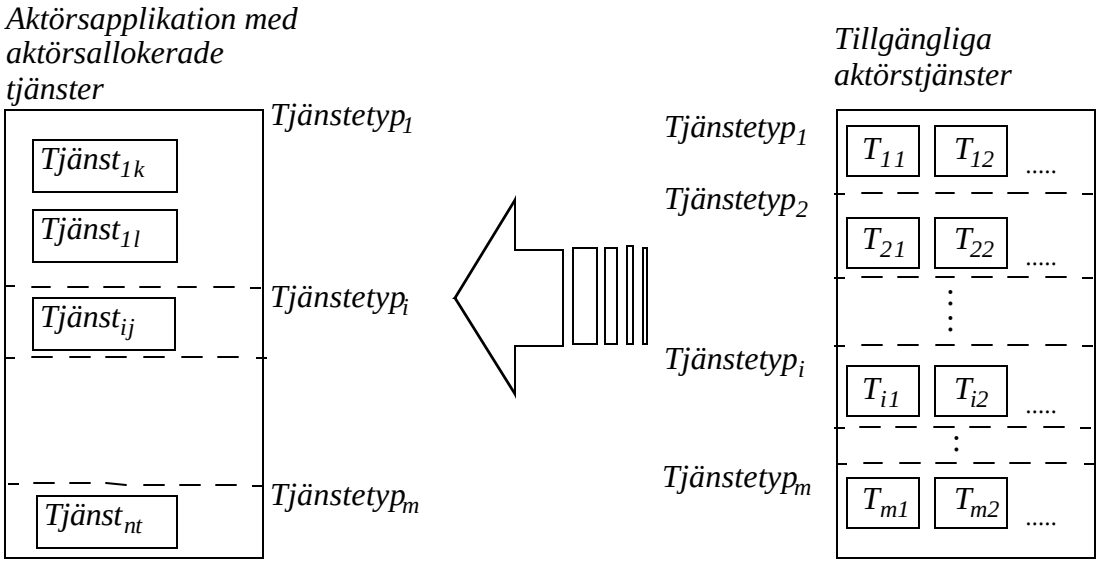
Figur 2. En illustration av en aktörsapplikation.

2.2 Generering av aktörsapplikationer

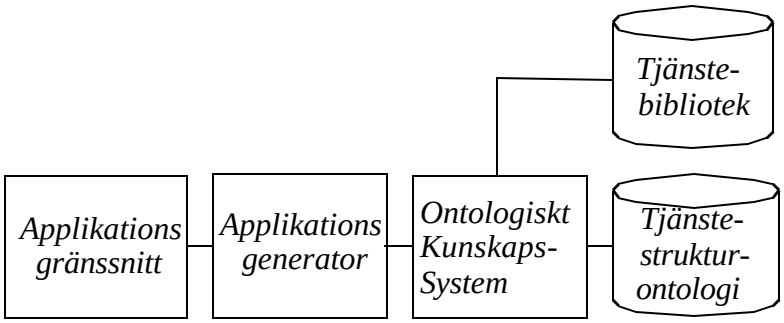
Generering av aktösapplikationer skall ske interaktivt med stöd av ett interaktivt system som utgör en obligatorisk tjänst till vilken i princip alla tillgängliga aktörstjänster finns knutna i enlig-

het med ontologin. I huvudsak skall genereringsprocessen ske med enkla visuella kommandon där aktörer väljer lämpliga tjänster från en meny och flyttar över dessa till sitt arbetsfält (figur 3). Flera tjänstetyper av samma slag är tillåtna varigenom det blir möjligt för aktörerna att välja den tjänst som lämpar sig bäst för ett givet läge eller som aktörerna känner sig mest bekväm med. Applikationsgeneratorn kan betraktas på flera olika sätt. Ett möjligt betraktelsesätt är att se den som en obligatorisk tjänst. Av figur 4 framgår att det förutom ett tjänstebibliotek skall finnas en ontologi med ett kunskapssystem till denna tjänst. Härigenom blir det möjligt att skapa applikationer automatiskt eller fördefiniera dem för olika typer av *roller*.

TAT kommer att automatiskt knytas till de AAT. I de fall när dessa utgörs av sensorer måste denna knytning ske vid exekveringstillfället, eftersom sensortyper kan variera över tiden map ljusförhållanden samt väder och vind. Undantag från detta måste, som redan nämnts i avsnitt 1.2, kunna medges i de fall då aktörer har behov av en speciell tjänst, t ex sensortjänster eller andra. En ytterligare orsak till att det måste vara möjligt att på ett aktörsspecificerat sätt knyta specifika tjänster till sin verksamhet hänger samman med de fall då aktörerna vill prenumerera på vissa data från en given sensortjänst. Den aktuella tjänsten måste vara anpassad till detta. Detta måste naturligtvis ske med stöd av tjänsteontologin se avsnitt 1.6. Figur 4 beskriver kunskapsstrukturen för generering av aktörsapplikationer



Figur 3. Principen för hur en aktörsapplikation skapas.



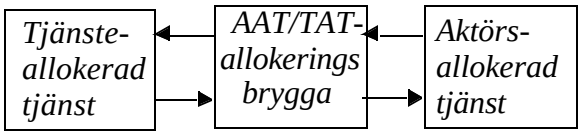
Figur 4. Kunskapsstrukturen för generering av aktörsapplikationer.

2.3 Allokeringsbryggor

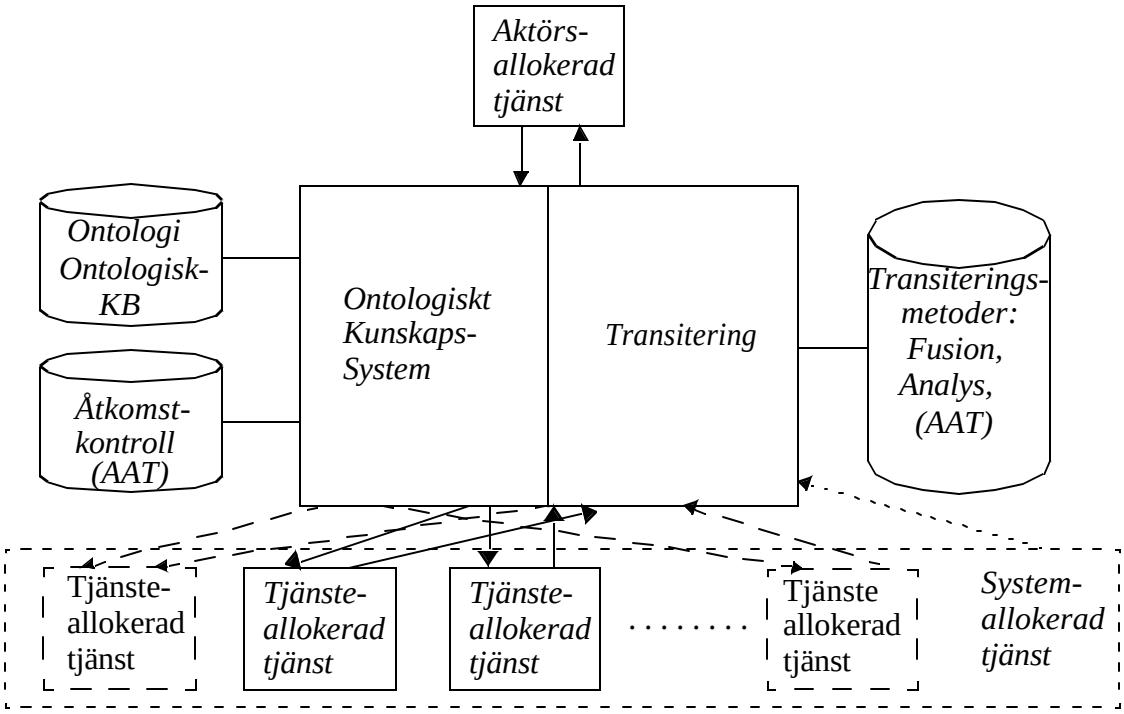
Behovet av att på ett enkelt och kraftfullt sätt allokera underordnade TAT till en överordnad, oftast en AAT, har redan omnämnts. För att lösa detta problem krävs att de olika tjänsterna kan *skaka hand med varandra* med hänsyn till de villkor som definieras av det ontologiska kunskapssystemet. Detta kan naturligtvis genomföras på en mängd olika sätt vilka diskuteradas i avsnitt 7.2 i del 1 utgående från det exempel som studerats vid FOI där man automatiskt kan knyta sensortjänster till ett frågespråk. Således är det möjligt att med stöd av ett ontologiskt kunskapssystem styra kopplingen och kommunikationen mellan tjänster på olika nivåer. Det delsystem som krävs för att genomföra detta kallas här för en *allokeringsbrygga* (figur 5).

