

ERLAND JUNGERT, CHRISTINA GRÖNWALL,  
NIKLAS HALLBERG, FREDRIK LANTZ



FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1250 anställda varav ungefär 900 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

Erland Jungert, Christina Grönwall,  
Niklas Hallberg, Fredrik Lantz

# Systemkoncept för intelligent övervakning av skyddsobjekt

<b>Utgivare</b> FOI - Totalförsvarets forskningsinstitut Ledningssystem Box 1165 581 11 Linköping	<b>Rapportnummer, ISRN</b> FOI-R--2309--SE	<b>Klassificering</b> Metodrapport
	<b>Forskningsområde</b> 7. Ledning med MSI	
	<b>Månad, år</b> Juni 2007	<b>Projektnummer</b> E7586
	<b>Delområde</b> 71 Ledning	
	<b>Delområde 2</b>	
<b>Författare/redaktör</b> Erland Jungert Christina Grönwall Niklas Hallberg Fredrik Lantz	<b>Projektledare</b> Erland Jungert	
	<b>Godkänd av</b> Martin Eklöf	
	<b>Uppdragsgivare/kundbeteckning</b> Svenska Kraftnät	
	<b>Tekniskt och/eller vetenskapligt ansvarig</b> Erland Jungert	
<b>Rapportens titel</b> Systemkoncept för intelligent övervakning av skyddsobjekt		
<b>Sammanfattning</b> <p>Behovet av övervakningssystem för viktiga anläggningar har under senare år ökat dramatiskt som en följd av allvarliga attacker mot både människor och anläggningar. Syftet med detta arbete har varit att utveckla ett systemkoncept för intelligent och flexibelt övervakning av skyddsanläggningar där <i>tidig</i> och <i>tillförlitlig</i> bestämning av händelser som kan leda till intrång i anläggningarna varit i fokus. Systemkonceptet gör övervakning utanför avspärrat område möjlig. Konceptet innehåller flera olika typer av sensorer som samverkar, vilket ger systemet möjligheter att klassificera objekt och följa väsentliga händelseförlopp. Därmed kan antalet falsklarm undertryckas kraftigt. Det koncept som redovisas kan hantera insamling och bearbetning av de stora sensordatamängder som genereras vid övervakningen. Systemets struktur är modulär och tjänstebaserad, varför det medger evolutionär systemutveckling och ett ökat leverantörsberoende. Konceptet innehåller delsystem för presentation av lägesbilder och användardialog för att ge användarna god situationsförståelse och ett adekvat beslutsunderlag. Det är möjligt att bygga en demonstrator som är baserad på de grundläggande principer som finns beskrivna i denna rapport. Vidare kommer man att kunna använda detta arbete som ett beslutsunderlag för att också i fortsättningen kunna förbättra sin övervakningsverksamhet, sitt systemutvecklingsarbete och sin förmåga att upphandla ändamålsenliga system för övervakning.</p>		
<b>Nyckelord</b> Intelligent övervakningssystem, tjänster, beslutsstöd, sensorsystem, datafusion.		
<b>Övriga bibliografiska uppgifter</b>	<b>Språk</b> Svenska	
<b>ISSN</b> 1650-1942	<b>Antal sidor:</b> 48 s.	
<b>Distribution enligt missiv</b>	<b>Pris:</b> Enligt prislista	

<b>Issuing organization</b> FOI – Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping	<b>Report number, ISRN</b> FOI-R--2309--SE	<b>Report type</b> Methodology report
	<b>Programme Areas</b> 7. C4I and Human Factors	
	<b>Month year</b> June 2007	<b>Project no.</b> E7586
	<b>Subcategories</b> 71 Command, Control, Communications, Computers, Intelligence (C4I)	
	<b>Subcategories 2</b>	
<b>Author/s (editor/s)</b> Erland Jungert Christina Grönwall Niklas Hallberg Fredrik Lantz	<b>Project manager</b> Erland Jungert	
	<b>Approved by</b> Martin Eklöf	
	<b>Sponsoring agency</b> Swedish National Grid	
	<b>Scientifically and technically responsible</b> Erland Jungert	
<b>Report title (In translation)</b> A system concept for intelligent surveillance of important establishments		
<b>Abstract</b> <p>Surveillance systems for protection of important physical establishments have become increasingly important due to serious attacks during the last few years against both people and establishments. The purpose of this work has been to develop a concept for intelligent and flexible surveillance of physical establishments, where <i>early</i> and <i>reliable</i> determination of activities and events has been in focus. Surveillance outside enclosed areas is made possible through the concept. It includes several types of sensors that co-operate, which gives the system an ability to classify objects and track important events. Therefore the number of false detections can be dramatically reduced. Collection and mangement of large volumes of surveillance data are made possible. The system structure is modular and service based, which allows for evolutionary systems development and increased supplier indendance. Subsystems for presentation of operational pictures and user dialogue are included to provide the user with adequate situation awereness. It is possible to use the system concept to build a demonstrator. The concept report will also be useful as a basis for decision making regarding surveillance activity, to improve surveillance system development and to improve the ability to procure appropriate systems for surveillance.</p>		
<b>Keywords</b> Intelligent surveillance system, service based, decision support, sensor systems, data fusion.		
<b>Further bibliographic information</b>	<b>Language</b> Swedish	
<b>ISSN</b> 1650-1942	<b>Pages</b> 48 p.	
	<b>Price acc. to pricelist</b>	

## Innehåll

1. Inledning .....	5
2. Behovsanalys .....	7
2.1 Anläggningarna .....	7
2.2 Intrång och övervakning .....	7
2.3 Larm och falsklarm .....	8
2.4 Sensorer .....	8
2.5 Larm till driftcentralen .....	8
2.6 Operatörsaspekter .....	9
2.7 Aktiviteter riktade mot ställverk .....	10
2.8 Ekonomiskt relaterade aspekter .....	10
2.9 Slutsatser .....	10
3. Problemidentifiering .....	12
3.1. Händelser runt skyddsanläggningen .....	12
3.2. Andra händelser .....	15
3.3. Kombinationer av händelser .....	15
4. Sensorer för intelligent övervakning .....	17
4.1 Beskrivning av sensorerna .....	17
4.2 Placering av sensorer .....	19
4.3 Exempel på sensorsystem .....	20
5. Dataanalys för intelligent övervakning .....	21
5.1 Sensordataanalys .....	21
5.2 Händelseanalys .....	22
5.3 Situationsanalys .....	23
5.4 Konsekvensanalys .....	25
5.5 Dataosäkerhet .....	26
5.6 Sensorstyrning .....	26
6. Systemarkitektur för intelligent övervakning .....	27
6.1 Tjänstebegreppet .....	27
6.2 Vyer och användarroller .....	28
6.3 Systemöversikt .....	30
6.4 Systemsektioner .....	30
6.5 Rollstruktur .....	32
6.6 Vyrelaterad information .....	34
6.7 Definierade tjänster .....	35
6.8 Beslutsstöd .....	37
7. Förmågor för intelligent övervakning .....	40
7.1 Scenario 1 .....	40
7.2 Scenario 2 .....	41
7.3 Scenario 3 .....	43
8. Systemutveckling och -integration .....	44
8.1 MOSART .....	44
8.2. Systemutveckling med MOSART .....	44
9. Sammanfattning .....	46
Referenser .....	48