Genom att låta det ontologiska kunskapssystemet hantera kopplingen mellan tjänsterna blir det också möjligt att knyta andra tjänster till verksamheten. Till de senare hör t ex tjänster för åtkomstkontroll av utgående respektive inkommande meddelanden. Vidare blir det möjligt att specificera de sensordataanalysprogram som behövs för att på ett adekvat sätt analysera sensordata. I anslutning till detta blir det möjligt att i förekommande fall fusionera analyserade sensordata från multipla sensorer för att resultatet skall bli mer tillförlitligt. Sammanfattningsvis så stödjer kunskapssystemet allokeringen av de underliggande tjänsterna för hantering av utgående information, medan den i motsatt riktining inkommande informationen passerar den s k transiteringsmodulen (figur 6). Vad som här kommer att krävas är således utveckling av ett antal olika allokeringsbryggor med förmåga och uppgift att koppla de olika typerna av tjänster till varandra. Grundläggande för detta kommer att vara en utveckling av de olika ontologier som behövs för de olika tjänstetyperna. I [37] finns en ontologi för sensordatatjänster beskriven. På motsvarande sätt kommer andra ontologier behöva utvecklas för övriga tjänstetyper. Till detta kommer

de regler som behövs i det ontologiska kunskapssystemet som är specifika för de olika tjänstetyperna. Gemensamt i samtliga fall är dock att det kunskapssystem som skall användas är detsamma för samtliga allokeringsbryggor. Genom att på detta sätt hantera och överbrygga kopplingarna mellan tjänster på olika nivåer blir det möjligt att koppla redan existerande delsystem till ledningssystemet även om detta inte i alla lägen kommer att vara trivialt.



Figur 5. Tjänster på lägre nivå allokeras till tjänster på högre nivå via en allokeringsbrygga.

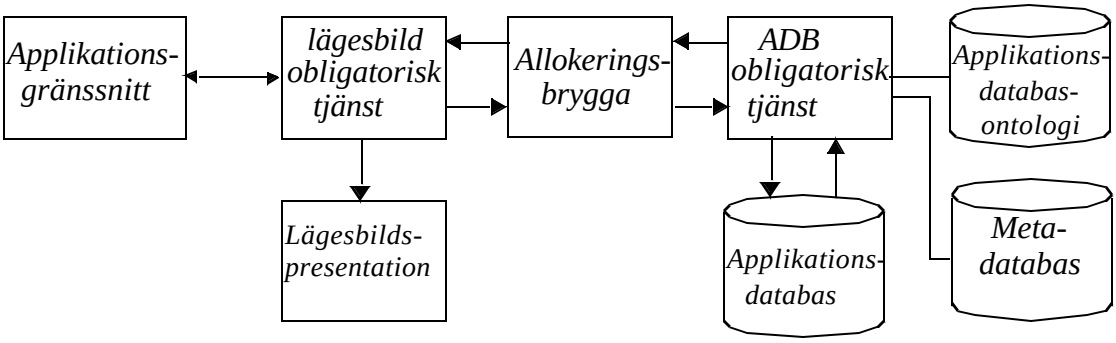


Figur 6. Strukturen för en allokeringsbrygga mellan AAT och en TAT.

2.4 Applikationsdatabas och konsistent lägesbild

Till varje aktörsapplikation hör de två obligatoriska tjänsterna för lägesbild och applikationsdatabasen (figur 7). Även dessa båda tjänster är sammankopplade via en allokeringsbrygga. Till applikationsdatabasen knyts en ontologi. Denna ontologi beskriver applikationsdatabasens information map dess struktur. En metadatabas som beskriver aktuella applikationsdata samt data

som beskriver deras bakomliggande kontext måste finnas tillgänglig. Dessa båda tjänster är kopplade till applikationsgränssnittet genom lägesbildstjänsten.



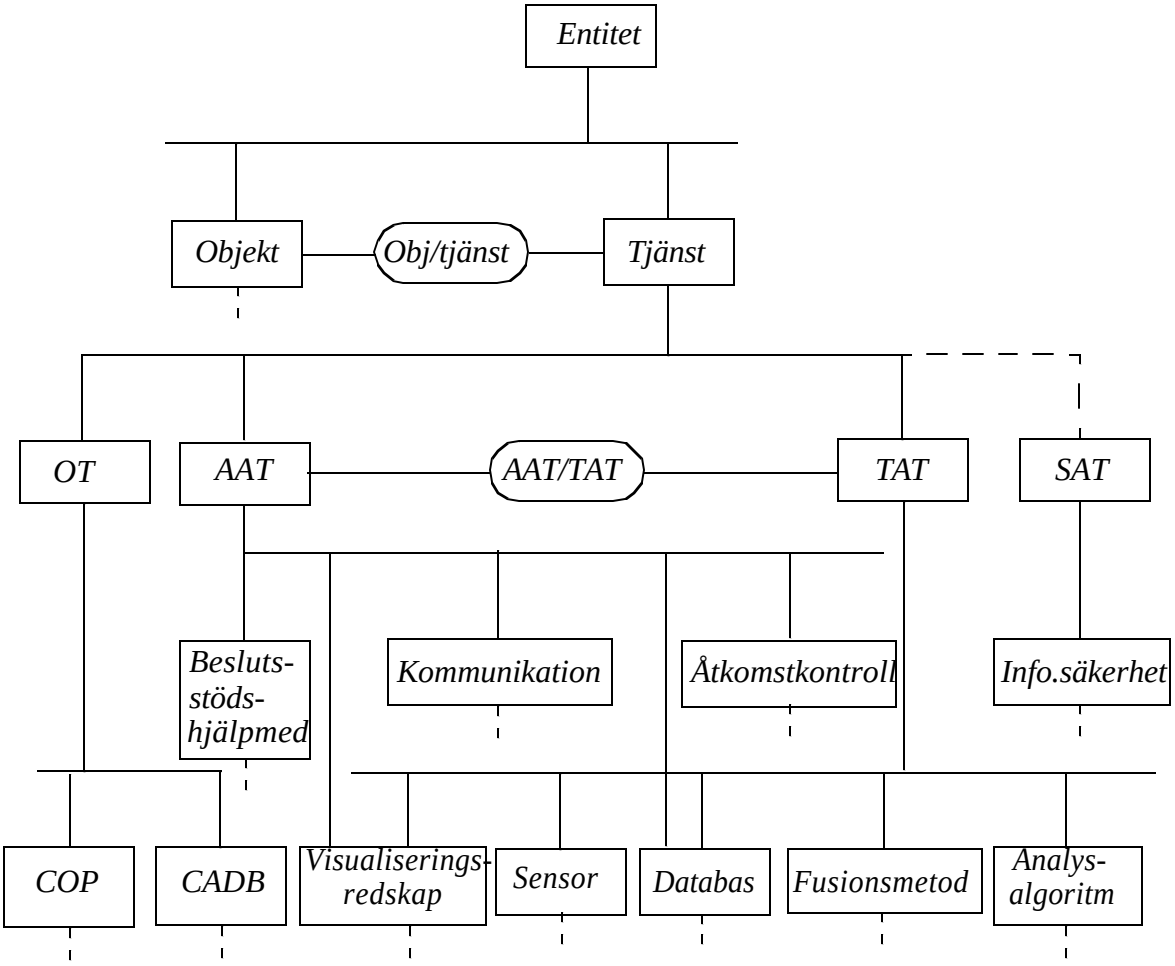
Figur 7. Allokeringsbrygga mellan lägesbild och applikationsdatabas.

2.5 Ontologierna och deras strukturer

En ontologi är en hierarkisk beskrivning av olika typer av objekt som också kan innehålla olika förekommande objektrelationer. Information som beskrivs på högnivå kan också ärvas av objekt på lägre nivå. Rotobjektet kallas här ting (eng. thing) men kallas ibland också entitet. Den ontologi som finns beskriven i figur 8 beskriver de tjänster som kan förekomma i anslutning till den här beskrivna ledningsmodellen. Det bör emellertid betonas att den aktuella ontologin inte på något sätt är komplett. De förekommande tjänsterna har bara till uppgift att illustrera några troliga typer. Som framgår återfinns de fyra grundtyper som diskuterades i del 1, dvs obligatoriska tjänster (OTT), aktörsallokerade tjänster (AAT), de tjänsteallokerade tjänster (TAT) samt systemallokerade tjänster (SyAT). I strukturen ligger alla dessa fyra typer på samma nivå. Under var och en av de fyra typerna återfinns olika representanter för dessa, t ex finns till AAT:erna kommunikation och beslutsstöd kopplade. Databastjänstetyperna finns kopplade till både AAT och till TAT, vilket hänger samman med att både aktörer och AAT har behov av att allokera sådana tjänster. Ontologin innehåller vidare också två objektrelationer (ontologin är inte heller komplett med avseende på möjliga relationer) dvs en relation mellan tjänstetyper och objekttyper. Med objekt avses här objekt som kan återfinnas i insatsmiljön, t ex hot av olika slag. Avsikten med denna relation är att göra det möjligt att genom att fråga efter ett visst objekt enkelt kunna avgöra vilka tjänster som kan användas för att avgöra om det aktuella objektet kan hittas i insatsområdet. I ett sådant sammanhang kan tjänsten vara en speciell sensor. Den andra relationen gäller mellan AAT och TAT och kan användas för att bestämma vilka TAT som kan knyttas till en viss AAT. Både dessa relationer kan fungera även i motsatt riktning dvs ur en gi-

ven sensortjänst kan det bestämmas vilka objekt som den är lämplig för. Dessa relationer är båda av s k många till många typ, dvs det kan finnas många sensorer som kan användas för att hitta ett givet objekt liksom det också går att använda en given sensor för att hitta många olika objekttyper.

I figur 8 har de systemallokerade tjänsterna en streckad bindning till tjänstenoden i den ontologiska strukturen. Detta har endast gjorts för att markera att en aktör utan speciell behörighet inte har åtkomst till tjänster av denna typ.



Figur 8. Delar av den ontologi som, för stöd till selektering av olika tjänstetyper och för stöd till allokeringsbryggan, beskriver olika förekommande tjänstetyper och deras relationer.

Andra typer av ontologier kommer också att behöva utvecklas. T ex kommer en ontologi att behövas för att bestämma vilka sensortjänster som kommer att behöva knytas till, exempelvis ett

frågespråk. Exempel på denna ontologi och dess struktur finns att läsa i [37]. Till ontologierna i tjänstebryggorna kommer också ontologierna i anslutning till de SyAT:erna. En konsekvens av detta är att ontologierna kan ses som *distribuerade* ontologier som var och en kommer att bidra till att styra verksamheten i ledningssystemet.

3. Riskmodellen

En central del i ledning vid riskhantering är förmågan att kunna bedöma och hantera hot och risken för att dessa realiseras. Detta innebär att stöd för att genomföra riskbedömningar kommer utgöra en viktig funktion i ett framtida ledningssystem. För att få en förståelse av vad riskbedömning innefattar togs en konceptuell modell av riskbedömning fram under förstudien [3].

Den konceptuella riskmodellens främsta syfte var att skapa insikt i hur koncept som skyddsvärda objekt, hotagenter, hot, risker, konsekvenser och motåtgärder förhåller sig till varandra. Detta sker genom att ge stöd för att beskriva skyddsvärda objekt, vilka hot de är utsatta för, vilken risk dessa hot utgör samt vilka konsekvenser realisering av ett hot skulle innebära. I modellen tas även hänsyn till hur förebyggande åtgärder påverkar risken för att ett hot realiseras, samt hur insatser minskar konsekvenserna av ett realiserat hot. Konsekvenserna av en realisering av ett hot inverkar såväl på det påverkande skyddsvärda objektet som dess omgivning. Det vill säga påverkan av ett skyddsvärt objekt kan i sig utgöra ett hot mot andra objekt. Detta innebär att det kan uppstå kedjereaktioner av hot som realiseras, vars konsekvenser utgör realiseringen av nya hot mot andra objekt o s v. Denna kedjereaktion kan såväl eskalera som avta.

En väl genomarbetad riskmodell kan används som grund för att simulera hot, dess konsekvenser och möjliga kedjereaktioner. Möjligheten att simulera ger ett bättre beslutsunderlag för riskbedömningar och utveckling av motåtgärder, såväl för preventiv som operativ krishantering. Lärdomar av konsekvenser, av realiserade alternativt simulerade realiseringar av hot, kan används som underlag för att göra bättre riskbedömningar framöver.