# 1. Inledning

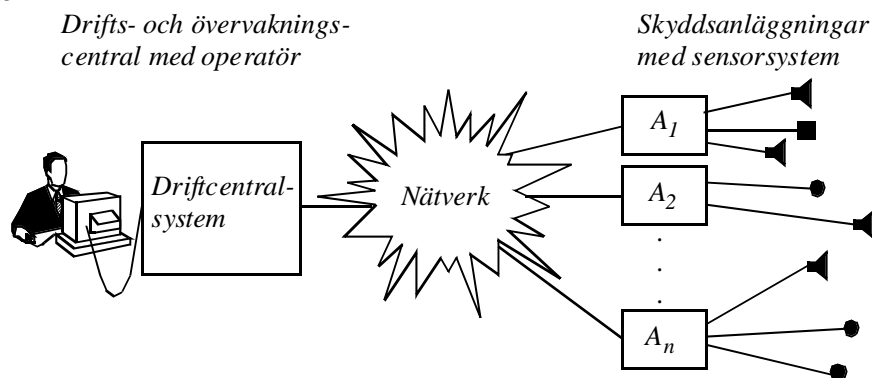
Syftet med denna rapport är att beskriva ett systemkoncept för intelligent övervakning av skyddsvärda anläggningar. Rapporten utgör ett underlag för utveckling av en system-demonstrator. Arbetet med att ta fram systemkonceptet har genomförts vid FOI på uppdrag av Svenska Kraftnät. Visionen är ett övervakningssystem som ger högre säkerhet till lägre kostnader, samt är anpassningsbart till de enskilda anläggningarna. Högre säkerhet uppnås genom att systemet bidrar till tidigare och mer tillförlitlig varning för intrång än dagens system för övervakning.

De skyddsanläggningar som systemkonceptet utvecklats för omfattar främst ställverk, kärnkraftverk och kraftverksdammar, men det kan lika gärna nyttjas för andra typer av anläggningar som behöver skyddas. Exempel på sådana anläggningar är olika typer av militära anläggningar, såsom förråd och baser. Gemensamt för dessa anläggningar är att de kan utsättas för icke-önskvärd påverkan som kan få stora konsekvenser. Exempel på icke-önskvärd påverkan är inbrott, stöld och sabotage, men även skadegörelse utförd av personer som inte är medvetna om riskerna med sitt handlande. Dessa anläggningar kan även drabbas av olyckshändelser och naturkatastrofer. Att helt skydda sig mot de senare, eller ens förutspå dem, är inte möjligt, men övervakningssystemet kan trots detta användas för att upptäcka när sådana händelser inträffar.

Förmågan att tidigt och tillförlitligt registrera händelser och aktiviteter som kan utgöra hot mot anläggningar är viktig. De objekt som behöver registreras utgörs främst av människor och fordon, men även kameror, kikare, vapen och verktyg är intressant att registrera. För att åstadkomma detta krävs att systemet:

- Automatiskt samlar in och analyserar information från sensorer och andra under rättelsekällor avseende händelser omkring skyddsanläggningar.
- Hanterar de stora och heterogena datavolymer dessa sensorer och underrättelsekällor ger upphov till.
- Sammanställer och underhåller lägesbeskrivningar över skyddsanläggningarna för att ge användarna ökad situationsförståelse.
- Stödjer en effektiv användardialog.
- Utnyttjar tekniska beslutsstöd för att ge användarna tillgång till ett adekvat beslutsunderlag.

Det föreslagna övervakningssystemet består av tre huvuddelar; ett delsystem vid anläggningen, ett delsystem i driftcentralen och ett kommunikationsnätverk. Vid anläggningarna finns anläggningssystemet omfattande ett antal olika sensorer. Detta system har kapacitet att utföra automatisk analys av sensordata. Vid övervaknings- eller driftcentral finns driftcentral-systemet. Detta ger användarna möjlighet att ta emot och hantera larm som genereras och att analysera den information som anläggningssystemen producerar. Eftersom anläggnings-systemen kommer att vara geografiskt skilda från den central där användarna hanterar information och larm krävs ett kommunikationsnätverk som binder samman anläggnings-systemen och driftcentralssystemet. Detta leder till en systemstruktur som framgår av figur 1.1. Kommunikationsnätverket kommer dock inte att utvecklas i det projekt som föreslås här, utan det kommer att ersättas av ett simuleringsramverk som också kan utnyttjas för system-utveckling och tester av olika slag.



Figur 1.1. Systemstrukturen för övervakningssystemet med dess tre huvudbeståndsdelar: driftcentralssystemet, kommunikationsnätverket och skyddsanläggningssystemen.

Rapporten har följande struktur. I kapitel 2 redogörs för resultatet av de intervjuer som genomfördes under projektets inledningsfas med, främst, anställda vid Svenska Kraftnät. Kapitel 3 presenterar ett antal olika händelser som är intressanta att identifiera i och omkring en skyddsanläggning. Dessa händelser har, tillsammans med intervjuerna i kapitel 2, varit utgångspunkten för definitionen av konceptets innehåll. En genomgång av sensorer som kan komma till användning, samt deras egenskaper och förmågor, görs i kapitel 4. I kapitel 5 presenteras den dataanalys som behövs för att avgöra vilka händelser som inträffat. I kapitel 6, görs en genomgång av den föreslagna tjänstebaserade systemarkitekturen dels med avseende på anläggningssystemen och dels med avseende på driftcentralssystemet. Vidare, i kapitel 7 presenteras några olika scenarier för demonstration, utgående från de händelser som presenterats i kapitel 3. För att på ett effektivt sätt realisera demonstratorn krävs en lämplig miljö för utveckling och testning, vilken presenteras i kapitel 8. Till sist följer en sammanfattning av arbetet i kapitel 9.

## 2. Behovsanalys

För att få en uppfattning om de förutsättningar som råder samt vilka behov av stöd för övervakning och intrångshantering som föreligger genomfördes intervjuer med personal från Svenska Kraftnät och Vattenfall. För att få en holistisk bild intervjuades ett antal personer som representerade olika personalkategorier. Bland de olika personer som intervjuades kan nämnas: Säkerhetschefen vid Svenska Kraftnät Lars Johanson, Ekonomiansvarige för investeringsobjekt vid Svenska Kraftnät Kerstin Keerweer-Höglund och Per Nastell projekt- och säkerhetssamordnare. Vid driftcentralen (driftcentralen) intervjuades systemansvarige Göran Bergius och operatören Gunde Claesson. Från Vattenfall intervjuades drift- och områdesansvarige för anläggningen i Kimstad Tomas Olson, samt serviceteknikern Dag Ahlquist båda vid ställverket i Kimstad.

Syftet med intervjuerna var att erhålla en förståelse för (1) verksamheten, (2) vilka behov av intelligenta intrångsskydd som föreligger, (3) nuvarande system och lösningar för att hantera övervakning och intrångshantering samt (4) den upplevda hotbilden mot dessa anläggningar. Resultatet av intervjuerna låg sedan till grund för det fortsatta arbetet. Detta kapitel presenterar en sammanfattning av de, för projektet, viktigaste observationerna från dessa intervjuer.

### 2.1 Anläggningarna

De allra flesta ställverk ligger ovan jord och är omgärdade av staket som normalt är dubblerade, om än inte till alla delar. Anläggningarna kan ligga så väl i bebyggelse som på enskilda platser.

Anläggningarna rondas med jämna mellanrum. Detta genomförs dels för att säkerställa drift och underhåll, så kallad teknisk rond och dels för att säkerställa funktionen hos de skydds-mekanismer som finns vid respektive ställverk, så kallad säkerhetsrond. Det senare innefattar bland annat att besiktiga staket för att tillse att dessa är intakta.

Vid ställverk finns objekt som är av speciellt viktiga att skydda eftersom de är kostsamma och svåra att ersätta. Vidare är det av viktigt att skydda driftcentralerna.

Driftcentraler kan skyddas med hjälp av ett liknande övervakningssystem som ställverken skyddas av. Tomtmarken utanför driftcentralen tillhör fastighetsägaren och bör kunna övervakas på samma sätt som ställverken. Vidare bör reservanläggningar övervakas eftersom ingen obehörig skall befinna sig runt eller i dessa anläggningar.