I denna studie vidareutvecklas den konceptuella riskmodellen genom att preciseras och formaliseras. Riskmodellen delades upp i (1) en *datamodell* som kan utgöra en grund för en implementering av en riskdatabas, (2) en *ontologi* för att beskriv vad som avses med de olika entiteter

(objekt) som finns i datamodellen samt (3) tre *aktivitetsmodeller* som beskriver hur arbetet genomförs exempelvis med att bedöma en risk.

3.1 Datamodellen

Datamodellen som ingår som en del av riskmodellen beskrivs med notationen entitets-relationsdiagram (figur 9). Generellt består denna notation av tre delar (1) entiteter, (2) relationer och (3) egenskaper. Det finns ett antal utökningar av den generella formen, men ingen av dessa används här. Entiteter beskriver enheter som kan vara olika typer av artefakter, individer och abstrakta objekt. Relationer används för att beskriva relationerna mellan de olika typerna av entiteter. Så väl entiteter som relationer kan ha egenskaper. Den nya datamodellen som tagits fram innefattar fyra entiteter: (1) Hotagent, (2) Aktivitet, (3) Skyddsvärt objekt och (4) Kontext.

Entiteten *Hotagent* omfattar individer, grupper av individer och organisationer/nätverk samt objekt som anses utgöra ett hot under vissa betingelser. Individer utgörs av exempelvis enskilda terrorister och extremister. Organisationer är exempelvis av terrorist- och extremistorganisationer, medan nätverk är av löst kopplade sammanslutningar av organisationer och/eller individer. Andra typer av hotagenter är objekt i vårt samhälle vars primära syfte inte är ett hot, men som kan manipuleras eller vid tekniska fel kan utgöra ett påtagligt hot. Exempel på detta är kärnkraftverk och transporter av farligtgods som vid attentat eller olyckor utgör ett hot mot omgivningen. Hotagent har fyra egenskaper (1) Hotnivå, (2) Kategori, (3) Lokalitet och (4) Kännedom. Hotnivå är ett mått på vilket hot som en viss hotagent anses utgöra. För att avgöra vilken hotnivå en hotagent har så behövs hotanalyser genomföras. Kategori beskriver vilken typ av hotagent det är, exempelvis terrorist. Lokalitet beskriver var en specifik hotagent anses befinner sig. Kännedom är ett mått på vilken mängd av och säkerheten på den kunskap som finns gällande en specifik hotagent.

Entiteten *Aktivitet* utgörs av de aktiviteter som hotagenter utför. Dessa kan innefatta demonstrationer och olika typer av aktioner, men också sådana aktiviteter som inte i första skede ses som ett hot, men kan bli detta om något oförutsätt inträffar, exempelvis om en långtradare som transporterar farligt gods råkar ut för en olycka. Entiteten Aktivitet har två attributet (1) Kategori och (2) Hotnivå. Kategori beskriver vilken typ av aktivitet som en specifik aktivitet utgör, exempelvis en demonstration. Hotnivå beskriver graden av hot som aktiviteten utgör, exempelvis en de-

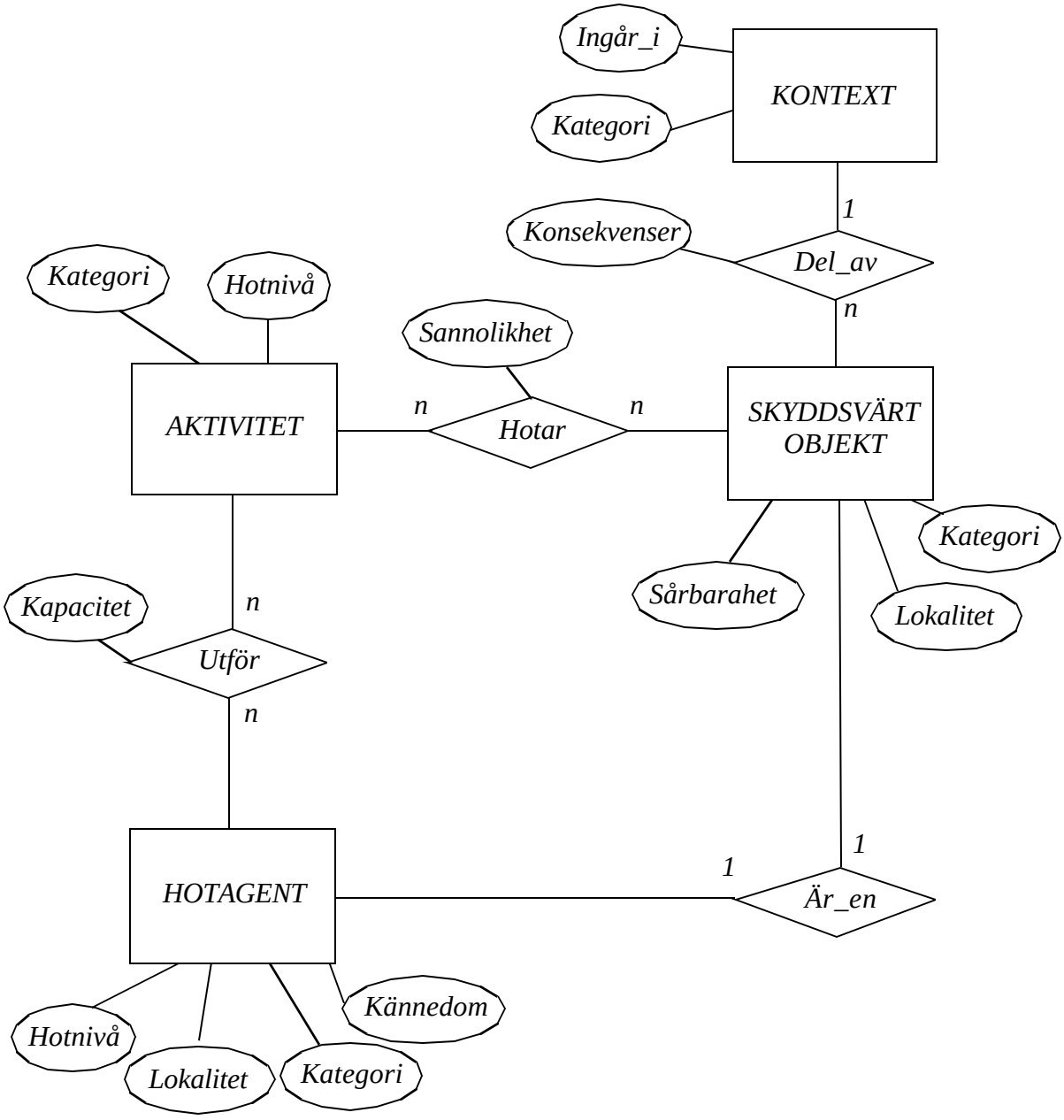
monstration gällande arbetstider har en relativt låg hotnivå medan aktioner vid ett möte gällande internationalisering kan anses medel hotnivå samt att införsel av illegala vapen kan anses ha hög hotnivå.

Skyddsvärda objekt utgörs av objekt som finns permanent eller tillfälligt i omgivningen och som anses vara skyddsvärda. Exempel på detta kan vara kärnkraftverk, flygplatser, ledningsfunktioner och skolor. Vissa skyddsvärda objekt kan om de utsätts för avsiktlig påverkan eller olyckor utgöra en hotagent. Till entiteten Skyddsvärt objekt kopplas tre egenskaper (1) sårbarhet, (2) kategori och (3) lokalitet. Sårbarhet beskriver graden av sårbarhet som ett objekt anses ha. För att avgöra sårbarheten måste en sårbarhetsanalys genomföras. Kategori beskriver vilken typ objektet utgör, exempelvis ett sjukhus eller en flygplats. Lokalitet beskriver var det skyddsvärda objekt fysiskt finns. Detta kan röra sig om ett statiskt värde som exempelvis för en flygplats, men också ett förändligt värde som exempelvis farliga transporter.

Kontext utgörs av det område/omgivning som en specifik implementering av riskmodellen avser. Detta kan utgöras av en nation, ett län och en kommun, men även ett kärnkraftverk, ett sjukhus och en flygplats. Kontexten kan också utgöras av abstrakta företeelser som flygplats, det vill säga en virtuell flygplats som kan ses som en modell för de flesta flygplatser. Entiteten Kontext har två attribut (1) Kategori och (2) Ingår_i. Kategori beskriver vilken typ av kontext en specifik kontext är. Ingår_i beskriver vilka kontexter den specifika kontexten finns i, exempelvis ett sjukhus ligger fysiskt placerat i en kommun och tillhör organisatoriskt ett landsting.

Datamodellen innefattar även fyra relationer mellan entiteterna. Mellan Skyddsvärt objekt och Kontext finns relationen Del_av. Detta innebär att flera skyddsvärda objekt är delar av en kontext. Denna relation har egenskapen Konsekvenser som utgör ett mått på vilka konsekvenser det skulle få för den aktuella kontakten om det skyddsvärda objektet skulle förolyckas. Mellan Aktivitet och Skyddsvärt objekt finns relationen Hotar. Detta innebär att flera aktiviteter utgör ett hot mot flera skyddsvärda objekt. Denna relation har egenskapen Sannolikhet som utgör ett mått på sannolikheten för att hot realiseras. Mellan Hotagent och Aktivitet finns relationen Utför. Detta innebär att flera hotagenter utför en eller flera aktiviteter. Denna relation har egenskapen Kapacitet, som utgör ett mått på kapaciteten en hotagent har att genomföra en viss aktivitet.

Mellan Skyddsvärt objekt och Hotagent finns relationen Är_en. Detta innebär att ett skyddvärt objekt under vissa förutsättningar kan utgöra ett hot, det vill säga är en hotagent.

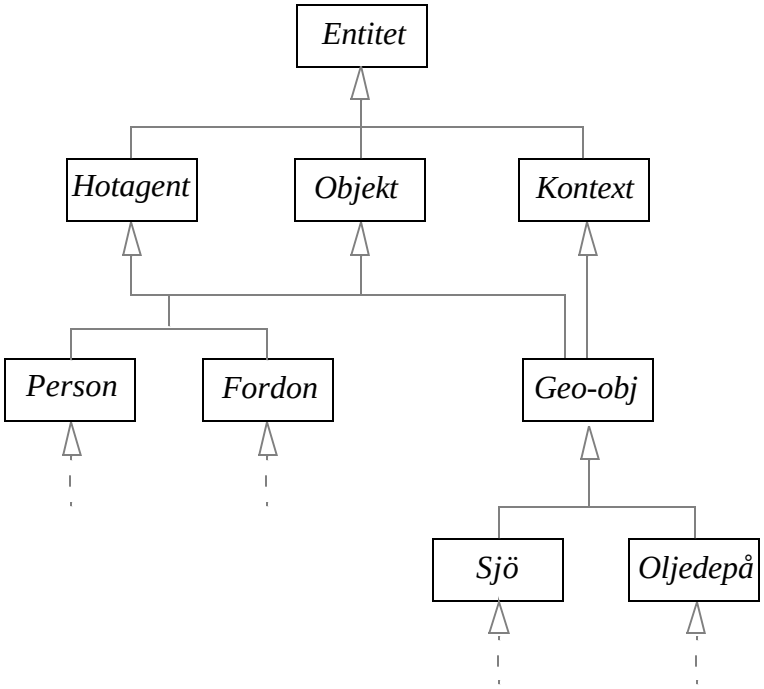


Figur 9. Datamodellen som beskriver de i riskmodellen ingående entiteterna, samt deras egenskaper och relationer.

3.2 Ontologi för riskmodellen

Ontologi för riskmodellen beskriver koncepten skyddsvärda objekt, hotagenter samt kontext (figur 10). Skyddsvärda objekt utgörs av personer, fordon och geografiskt lokaliserade objekt (geo-obj). I den första version av ontologi för riskmodellen beskrivs inte vidare vilka typer av

personer och fordon som kan ingå. Exempel på geografiskt lokaliserade objekt är sjöar och oljedepåer som i detta fall anses vara skyddsvärda. Hotagenter utgörs av personer, fordon och geografiskt lokaliserade objekt. Terrorister är exempel på personer som är hotagenter. Transport av farligt gods på lastbil är ett exempel på fordon som kan ses som hotagenter. Även brinnande oljedepåer är exempel på hotagenter. Kontext utgörs av geografiska lokaliserade objekt dessa kan vara en flygplats, en kommun, flygplats eller större sjö. Kontexterna innehåller skyddsvärda objekt.

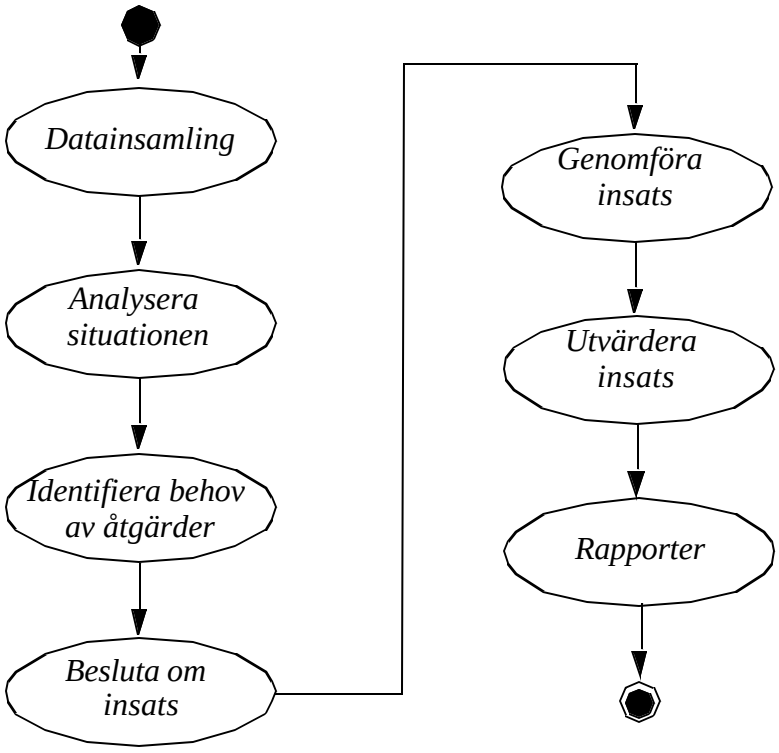


Figur 10. Ontologi för beskrivning av skyddsvärda objekt, hotagenter samt kontext.