### 2.2 Intrång och övervakning

Intrång innebär att någon går in i en anläggning utan tillstånd. Exemplet på detta är när personer forcerar grindar och staket för att stjäla, saboterar eller genomföra annan typ av skadegörelse. Intrång i anläggningar i form av stölder och sabotage har ökat. Försök har även gjorts att förstöra anläggningar för att skada tredje part och stoppa deras verksamhet. Vidare finns det exempel på när förvirrade personer lyckas "smitta" in när en öppen grind lämnas obebvakad för en kort tid. Obehörig närvaro omfattar även när personal går in i en anläggning utan att ha tillstånd för detta. Det främsta skälet att förhindra intrång är att stänga ute kriminella, samt barn och människor utan fullständig sinnesnärvaro.

Det ska inte vara möjligt att ta sig vare sig över, under eller genom staketet som finns runt anläggningar. Därför vore det bra om ett framtida system för intrångsskydd kan detektera hål i och under staketet.

Ett övervakningssystem skall inte enbart omfatta skydd mot intrång utan även kontroll av in- och utpasseringar samt larm vid brand. Vidare bör möjligheten att övervaka personalen när det utför kritiska arbetsmoment och olika delar av anläggningen för att öka arbetsskyddet för individer beaktas. Ingen av de intervjuade upplever, eller tror att andra upplever, en ökad övervakning i form av intrångsskydd som integritetskränkande.

### **2.2.1 In- och utpasseringar**

Kontroll av in- och utpasseringar omfattar kontroll av personal som har arbetsuppgifter att genomföra i anläggningarna och som har behörighet för detta. Syftet med kontrollen av utpassering är att larma om personer inte lämnat anläggningen inom rimlig tid, dvs. då det finns anledning att anta att något hänt personen i fråga. Kontroll för inpasseringar ska larma om personer utan behörighet försöker gå in i anläggningen. Systemet bör också kunna avgöra när grindar är stängda eller öppna samt larma om de lämnats öppna.

In- och utpassering sker med kort och inte med nycklar; detta gäller idag dock inte vid alla anläggningar. In- och utpassering till anläggningen sker ibland med bil.

### **2.2.2 Brand**

Ytterligare motiv för övervakning av ställverk är behovet av att tidigt kunna detektera och larma vid brand. Konsekvenserna av brand i ett ställverk kan vara omfattande och medföra att ställverket inte kan användas under lång tid.

## **2.3 Larm och falsklarm**

En central aspekt vid övervakning av anläggningar är att övervakningssystemet inte får generera för många falsklarm, så att dessa hindrar operatörerna att uppmärksamma och agera på riktiga larm. Falsklarmen hänger samman med sensorernas förmåga att tolka data på ett korrekt sätt, dvs. data är på något sätt förknippade med osäkerheter. Valet av lämpliga sensorer blir därför speciellt angeläget. I vissa situationer bör ett larm kunna verifieras genom att man till operatören överför t. ex. en kamerabild. Exempel på en sådan situation är när det som systemet tolkar som ett intrång visar sig vara ett djur som vidrört staketet.

## **2.4 Sensorer**

Ett relativt stort antal sensortyper har testats av Svenska Kraftnät med avseende på aspekter som driftssäkerhet, driftskostnader och robusthet. Dessa tester har, sedan 2003, genomförts vid ett antal demonstrationsanläggningar. Bland har tester genomförts med fiberoptisk kabel för mark- och stängsellarm. Vid en av demonstrationsanläggningarna finns 10 kameror, varav två är rörliga, s. k. dome-kameror, samt en mikrovågsradar från Saab, som ger bäring och avstånd. Vissa delar av anläggningen fungerade dock som reflektorer som störde radarn. Vidare testas kameror med inbyggd signalbehandling, till exempel för rörelsedetektion. Tidigare problem med falsklarm på grund av sol och skuggor har man kommit till rätta med. Kameror med algoritmer för "human detektion" kommer att testas. I realiserbarhetsstudien redovisades problem med Thermovision (IR-kamera), [Nastell, 2002]. De IR-kameror som har testats nyligen har visat sig ge bra data för bildanalys. En förbättring som troligen beror på bättre bildbehandling i kameran. Sensorerna justeras vår och höst för att fungera önskvärt under rådande väder.

En annan demonstrationsanläggning ligger nära bebyggelse och har tidigare drabbats av inbrott. Där testas en kombination av vanligt stängsel och elstängsel. Elstängslet är av samma typ som sitter runt kohagar. När någon vidrör elstängslet får denne en ofarlig stöt och larmet går.

## **2.5 Larm till driftcentralen**

Till driftcentralen inkommer larm av olika typer. Väsentligen skiljs på stort och litet larm, men också på specificerade larm och klartextlarm. Stort larm inkluderar telelarm, brandlarm, nödlarm om någon skadad befinner sig i anläggningen, samt inbrottslarm. Operatören erhåller dessa larm kodade i olika färger. Enligt uppgift är dock inte sambandet mellan larmtyp och färger helt klart definierat. Till exempel så kan ett stort larm ha olika färger. Larmen kommer upp på operatörens skärm som en färgkodad textrad. Okvitterade larm blinkar till dess de blivit kvitterade av operatören. Larm som är kopplade till ett fysiskt objekt får en markering på textraden när de kvitteras. Andra larm som inte är kopplade till något fysiskt objekt, till exempel för höga strömmar, får ingen symbol kopplad till sig när de kvitteras.

Ett larmsystem för intrångsskydd bör inte integreras i nuvarande system för hantering av driftlarm, utan bör vara separat från detta. Ett system för intrångsskydd får inte störa driften av systemet, till exempel genom att överskicket av bilder från en anläggning fördröjer eller hindrar att driftlarm når driftcentralen.

För stora larm gäller att dessa skall åtgärdas omedelbart, dvs. personal skall skickas ut till den aktuella anläggningen direkt. Tiden från det att ett larm har gått och en person kan finnas på ställverket varierar. För vissa avlägset belägna ställverk kan det ta över 1 timme för personal att finnas på plats. För litet larm gäller att personal behöver skickas ut till anläggningen först nästa ordinarie arbetsdag. Vad personalen bör göra vid larm finns inte reglerat i föreskrifter, utan detta är erfarenhetsbaserat.

## 2.6 Operatörsaspekter

Operatörerna har på sina skärmar tillgång till schematiska bilder över linjer, stationer, brytare, och frånskiljare med mätvärden och uppgifter om status. Utöver "huvudsystemet" finns loggar och journalsystem som lagras på en PC. Vidare finns lokala porttelefonsystem med kameraövervakning och låssystem till stationerna samt ett reservlarmsystem.

Säkerhetssystem finns i form av inbrottslarm i dörrbrytare och rörelsedetektorer på flertalet stationer. Till detta kommer brandlarm och personella nödlarm. De senare aktiveras själv av nödställd personal och larmar förutom driftcentralen även övrig personal vid anläggningen. Även timlarm förekommer som automatiskt larmar om personal inte hört av sig efter viss tid, typiskt efter 30-60 min.

Driftlarm ges vid fel på utrustning, såsom när säkringar och brytare löser ut. Trasiga komponenter kan också ge driftlarm, liksom för låga respektive höga spänningar i nätet. Dessa kan regleras och åtgärdas från driftcentralen. Driftcentralen kan inte ta anläggningar ur drift för att utföra tester, utan dessa måste vara igång kontinuerligt.

När larm kommer in till driftcentralen identifieras stationen och dess larmlista kan plockas upp för att granskas närmare. Vissa stationer har högre prioritet än andra och måste därför åtgärdas först om flera larm skulle uppstå samtidigt. En viss prioritering av larmen kan göras av systemet för att stödja operatörerna, men funktionen anses av operatörerna kunna göras mer lättanvänd. Kvittring av larm innebär att dessa "nollas" och måste sökas i larmloggen för att kunna granskas på nytt.