3.3 Operativ krishantering

Operativ krishantering sker i syfte att avhjälpa och minska konsekvenser samt förhindra eskalerande kedjereaktioner vid incidenter. Aktivitetsmodellen som beskriver operativ krishantering innefattar (1) Datainsamling, (2) Analysera situationen, (3) Identifiera behov av åtgärd, (4) Besluta om insats, (5) Planera insats, (6) Genomföra insats, (7) Utvärdera och (8) Rapportera (figur 11). Aktivitetskedjan Operativ krishantering initieras av att indikationer på behov av en operativ insats mottas, detta genom begäran från någon annan organisation eller igenom information gällande en incident.

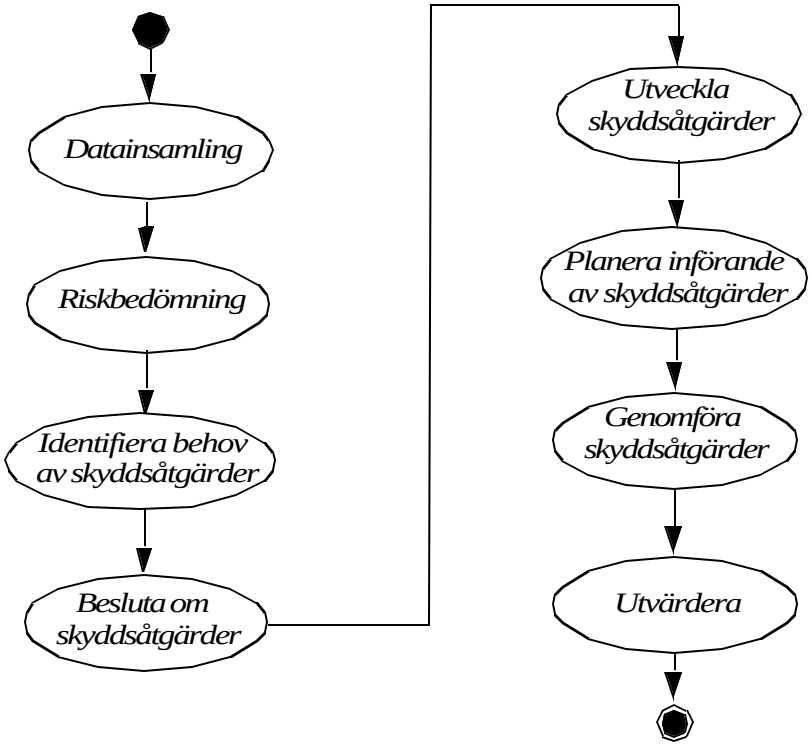
Aktiviteten *Datainsamling* syftar till att samla in data och information som behövs för att kunna agera mot krisen. Detta kan ske från såväl olika former av tekniska sensorer som observationer, men innefattar även införskaffandet av information om vilka resursers som står till förfogande för att hantera krisen. Det gäller att skaffa sig data/information som kan ligga till grund för en lägesförståelse. Aktiviteten *Analysera situationen* syftar till att skaffa sig en bild av situationen, det vill säga krisen, den omgivning som krisen förekommer i och vilka egna resurser och möjligheter som finns för att hantera situationen. Aktiviteten *Identifiera behov av åtgärder* syftar till att ta reda på vad som behöver genomföras för att hantera situationen. Aktiviteten Besluta om insatser syftar till att baserat på behovet av åtgärder och de resurser som står till förfogande besluta vilka insatser som skall genomföras. Aktiviteten *Planera insats* syftar till att besluta när i tiden och av vem insatser skall genomföras. Aktiviteten *Genomföra insats* syftar till att leda genomförandet av de insatser som beslutats. Detta innefattar bland annat att koordinera verksamheten. Aktiviteten *Utvärdera* syftar till att bedöma effekten av genomförda insatser samt om insatserna genomfördes som planerat. Utvärderingen skall ligga till grund för beslut som skall fattas om fortsatta aktiviteter. Aktiviteten *Rapportera* innefattar att informera berörda parter om den insats som genomförts.



Figur 11. Aktivitetsdiagram som beskriver operativ krishantering.

3.4 Preventiv krishantering

Preventiv krishantering sker i syfte att förebygga att hot realiseras och att konsekvenserna vid realisering av hot blir så små som möjligt. Denna typ av krishantering innefattar aktiviteterna (1) Datainsamling, (2) Riskbedömning, (3) Identifiera behov av skyddsåtgärder, (4) Besluta om skyddsåtgärder, (5) Utveckla skyddsåtgärder, (6) Planera införandet av skyddsåtgärder, (7) Genomföra skyddsåtgärder och (8) Utvärdera (figur 12).



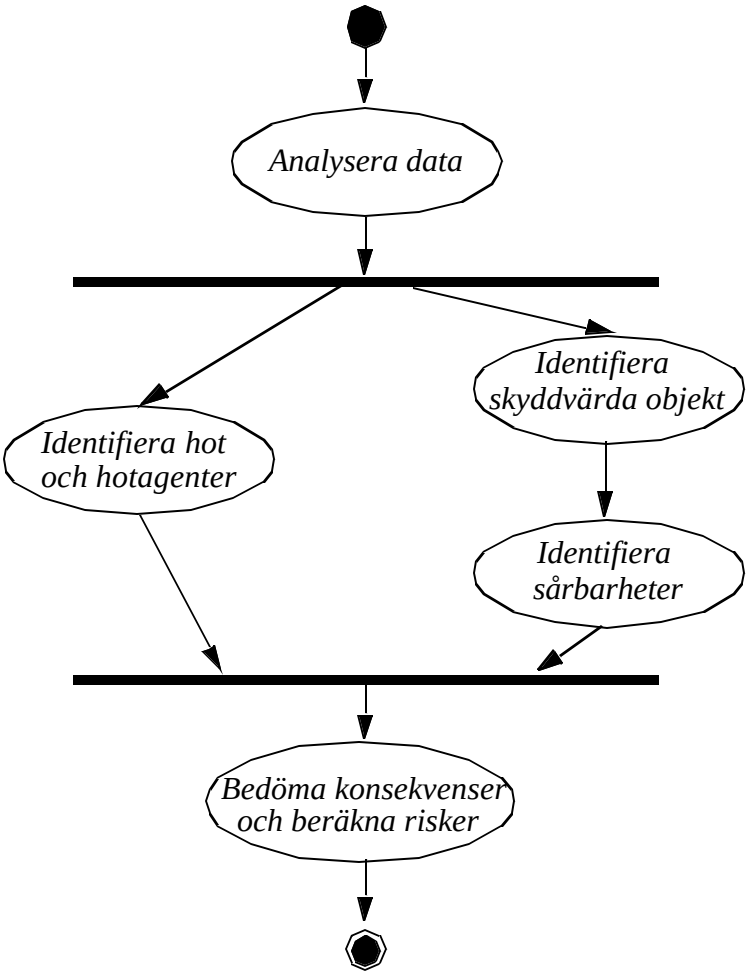
Figur 12. Aktivitetsdiagram som beskriver preventiv krishantering.