Anläggningarna har ofta ett likströmssystem med batteribackup som driver växelriktare för att hålla igång exempelvis mätutrustning, larm, belysning och pumpar, även vid ett nätbortfall.

”Intelligentare” hantering av larm vore önskvärt i ett nytt övervakningssystem. Vid den senaste större störningen uppkom 90 sidor larm att hantera och att då identifiera var ursprungsfelet finns är svårt. Larmen tidsstämplas dessutom *inte vid uppkomst i anläggningen utan vid ankomst till driftcentralen*. Loggning av registrerade larm sker sedan i larmlistan i kronologisk ordning, det vill säga att någon sortering på objekt eller händelse inte kan göras, varför orsak och följdverkan kan vara svåra att urskilja.

Automataktiverade brandlarm går direkt till driftcentralen. Det varierar över landet huruvida Räddningstjänsten gör en uttryckning innan man fått en verifiering från driftcentralen. Personal från anläggningen måste också finnas på plats innan räddningstjänsten släpps in. De flesta brandlarm är falska (9 av 10) varför någon form av verifiering, t.ex. i form av en kamerabild, vore bra. Brand inträffar mindre än tio gånger per år.

Loggning av besökare vid anläggningen sker i den så kallade loggboken, som finns på en PC. Detta sker genom registrering av stationen samt personens namn och telefonnummer. Vad som ska åtgärdas i ställverket dokumenteras alltså inte. Om inte personal meddelat utpassering vid dagens

slut så kontrolleras att besökarna lämnat anläggningen. Det finns ingen koppling mellan loggbok och övriga larmsystem. Detta innebär att inget larm initieras från loggboken. Även linjearbeten, röjningar och markarbeten på stationer noteras i loggboken. Alla tre operatörsplatserna på driftcentralen använder samma loggbok och antalet noteringar kan variera mellan någon enstaka upp till ett tjugotal per dag.

Äldre larm och händelser lagras i ett separat system, den så kallade "Banken". Där lagras larm och händelser i tidsordning i en textfil. "Banken" är alltså ingen riktig databas, vilket gör att det inte enkelt går att erhålla all information om en specifik anläggning.

## 2.7 Aktiviteter riktade mot ställverk

Vad beträffar terrorister så föreligger enligt så väl Svenska Kraftnät som SÄPO inga kända hotbilder. Polisen anses dock ha relativt låg kunskap om hoten mot elproduktion och eldistribution och prioriterar inte denna typ av skyddsverksamhet. I ett längre perspektiv kan dock inte terroristattacker helt uteslutas, även om det inte föreligger någon känd hotbild.

Bland de aktiviteter som hittills riktats mot ställverk i Sverige finns inga av typen terroristhandlingar eller försök till sabotage. 1998 utsattes stamnätet i Jämtland för ett sabotage, två parallella ledningar sprängdes men det påverkade inte driften.

Vad som främst har förekommit är inbrott, klotter och några mer eller mindre medvetna intrångsförsök. Inbrott sker främst vid ombyggnadsarbeten. Det förekommer även att stölder av viktiga komponenter ger upphov till avbrott i elförsörjningen.

Det är av speciell vikt att säkerställa så att barn, äldre och förståndshandikappade personer inte kan ta sig in anläggningarna. Detta eftersom anläggningarna är farliga platser att uppehålla sig på.

## 2.8 Ekonomiskt relaterade aspekter

System för intrångsskydd har flera ekonomiska konsekvenser. Generellt gäller att personalkostnaderna är de som utgör den största kostnaden för övervakning och skydd av anläggningarna. Kostnaderna för avbrott i elförsörjningen varierar kraftigt mellan olika anläggningar. De stora kostnaderna för detta drabbar dock inte Svenska Kraftnät, utan drabbar den del av samhället som el-försörjs genom ställverket.

## 2.9 Slutsatser

Ur de gjorda intervjuerna har följande slutsatser dragits, vilka sammanfattar de synpunkter som framkommit under intervjuerna.

- Det finns idag inga kända, antagonistiska hot mot Svenska Kraftnäts anläggningar. Sabotage för att skada tredje man har dock förekommit.
  - Stölder av material vid och klotter på anläggningarna är kostsamma.
  - Barn, samt äldre och förvirrade personer måste skyddas från att skada sig på anläggningen.
- Polisen prioriterar idag inte skydd av denna typ av anläggningar. I flera områden ingriper vare sig polisen eller brandmyndigheter utan direkt, visuell verifiering av hot. Dessutom måste polisen vid insats släppas in i anläggningarna av behörig personal. Kameran system för fjärrverifiering bör kunna korta tiden för insats väsentligt.
- Uppgiften för ett övervakningssystem på anläggningar är flerfaldig och varierande.
  - Förutom skydd mot obehöriga bör systemet kunna användas för att säkerställa att anläggningens personal inte har råkat ut för olyckor.
  - Sensorer som installeras för övervakning ska också kunna användas för drift och brandövervakning. Samutnyttjande är viktigt, inte minst av ekonomiska skäl.
  - Det finns önskemål om att kunna kontrollera att stängsel är hela.

- Övervakningssystemet måste hantera att personer vid anläggningen inte anmäler sig på korrekt sätt till driftcentralen, att vissa anläggningar enbart har nyckellås samt att det förekommer att grindar till områdesskyddet lämnas öppna och obevakade.
- Svenska Kraftnät har gjort gedigna studier av olika slags sensorer för intrångsskydd. Det kvarstår dock att utreda hur sensorinformationen vid anläggningar ska användas för att generera larm, hur och vilken information som ska sändas över till driftcentralen vid olika situationer, samt hur den ska presenteras för operatörer.
  - Om sensorer för övervakning för intrång, drift och larm ska samutnyttjas, måste hänsyn tas till det när de placeras på anläggningarna.
  - Systemet får inte generera för många falsklarm. Detta kan hanteras av redundans avseende sensorer och bättre metoder för att väga samman information från flera sensorer.
- System för bättre hantering av larm i driftcentralen efterfrågas. Detta behövs för att ge operatören bättre möjligheter att identifiera orsaken till larm. Bland annat bör larm tidsstämplas vid uppkomsten i anläggningen snarare än när de anländer till driftcentralen.
- Samtidigt som sensorer ska kunna användas till flera olika saker så får beslutsstöds-systemet för övervakning på driftcentralen inte konkurrera med driftövervakningen. Därför måste det nya beslutstödssystemet vara separerat från driftövervaknings-systemet. Systemets olika tillämpningar gör däremot sensorsystemet måste kunna styras både från driftövervakningssystemet och ifrån beslutstödssystemet.
- Inga hinder för ökad övervakning finns i form av integritetshänsyn till personalen.
- De största kostnaderna förknippade med avbrott i elförsörjningen är samhälls-ekonomiska.
- System för intrångsskydd, där övervakning sker enbart av området inne på ställverks-området, har små möjligheter att tillräckligt tidigt upptäcka attacker. Skydd mot attacker kräver system med förmåga att upptäcka och verifiera potentiella hot och måste kunna användas för att analysera aktiviteter utanför anläggningarnas staket. Händelser vid en anläggning måste kunna analyseras med händelser vid andra anläggningar och tillsammans med underrättelser från externa källor.

### 3. Problemidentifiering

Detta kapitel beskriver några olika händelser som är intressanta att upptäcka vid övervakning av området runt en skyddsanläggning. Händelserna beskrivs tillsammans med förslag på en lösning som tar upp de sensorer, den signalbehandling och den situationsanalys som kan användas för att hantera händelserna. Tanken är inte att dessa händelser direkt behöver ge upphov till larm, men att kombinationer av dessa händelser är viktiga att upptäcka och analysera för att få förvarning om potentiella intrång i en skyddsanläggning. Eventuella åtgärder som användarna ska utföra vid larm eller andra meddelanden diskuteras inte i detta kapitel.