Aktiviteten *Datainsamling* syftar till att samla in data och information om skyddsvärda objekt, hotagenter och aktiviteter som pågår. Aktiviteten *Riskbedömning* är en komplex aktivitet, vilken består av flera aktiviteter som beskrivs nedan. Aktiviteten *Besluta om skyddsåtgärder* syftar till att baserat på bedömningen av risker och konsekvenser besluta om vilka skyddsåtgärder som skall vidtas. Aktiviteten *Utveckla skyddsåtgärder* syftar till att ta fram de skyddsåtgärder som inte finns tillgängliga. Aktiviteten *Planera införandet av skyddsåtgärder* syftar till att ta fram en plan över genomförandet (införandet) av de skyddsåtgärder som beslutats. Detta innefattar när och av vem som skyddsåtgärderna skall genomföras. Aktiviteten *Genomföra skyddsåtgärder* syftar till att realisera den plan för genomförande av skyddsåtgärder som tagits

fram. Aktiviteten *Utvärdera* syftar till att utvärdera om de skyddsåtgärder som genomförts får den effekt som avsetts och om dessa kan anses som tillräckliga.

3.5 Riskbedömning

För att få kännedom om vilka risker som föreligger rörande skyddsvärda objekt och vilka konsekvenser en realisering av hot skulle få, behövs en riskbedömning. Denna baseras på objektets sårbarhet, sannolikhet för att ett hot realiseras samt vilka konsekvenser resultatet av en realisering av ett hot får. Riskbedömningen syftar till att bedöma risker för hot och deras konsekvenser för att kunna ta beslut om skyddsåtgärder. Denna bedömning innefattar fem aktiviteter (1) Analysera data, (2) Identifiera hot och hotagenter, (3) Identifiera skyddsvärda objekt, (4) Identifiera sårbarheter och (5) Bedöma konsekvenser och beräkna risker (figur 13).



Figur 13. Aktivitetsdiagram som beskriver genomförandet av riskbedömning.

Aktiviteten *Analysera data* syftar till skaffa sig en överblick av tillgänglig data och information. Aktiviteten *Identifiera hot och hotagenter* syftar till att bedöma vilka hot som finns mot de skyddsvärda objekten och vilka hotagenterna är som anses kunna realisera dessa. Aktiviteten *Identifiera skyddsvärda objekt* syftar till att bedöma vilka objekt i kontexten som anses vara skyddsvärda. *Identifiera sårbarhet* syftar till att identifiera och bedöma sårbarheter hos de skyddsvärda objekten. Aktiviteten *Bedöma konsekvenser och beräkna risker* syftar till att avgöra vilka konsekvenser realiseringen av hot skulle få och göra en beräkning av sannolikheten för att hot realiseras.

4. Informationssäkerhetsmetodik

Utvecklingen av säkerhetsfunktionalitet inom ledningssystem för krishantering bör baseras på noggrann analys av aktuellt behov av säkerhet och hur detta på bästa möjliga sätt kan realiseras. Detta kan i den föreslagna designfilosofin förenklas till två grundläggande idéer:

- Design av säkringsbara system.
- Design baserad på allokeringsbryggor och distribuerade ontologier.

Allokeringsbryggor och distribuerade ontologier diskuteras mera i detalj i andra delar av rapport, men en fördel vid identifiering och design av säkerhetstjänster är att man på ett strukturerat sätt kan beskriva tjänsters uppbyggnad och relationer till varandra. Därmed underlättas identifieringen av avsaknader och förbättringsbehov i det system som utvecklas.

4.2 Design av säkringsbara system

Design av säkringsbara system, d v s system som kan säkras under drift, kan i enlighet med förstudien [3] delas upp i tre huvudprocesser:

- Kontextuell modellering
- Hantering av säkerhetskrav
- Implementering av säkerhetskrav

Alla tre huvudprocesser löper under hela systemets livscykel och det finns beroenden och överlapp mellan dem. Detta ger en dynamisk design, vilket torde vara en fördel för dynamiska och anpassningsbara system med höga säkerhetskrav. Samtliga huvudprocesser inrymmer också ett

antal relevanta forskningsfrågor, vilka kräver adekvata lösningar för att en rimlig nivå av informations- och IT-säkerhet skall erhållas.

Med denna utgångspunkt och ur informations- och IT-säkerhetssynvinkel är följande forskningsfrågor, som förstudien [4] identifierade, speciellt viktiga:

- Hur skall metoder för hantering av säkerhetskrav utvecklas?
- Hur interagerar dessa med motsvarande metoder för andra systemkrav, d v s systemutvecklingsprocessen i stort?
- På vilket sätt påverkar IT-säkerheten, eller systemets IT-säkerhetsnivå, tilltron till systemet och vice versa?
- Hur bör risk- och ledningsmodeller påverka modellering av informations- och IT-säkerhet i ledningssystem för krishantering och vice versa?

4.2 Ontologibaserad design av säkerhetstjänster och några relaterade avvägningar

Med avseende på säkra agenter på den så kallade semantiska webben, observerar Farkas och Huhns [43] att "enhanced processing power can be a double-edged sword” och att “malicious users and their agents can disclose sensitive information or sabotage the information of others". Detta torde även vara en giltig observation rörande ledningssystem för krishantering. Förstärkt beräkningsförmåga hos involverade system med höggradig automation är nödvändigt för att nå den funktion som krävs i krislägen. Vad som automatiseras skall vara det mera rutinmässiga, mänskliga aktörer skall fortfarande hantera svårare ej rutinmässiga beslut. En betydande svårighet existerar helt klart i att dra gränsen mellan vad som är rutinmässigt respektive ej rutinmässigt.

Inferensproblem, det vill säga att känsliga data kan avslöjas genom att kombinera icke-känsliga data med databasers metadata vilka möjliggör databassökningar, är ett problem som kräver närmare studier för hur detta med avseende på krishantering bäst hanteras. I det förslag till systemarkitektur som föreslås kommer med nödvändighet viss information att vara distribuerad, men ägas av en aktör eller en grupp av aktörer. För ytterligare aktörer kan informationen dock vara tillgänglig, eventuellt med restriktioner för vissa aktörer.

I en nätverksbaserad heterarkisk lösning medför detta en betydande utmaning, eller rent av en uppsättning av olika utmaningar. Den öppna miljön detta resulterar i, baserad kring Web Services eller likartade metodiker, medför rika möjligheter för aktörer att komma åt för dem icke-auktoriserad information, vilket indikeras av [43] som ett problem. Detta kan ske via databassökningar med stöd av metadata. Det kan även ske genom att vid utformning av åtkomstkontroll beakta behov i en lokal miljö (till exempel en lokal aktörs behov), men ej i tillräcklig grad beakta annorlunda behov i en mera global miljö (till exempel mera restriktiva behov för vissa andra aktörer).

Autonomitet är en typ av problem som kan uppstå i nätverksbaserade situationer. Krishantering kan mycket väl medföra sådana situationer, exempelvis genom att insatsenheter kommunikationsmässigt isoleras från andra enheter och aktörer. Hur detta säkerhetsmässigt bör hanteras diskuteras i [44]. Det bör dock observeras att så här långt existerar ingen enkel och heltäckande lösning på problemet. Bör man på förhand definiera hur problem som autenticering och auktorisering skall hanteras vid autonomitet? Det medför ett betydande arbete med att definiera vilka autonomitetssituationer som kan uppstå och hur dessa skall hanteras. Exempelvis torde samarbete mellan olika enheter krävas i en krissituation, vilka kanske inte tidigare har samarbetat. Hur väl kan regler för detta utformas på förhand? En alternativ strategi är att från början minimera säkerhetsåtgärder, men detta kräver också en noggrann riskanalys och ett medvetet policymässigt ställningstagande.