Vissa sensorer som beskrivs har förmåga att samla in data med hög upplösning, som kan användas för att t. ex. känna igen nummerplåtar eller logotyper på fordon, eller för att identifiera individer. Den signalbehandling som beskrivs nedan syftar inte till att identifiera individer, men om data har lagrats kan sådan teknik användas vid ett eventuellt rättsligt efterspel.

Vissa av händelserna initieras av att sensorsystemen som bevakar området runt anläggningen reagerar. Dessa händelser har sorterats i olika problemtyper som kan uppstå på olika avstånd från anläggningens yttre staket, se kapitel 3.1. Vissa händelser som påverkar systemet initieras inte av att sensorsystemen reagerar, utan av att hotbilden för anläggningen höjs baserat på andra informationskällor. Dessa beskrivs i kapitel 3.2. I kapitel 3.3 beskriver vi några exempel på mer komplexa händelser.

#### 3.1. Händelser runt skyddsanläggningen

Området runt skyddsanläggningen har delats upp i tre områden; ett *närområde* som är 0-10 m från anläggningens yttre staket, *tillfartsvägar* till anläggningen vilket avser vägar som endast behöver trafikeras då man ska till/från anläggningen, och ett *fjärrområde* som är 10-100 m från anläggningens yttre staket.

##### 3.1.1. Närområdet

**A. Händelse:** En person går runt större delen av staketet.

**Risker:** Personen förbereder inbrott eller sabotage.

**Lösningsförslag:** Att en person är närvarande kan detekteras med doppler-radar (liknar de system som öppnar dörrar i affärer) eller med kameror. Personen kan följas med kameror i det visuella eller IR-området. För att få mörkerkapacitet med en kamera i det visuella området får man komplettera med belysning eller använda bildförstärkare. IR-kameror har mörkerkapacitet. En magnetometer kan också användas för att detektera personers och fordons rörelser. Geofoner kan användas för detektion och klassificering av gående/springande person eller personer.

Insamlad sensordata behöver analyseras. Till exempel behövs signal- och bild-behandling för att detektera personer och deras rörelser. Även metoder för följning av personens rörelse runt staketet krävs. Med bildalstrande sensorer kan man avgöra storleken på den som rör sig och särskilja människor från djur. Från högupplösande, bildalstrande sensorer kan man följa olika kroppsdelars inbördes rörelser, vilket kan användas för identifiering av en viss person. Det kan tjäna som underlag vid en brottsutredning. Med situationsanalys kan personens rörelser i förhållande till anläggningen analyseras och man kan avgöra om tidpunkten är olämplig.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer och geofoner.

**B. Händelse:** Ett barn befinner sig precis utanför staketet.

**Risker:** Barnet blir nyfiket och försöker komma in på anläggningen.

**Lösningsförslag:** Med bildalstrande sensorer kan man avgöra storleken på den som rör sig och därmed särskilja barn från vuxna och djur. Genom att analysera de ljud från personens rörelser och tal som mikrofoner och geofoner registrerar kan man styrka klassningen av barn/vuxen. För övrigt kan analys ske som i Händelse 1.1.A

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

**C. Händelse:** En person observerar anläggningen med en kamera, kikare eller annat sikte.

**Risker:** Personen förbereder inbrott eller sabotage.

**Lösningsförslag:** Närvaron av en person och dennes rörelser kan avgöras med teknik enligt Händelse 1.1.A. Lasersensorer kan användas för att upptäcka optisk utrustning (kikare etc.).

Signalbehandling av laserdata kan ge detektion samt beräkna riktning och avstånd till personen. Denna information kan sedan kombineras med personens rörelsemönster och med situationsanalys ge en beskrivning av beteende och troliga intentioner.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, geofoner och lasersensorer för siktesdetektion.

**D. Händelse:** En person betraktar anläggningen under en längre tid.

**Risker:** Personen förbereder inbrott eller sabotage.

**Lösningsförslag:** Sensorer och signalbehandling sker enligt Händelse 1.1.A. I situationsanalysen kombineras sensorinformation med förlagrad information om vad som kan betraktas som "onormalt länge". Det ger en beskrivning av beteende och troliga intentioner.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer och geofoner.

**E. Händelse:** En person med ett stort föremål i handen (kan vara ett vapen eller en redskap) befinner sig strax utanför staket och han gör något med föremålet.

**Risker:** Personen förbereder inbrott eller sabotage.

**Lösningsförslag:** Sensorer och dataanalys enligt Händelse 1.1.A används. En magnetometer kan detektera avvikelser i magnetfältet p. g. a. rörelser och även avgöra hur mycket metall som personen har på sig. Ljud från redskap/vapen och personens verksamhet kan analyseras.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

**F. Händelse:** En person befinner sig nära anläggningen på natten eller då inget arbete ska göras på anläggningen (inget arbete är anmält). Detta är troligen bara relevant då anläggningen inte ligger i tätbebyggt område.

**Risker:** Personen har gått vilse, förbereder inbrott eller sabotage.

**Lösningsförslag:** Sensorer och signalbehandling sker enligt Händelse 1.1.A. Detta kombineras med information om arbete som är anmält eller information om tiden på dygnet i situationsanalysen.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer och geofoner.

**G. Händelse:** En eller flera personer kastar in föremål över staketet. Syftet kan vara att försöka orsaka smällar och ljusbågar eller att skada anläggningen.

**Risker:** Anläggningen kan skadas, oavsiktligt eller avsiktligt (underlättar inbrott eller sabotage).

**Lösningsförslag:** Sensorer och signalbehandling sker enligt Händelse 1.1.A. Dopplerradar kan användas för att avgöra storlek och hastighet på inkommande föremål. Analysen av akustiska data ger följning av personernas rörelser och ljudet från det som kastas kan visa vilket material det är gjort av. Signal- och bildbehandling för att följa flera personers rörelser tillkommer. Situationsanalysen behöver utvidgas för att kunna analysera flera personers inbördes förhållanden och gruppens förhållanden i relation till anläggningen.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

### 3.1.2. Tillfartsvägar med nära omgivning

**A. Händelse:** Ett fordon (personbil, lastbil e dy) kör in på tillfartsvägen och tidpunkten är olämplig eller fordonet återkommer flera gånger.

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningsförslag:** Sensorer och signalbehandling enligt Händelse 1.1.A kan användas även här. Mikrofon och geofon kan användas för att mäta fordonets akustiska signatur, vilken kan användas för att klassificera fordonets typ. En magnetometer kan detektera fordonens närvaro. Med flera sensorer kan man följa fordonets rörelser. Optiska sensorer (kameror eller laserradar) kan klassificera fordonen och vid goda förhållanden (bra väder, nära avstånd) läsa av registreringsnumret. Signalbehandling för analys av akustiska data och bildbehandling för bestämning av registrerings-nummer tillkommer. Situationsanalysen utökas för att hantera även dessa informationskällor och att fordon av samma typ återkommer flera gånger.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

**B. Händelse:** Ett fordon parkerar på tillfartsvägen på en plats där anläggningen kan observeras. Ingen person kliver ur och lämnar området.

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningsförslag:** Sensorer och dataanalys enligt Händelse 1.1.A, Händelse 1.1.C och Händelse 1.2.A kombineras. Med en laser kan man se hur många personer som finns i fordonen (även genom mörka fönsterrutor). Situationsanalysen blir mer kvalificerad för att hantera dessa datakällor.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, geofoner, lasersensorer (gated viewing eller 3D-laser).

### 3.1.3. Fjärrområde

**A. Händelse:** Ett fordon stannar på en allmän väg i nära anslutning till ställverket. Bilen är parkerad på ett sätt som gör det möjligt att observera anläggningen, tidpunkten kan vara olämplig, det kan vara flera fordon passerar i tät följd, eller samma fordon återkommer vid flera olika tillfällen under en kortare tidsperiod.

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningsförslag:** Sensorer och signalanalys sker enligt Händelse 1.2.B. Med en tredimensionell karta över anläggningen och dess omgivning kan man identifiera speciella sektorer/platser där riskerna för spaning på anläggningen är större. Situationsanalysen behöver då utökas för att kunna utnyttja sådan information.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer och geofoner. 3D-kartor kan genereras från ritningar, kombination av visuella bilder eller från mätningar med laserradar.

**B. Händelse:** Brand uppstår utanför anläggningen och vinden ligger på mot anläggningen.

**Risker:** Branden hotar anläggningen eller dess skalskydd.

**Lösningsförslag:** En termisk IR-sensor kan indikera en brandhärd, rök-gassensorer kan upptäcka rökutveckling, väderdata kan användas för att kalkylera riskerna att anläggningen berörs. Situationsanalys för att hantera dessa sorters sensorinformation tillkommer.

**Exempel på sensorer:** Termisk IR-sensor, rök-gassensorer, väderstation.

**C. Händelse:** Ett terränggående fordon (kan också vara en snöskoter) passerar. Föraren kan ha kört in och parkerat på ett sätt som gör det möjligt att observera anläggningen, tidpunkten kan vara olämplig eller det kan vara flera fordon som passerar i tät följd.

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningförslag:** Sensorer och signalanalys enligt Händelse 1.3.A fungerar även om det inte finns vägar.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer och geofoner.

**D. Händelse:** En person observerar anläggningen under en längre tid (står still och betraktar anläggningen).

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningförslag:** Sensorer och signalbehandling sker enligt Händelse 1.1.A. Även lasersensorer kan användas för att penetrera delar av terrängen. Mätningar från två olika tillfällen kan användas för förändringsdetektion. Med data från lasersensorer kan volymen på personen (och hans/hennes utrustning) beräknas. Lasersensorer (avståndsmätare, avståndsupplöst avbildning eller 3D-genererande laserradar) ger avstånd och riktning till personen med hög precision. I situationsanalysen kombineras sensorinformation med lagrad information om vad som kan betraktas som "onormalt länge". Det ger en beskrivning av beteende och troliga intentioner.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, geofoner och lasersensorer (gated viewing eller laserradar).

### 3.2. Andra händelser

**A. Händelse:** Säkerheten är höjd för anläggningen, t. ex. beroende på information från polisen eller för att någon ringt in ett bombhot.

**Risker:** Förberedelse av sabotage.

**Lösningförslag:** Sensorer och signalbehandling sker enligt Händelse 1.1.A.

Situationsanalysen tar hänsyn till fler möjliga händelseförlopp när data bearbetas.

Programvaror för visualisering av anläggningen och sensorstatus används regelbundet, kanske en operatör bevakar anläggningen hela tiden.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

**B. Händelse:** Sensorer är ur funktion.

**Risker:** När sensorerna är satta ut spel är det lättare att göra intrång på anläggningen och sätta driften ur spel. Kan vara förberedelse för inbrott eller sabotage.

**Lösningförslag:** Sensorer och signalbehandling, för de delar som fungerar, sker enligt Händelse 1.1.A. Känsligheten i sensorerna kan ökas, med risk för fler falsklarm.

Känsligheten i signalbehandling och/eller situationsanalys kan också ökas. Situationsanalysen analyserar historiska data för att få information om varför sensorerna slutade fungera.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

### 3.3. Kombinationer av händelser

**A. Händelse:** Efter längre tids driftstörningar med långa avbrott, så har de boende i närområdet tappat tåla modet. Dagliga protester i olika former genomförs mot el-bolaget. En större folkmassa rör sig på tillfartsvägen i riktning mot ställverket.

**Risker:** Trafik för underhåll av anläggningen kommer inte fram, demonstrationen kan urarta så att anläggningen eller skyddet av den skadas.

**Lösningförslag:** Sensorer och signalbehandling enligt Händelse 1.1.A och Händelse 1.1.G kan användas. Akustiska sensorer kan detektera att flera personer kommer gående.

Kameror kan användas för att få en helhetsbild, där de akustiska sensorerna ger ett bra stöd för att aktivera andra sensorer när folkmassan rör sig.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

**B. Händelse:** Flera fordon kör i tät följd in på tillfartsvägen.

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningsförslag:** Sensorer och signalanalys enligt Händelse 1.2.A kan användas. Med situationsanalys kan man avgöra om fordonen har ett samstämt uppträdande.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

**C. Händelse:** Ett antal personer befinner utanför anläggningen på en olämplig tidpunkt (natt/oanmälda). Personerna agerar tillsammans (kommer/åker tillsammans, avlöser varandra).

**Risker:** Förberedelse av inbrott eller sabotage.

**Lösningsförslag:** Sensorer och signalanalys enligt Händelse 1.4.A och Händelse 1.2.B kan användas även här. Signalbehandling och situationsanalys för följning av individer tillkommer.

**Exempel på sensorer:** Doppler-radar, kameror verksamma i det visuella eller IR-området, magnetometer, mikrofoner och geofoner.

## 4. Sensorer för intelligent övervakning

De sensorer som nämnts i föregående kapitel beskrivs här något utförligare. Alla sensorer har fördelar och nackdelar, men med en kombination av sensorer kan man ofta få ett system där nackdelar hos en sensor delvis vägs upp av en annan.

I avsnitt (4.1) beskrivs sensorerna. Att beskriva en sensor fullständigt är mycket svårt. Beskrivningarna här är inriktade mot att sensorerna ska sitta utomhus, bevaka ett område utomhus och helst fungera utan alltför mycket underhåll under en lång tid. Sensorerna beskrivs kortfattat nedan, mer information finns i referenserna [Wiss & Kindvall, 2002] och [Jungert & Lantz, 2006]. Följande sensorer är jämförelsevis billiga i inköp och drift: doppler-radar, TV-kamera, magnetometer, mikrofon och geofon. En IR-kamera är dyrare i inköp än en TV-kamera. En IR-kamera och en optikspaningslaser ligger ungefär i samma prisläge. System för pulsstyrd avbildning (eng. gated viewing) är enklare och billigare än fullt 3D-avbildande lasersystem. Priserna på skannade, 3D-avbildande lasersystem sjunker dock nu när fler och fler civila tillämpningar kommer.

Alla sensorer har begränsningar i sitt utbredningsområde/synfält. Bildalstrande sensorer ser inte genom väggar, vissa sensorer kan "höra" runt hörn medan andra kan störas av metallkonstruktioner på anläggningen. Placering av sensorer med hänsyn till deras förmågor och begränsningar diskuteras i avsnitt (4.2).

I avsnitt (4.3) föreslås några exempel på sensorsystem, där flera sensorer kombineras, i olika prislägen. De olika sensorkombinationerna har olika förmåga. Alla sensorer har tillfällen då de fungerar sämre, till exempel nattetid eller vid extremt väder som stormar. Här får man göra en avvägning om man accepterar sämre täckning vid vissa tillfällen och kanske få komplettera med personal vid vissa tillfällen. Alternativet är att ha många sensorer, både av samma och av olika typer, för att få ett robust och redundant system. Detta innebär att sensorsystemet vid anläggningen blir dyrare. Behovet av robusthet och redundans i sensorsystemet bör vägas mot anläggningens utsatthet och vilka konsekvenser ett driftsavbrott får.