Spårning av identiteter vid samverkan mellan enheter/aktörer kan vara en dellösning på dessa och liknande problem. Därigenom är det möjligt att förhindra att någon agerar i annans namn eller döljer sin medverkan. Ett förslag till identitetsspårning i Web-Service-sammanhang skisseras i [45].

Krishantering bör, så långt möjligt, vara baserade på väldefinierade och verksamhetsanpassade aktörsroller, policyn och beräkningsregler för att uppfylla ställda säkerhetskrav. Den höggradiga automationen kräver systemstöd för att hantera åtminstone enklare typer av intrång. I sin tur kräver detta högkvalitativ intrångsdetektering, beräkningsregler och sätt att välja åtgärder. Detta kräver omfattande vidare forskning. Att som det föreslås i [43] aktivt spåra samarbeten mellan

illasinnade användare och spåra data och ändringar av dessa, är en tänkbar lösning eller åtminstone som start på en sådan.

Vid detaljerad design av en säkerhetsarkitektur för ledningssystem vid krishantering kan en del inspiration hämtas från [46], där en uppsättning ontologier för auktorisering och personlig integritet inom semantiska Web-Services skisseras. För respektive tjänst ges en generell beskrivning i en *profil*, prestanda beskrivs i en *processmodell* och atomära processer hos processmodellen beskrivs av en *underbyggnad*[1]. Rörande säkerhetsrelevanta rättigheter, avgränsningar, åligganden och dispenser definieras dessa av särskilda attribut.

Huruvida en metodik som denna fungerar väl, i den besvärliga miljö som operativ krishantering kan vara, återstår att närmare studera. Likaså bör det studeras huruvida metodiken kan vidareutvecklas för andra områden än auktorisering och personlig integritet. Likaså krävs en nära och omfattande dialog med användargrupper och utvecklare för att nå något i närheten av önskade säkerhetskrav. Som tidigare konstaterat är situationsförståelse oerhört viktigt, men en betydande komponent för att uppnå denna är säkerhetsförståelse. Om man inte vet vad man kan riskera och hur dessa risker bör hanteras, vill man snabbt få betydande problem med utvecklade system när de sätts i drift i en operativ miljö. Gollmann [48] noterar att IT-säkerhet innebär ett grundläggande dilemma att hantera, eftersom säkerhetsomedvetna användare har specifika säkerhetskrav, men vanligen ingen säkerhetsexpertis.

Sammanfattningsvis rörande IT-säkerhet i ledningssystem för krishantering, bedöms följande områden som särskilt viktiga för utveckling av IT-säkerhetstjänster:

- Åtkomstkontroll innefattande identifiering, autenticering och auktorisering och vid behov kryptering
- Spårning (datahistorik för att spåra samverkan och även illegala aktörer).

1. *Grounding* används som begrepp för detta i den ursprungliga artikeln.

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI Ledningssystem Box 1165 581 11 Linköping	FOI-R--1569--SE	Metodrapport
	Forskningsområde 4. Ledning, informationsteknik och sensorer	
	Månad, år Januari 2005	**Projektnummer** E7919
	Delområde 41 Ledning med samband och telekom och IT-	
	Delområde 2	

Författare/redaktör	Projektledare
Erland Jungert Niklas Hallberg Amund Hunstad	Erland Jungert
	Godkänd av Johan Mårtensson
	Uppdragsgivare/kundbeteckning Krisberedskapsmyndigheten
	Tekniskt och/eller vetenskapligt ansvarig Erland Jungert

Rapportens titel

Arkitektur för tjänstebaserade krisledningssystem med preventiva och operativa förmågor

Sammanfattning (högst 200 ord)

Krishantering är ett område som kommer alltmer i fokus allt eftersom nya och mer omfattande kriser inträffat både nationellt, men också internationellt. För att krishantering skall kunna genomföras effektivt och på ett adekvat sätt framstår behovet av ledningssystem för preventiv och operativ krishantering som alltmer nödvändiga. Mot denna bakgrund kommer ett omfattande forsknings- och utvecklingsarbete att bli nödvändigt för att säkerställa de ledningsresurser som kommer att behövas. I detta sammanhang måste de behov och de krav som kommer att ställas på krisledningssystemen också att behöva säkerställas. I detta arbete beskrivs en arkitektur för krisledningssystem som skall ge stöd både för preventiv och operativ krishantering. Denna arkitektur grundar sig på behovet av ledningssystem som kan verka i nätverksbaserade miljöer och med utgångspunkt från ett tjänsteorienterat perspektiv. Centralt för detta arbete är att redan i ett tidigt stadium av utvecklingsfasen hänsyn tas till behov av IT-säkerhet, men även andra aspekter såsom ledningsstruktur, krisförståelse, funktionalitet, t ex beslutstöd, och förmågan till koordinering av krisverksamheten är av väsentlig betydelse i arbetet.

Nyckelord

Ledningssystem, krishantering, tjänstebaserad, nätverksbaserad, situationsförståelse, krisförståelse, IT-säkerhet, riskmodellering, beslutstöd, systemarkitektur, riskanalys.

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 73 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Command and Control Systems Box 1165 S-581 11 Linköping Sweden	FOI-R--1569--SE	Methodology report
	Programme Areas 4. C4ISTAR	
	Month year January 2005	**Project no.** E7919
	Subcategories 41 C4I	
	Subcategories 2	

Author/s (editor/s)	Project manager
Erland Jungert, Niklas Hallberg Amund Hunstad	Erland Jungert
	Approved by Johan Mårtensson
	Sponsoring agency Swedish Emergency Management Agency
	Scientifically and technically responsible Erland Jungert

Report title (In translation)

An architecture for service based command and control systems for crisis management with preventive and operative capabilities

Abstract (not more than 200 words)

Crisis management is an area that due to the occurrence of more frequent and extensive crisis, both nationwide and internationally, is getting increasingly attention. Thus, to handle crises effectively and efficiently the need for command and control systems for preventive and operative crisis management has become increasingly necessary. Hence, more resources must be used on research and development to secure the availability of such command and control resources that will be needed. In this context, the needs and the demands on crisis management systems for command and control must be identified. In this work, an architecture for command and control systems for crisis management is proposed. The architecture is intended to support both preventive and operative crisis management. The architecture is intended for command and control systems that are used in network oriented environments and with a service oriented perspective. Essential for this work has been to consider aspects of IT-security early in the development phase. Further, aspects such as the command and control structure, the functionality of the system, including e.g. decision support, and the capacity for coordination of the activities to be executed have been seen as critical features.

Keywords

Command and control systems, crisis management, service oriented, network oriented, situational awareness, crisis awareness, IT-security, decision support, systems architecture, risk analysis.

Further bibliographic information	Language Swedish

ISSN 1650-1942	Pages 73 p.
	Price acc. to pricelist