### 4.1 Beskrivning av sensorerna

Sensorerna beskrivs nedan i deras förmåga att operera vid olika väder och tider på dygnet, deras förmåga till yttäckning respektive precision. Med precision menas noggrannhet i vinkelangivelse i sidled och/eller höjddled. Vissa sensorer, speciellt radar- och laserbaserade, har förmågan att penetrera glesa strukturer som vegetation och buskage. Vissa sensorer kan även "se" genom fönsterglas eller tunna väggar. Dessa sensorer sägs ha en penetrationsförmåga, vilket beskrivs nedan.

#### **Dopplerradar**

Den här typen av dopplerradar är en enkel radarsensor som jobbar inom frekvensområdet 9-10 MHz. Den används i sin enklaste form bl. a. för dörröppning i varuhus. Sensorn registrerar rörelser.

**Väderkänslighet:** Fungerar i de flesta vädersituationer.

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Sensorn har bra yttäckning och långa detektionsavstånd är möjliga. Hög känslighet erhålls i mätningen, t. ex. kan man registrera en bröstorgs rörelser på grund av andningen. Med en sensor blir vinkelprecisionen inte så bra, används flera sensorer förbättras den.

**Penetrationsförmåga:** Kan penetrera buskage/skog, fönsterglas och bilrutor, samt till viss del bilchassin. Vissa konfigurationer kan även mäta genom väggar.

#### **Magnetometer**

Människor och fordon alstrar elektriska och magnetiska fält, som kan användas för att avslöja deras närvaro. En magnetometer mäter de förändringar i det magnetiska fältet. Magnetometrar har testats av Svenska Kraftnät, [Nastell, 2002].

**Väderkänslighet:** Sensorn fungerar vid de flesta väder. Det behövs automatisk omkalibrering av sensorn om bakgrundsbruset ändras (pga ändrat väder).

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Yttäckningen och precisionen beror på det magnetiska materialets storlek och magnetiseringsgrad. Till exempel kan handhållna vapen detekteras på 2 m och en personbil på ca 10 m.

**Penetrationsförmåga:** Icke-magnetiska material kan penetreras.

### **Mikrofon**

Mikrofonerna som avses här mäter vibrationer i mark och luft, som t. ex. genereras när någon går, talar, eller av en bilmotor. Akustisk sensorkabel har testats av Svenska Kraftnät, [Nastell, 2002].

**Väderkänslighet:** Varje modell har en väderprofil som visar specifik påverkan av vind, regn, snö och övrigt annat.

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Yttäckningen är god och precisionen kan bli hög om sensordelen består av flera mikrofoner. Detektionsavstånd på upp till 2 km för fordon har noterats.

**Penetrationsförmåga:** Kan penetrera buskage/skog och andra glesa strukturer.

### **Geofon**

Geofoner mäter vibrationer i marken, som t. ex. genereras när någon går, kör eller flyger i närheten av sensorn.

**Väderkänslighet:** Geofoner påverkas av regn, tjäle, markens beskaffenhet, rötter och stenar i marken. Man bör analysera markområdet där sensorerna ska placeras.

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Yttäckningen är god och precisionen kan bli hög om sensordelen består av flera geofoner. Detektionsavstånd på upp till 50m för en person och 2 km för fordon har noterats.

**Penetrationsförmåga:** Beroende på markegenskaper

### **Kamera verksam i det visuella området**

En (vanlig) kamera mäter reflektionen av naturlig strålning (solljus). TV-kameror har testats av Svenska Kraftnät, [Nastell, 2002].

**Väderkänslighet:** Räckvidden försämras vid t. ex. dimma och regn, men på dess korta avstånd (upp till 100 m) kan man nog ofta erhålla en acceptabel bild.

**Dygnskapacitet:** En vanlig kamera kräver dagsljus, om den ska användas i mörker måste man komplettera med belysning eller använda en ljusförstärkare (bildförstärkare). Nya typer av kameror med förbättrad mörkerkapacitet har nyligen introducerats på marknaden, de kommer att utvärderas av FOI under 2007.

**Yttäckning och precision:** Sensorn har bra yttäckning och precision

**Penetrationsförmåga:** Penetrationsförmågan är dålig.

### **Kamera verksam i IR-området**

Här avser vi en IR-kamera (värmekamera) som mäter den termisk emitterade infraröda strålningen som olika objekt avger. Det innebär att varma ytor/objekt syns tydligt mot en kallare bakgrund (och tvärtom). Upplösningen är inte lika bra som för visuella kameror. Termiska IR-kameror har testats av Svenska Kraftnät, [Nastell, 2002].

**Väderkänslighet:** Räckvidden försämras vid t. ex. dimma och regn, dock inte lika mycket som för visuella kameror. På korta avstånd (upp till 100 m) kan man nog ofta erhålla en acceptabel bild.

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Sensorn har bra yttäckning och precision.

**Penetrationsförmåga:** Penetrationsförmågan är dålig.

### **Optikspaningslaser**

När en laserstråle träffar optiken i en kamera, kikare eller liknande, reflekteras en del i frontytan och ibland även från inre delar i det optiska systemet. Retroreflektion, även kallad kattögereflektion,

innebär att en del av strålningen reflekteras tillbaka i exakt samma riktning som den inkommande och kan därför detekteras på långt avstånd. Denna effekt utnyttjas i en optikspanare.

**Väderkänslighet:** Räckvidden försämras vid t. ex. dimma och regn. På dess korta avstånd (upp till 100 m) bör man under de flesta omständigheter kunna ha full täckning.

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Sensorn har bra yttäckning, precision och långa detektionsavstånd är möjliga.

**Penetrationsförmåga:** Kan penetrera buskage/skog och andra glesa strukturer.

### **Pulsstyrd avbildning och 3D-avbildande lasersensor**

För att få avståndsinformation i en bild kan man komplettera en passiv sensor med en belysningskälla, vanligen en laser. Avståndsinformationen genereras antingen med pulsstyrd avbildning eller med full 3D-avbildning. Båda sensorsystemen brukar kallas *laserradarar*. Genom att använda en pulsad laser som belyser målet och synkronisera laserpulserna till en bildalstrande mottagare kan ett valbart avståndsintervall registreras. Den här tekniken kallas avståndsgrindad eller pulsstyrd avbildning (eng. gated viewing). Genom att lösa upp avståndsinformationen i horisontell och vertikal led över bilden, erhålls en 3D-avbildning av scenen. Den kommersiellt vanligaste tekniken är att skanna en laseravståndsmätare över scenen, för varje mätning erhålls 3D-värden till ett bildelement. Avbildningen byggs upp bildelement för bildelement under några mikrosekunder-sekunder. Det finns nya system under utveckling där man mäter med en bred laserpuls över hela scenen och en ny sorts mottagardel i laserradarn bygger upp hela 3D-bilden från en mätning. Dessa system kommer att kunna generera en 3D-bild på nanosekunder. Båda teknikerna gör att föremål på ett visst avstånd från sensorn avbildas och effekter från objekt, dimma, dis och rök från andra avstånd undertrycks.

**Väderkänslighet:** Räckvidden försämras vid t. ex. dimma och regn, dock i regel bättre än visuella/IR-sensorer. På korta avstånd (upp till 100 m) kan man nog ofta erhålla en acceptabel bild.

**Dygnskapacitet:** 24h

**Yttäckning och precision:** Denna sensor har bra precision eftersom den har hög upplösning. Den höga upplösningen innebär att då stora ytor söks av så skapas mycket data. Om man sänker upplösningen på sensorn kan den även klara yttäckande arbete utan att stora datamängder genereras.

**Penetrationsförmåga:** Sensorn kan penetrera buskage/skog och andra glesa strukturer. Det är också möjligt att ”se” igenom fönsterglas, t. ex. tonade bilrutor.

### **Väderstation**

En väderstation registrerar vindstyrka, vindriktning, luftfuktighet och lufttryck under dygnets alla timmar. Data från en väderstation kan användas för att välja de sensorer som fungerar bäst under rådande förhållanden. Den kan också användas som stöd för att avgöra tillförlitligheten i data från en viss sensor.

## **4.2 Placering av sensorer**

Den miljö som sensorerna placeras i är i högsta grad tredimensionell; byggnader, ställverk, master och annat begränsar synfält eller ger svårare utbredningsförhållanden. Om man verkligen vill optimera antalet sensorer och deras överlapp i synfält bör man ha tillgång till en 3D-beskrivning av anläggningen. Det kan också finnas delar på anläggningen som stör sensorerna, till exempel kan vissa radarsensorer ge falska detektioner för stora metalltytor, en termisk IR-sensor detekterar även skillnader temperatur hos strömförande delar och glasrutor kan ge reflexer i bildalstrande sensorer. En fördel med att ha sensorerna fast monterade i en fast anläggning, är att man kan detektera dessa artefakter i sensordata och kompensera för dem i sensordataanalysen.

### 4.3 Exempel på sensorsystem

Nedan beskrivs några exempel på kombinationer av olika sensorer till ett sensorsystem. Det första systemet är enkelt och med liten redundans, sedan följer mer komplicerade och dyrare system. Det är givetvis möjligt att kombinera sensorerna på andra sätt än de som beskrivs nedan. Vilka sensorer som ska användas, hur de ska placeras, behovet av överlapp i synfält och redundans måste anpassas till den anläggning som ska bevakas.

#### **A. Dopplerradar och kamera verksam i det visuella området**

Detta system består av två relativt billiga sensorer. Radarsensorn kompletterar kameran genom att vara mer robust mot väder och tid på dygnet. Med kameran kan man verifiera de detektioner som radarn gjort och förbättra riktningbestämning och klassificering. Radarsensorn kan ha ett större utbredningsområde än kameran, och utifrån detektioner i radardata kan kameran visas in mot det intressanta området.

#### **B. Dopplerradar, magnetometer, akustiska sensorer och kameror verksamma i både det visuella och IR-området**

Detta system innehåller mer redundans och är mer robust. Dopplerradarn, magnetometern och IR-kameran fungerar dygnet runt i del flesta väder medan den akustiska sensorn är mer väderkänslig och den visuella kameran behöver dagsljus eller en strålkastare. Den akustiska sensorn och kamerorna har god precision och klassificeringsförmåga. Den visuella kameran kompletterar IR-kameran genom att ha högre upplösning. Det är möjligt att detektera människor och fordon med samtliga sensorer.

#### **C. Dopplerradar, kameror, magnetometer, akustiska sensorer, och 3D-avbildande lasersensorer**

Detta system innehåller ännu mer redundans och robusthet. Dopplerradarn, magnetometern, IR-kameran och laserradarn fungerar dygnet runt i del flesta väder medan den akustiska sensorn är mer väderkänslig och den visuella kameran behöver dagsljus eller en strålkastare. Den akustiska sensorn, kamerorna och 3D-lasern har god precision och klassificeringsförmåga. Djupinformation kan erhållas från den akustiska sensorn och laserradarn. Det är möjligt att detektera människor och fordon med samtliga sensorer.

## 5. Dataanalys för intelligent övervakning

I detta systemkoncept kommer data från sensorer och andra informationskällor att analyseras i flera steg, där varje steg innebär en successiv förädling av analysresultatet. Förädlingen av sensordata och annan information kallas datafusion, [Hall & Llinas, 2001]. Datafusion är en process för att sammanställa data från olika källor och/eller tidpunkter i syfte att skatta eller förutsäga tillståndet hos någon bestämd del av omvärlden. Det vanligaste exemplet på datafusion är då det används för att sammanställa data från olika sensorer för att skatta eller förutsäga fordons eller människors positioner eller typ. I detta kapitel beskrivs vad de olika förädlingsstegen i datafusionsprocessen innebär i FOIs koncept för intelligent övervakning för skyddsanläggningar.

Datafusionsprocessen brukar delas upp i olika steg, där varje steg också motsvarar en viss abstraktionsnivå, se [Hall & Llinas, 2001]. I Tabell 1 visas de olika nivåerna i datafusionsprocessen tillsammans de modifierade benämningar som gjorts för denna tillämpning. Det som traditionellt kallas situationsbedömning har här delats upp i två delar, där händelseanalys innehåller analys som sker automatiskt vid anläggningen medan det som kallas situationsanalys är analys som sker vid en bemannad central, t. ex. en driftcentral, som bevakar flera anläggningar. Datafusionsprocessen togs ursprungligen fram för militära tillämpningar, varför nivå 3 i andra sammanhang kallas för hotbedömning. I fallet med skydd av anläggningar är termen konsekvensanalys mer adekvat.

*Tabell 1: De olika nivåerna i datafusionsprocessen (vänster) och de modifierade benämningarna för detta system (höger).*

Nivå	Namn enligt [Hall & Llinas, 2001]	Namn i detta system
1	Objekt assessment	Sensordataanalys
2	Situation assessment	Händelseanalys Situationsanalys
3	Impact assessment	Konsekvensanalys
4	Process refinement	Sensorstyrning

### 5.1 Sensordataanalys

Syftet med sensordataanalysen är att få fram så mycket information som möjligt ur sensordata för att skapa ett bra underlag för fortsatt analys. Den information sensordataanalysen genererar beskriver de objekt som är intressanta att övervaka i den aktuella tillämpningen, i detta fall människor eller fordon. Det rör sig om information knuten till objektens positioner, rörelse, attribut och identitet. Målet är att skapa en systemgemensam, utförlig och noggrann beskrivning av alla objekt. Denna beskrivning ska innehålla så många relevanta egenskaper och attribut hos objekten som möjligt, med så liten osäkerhet som möjligt. Bra information om objektens tillstånd ger goda möjligheter att genomföra resonemang om objektens relationer till varandra. Det möjliggör också förutsägelser av händelser och deras konsekvenser, vilket är grunden för tidig förvarning.

De data som sensorerna producerar behöver analyseras och förädlas innan de skickas vidare till nästa steg i förädlingsprocessen, händelseanalysen. I kapitel 3 kan man se att några olika förmågor kommer att krävas av sensordataanalysen för att producera den information som gör händelse- och situationsanalys möjlig. De förmågor som krävs är att:

- Upptäcka och positionera personer och fordon i respektive sensor. Varje upptäckt objekt tilldelas en unik identifierare av systemet.
- Följa personers och bilers rörelser i enskilda sensorer och mellan olika sensorer, då fordon eller människor rör sig mellan olika sensorers täckningsområden.
- Bestämma relevanta egenskaper och statusvärden hos objekt, t. ex. dess färg och storlek.
- Väga samman osäker information om objekten från olika sensorer till säkrare och mer komplett information.

- Avgöra om det är samma objekt som observeras av flera olika sensorer eller vid olika observationstillfällen, s.k. association.
- Särskilja vuxna, barn och djur. Vuxna och barn kan endast särskiljas genom deras storlek.
- Upptäcka och positionera kameror och kikare.

Beroende på aktuella intressenters specifika krav kan även andra förmågor vara aktuella.

Förmågor som kan inkluderas, men inte är en del av detta konceptförslag, är att:

- Känna igen olika fordonstyper (lätt personbil, tung personbil, lastbil, traktor, etc.). För en sådan förmåga krävs metoder för matchning mot bibliotek med lagrade referenssignaturer.
- Bestämma objektens momentana beteende, dvs. bestämma vad objektet gör under ett kort tidsintervall. Detta kan vara starkt korrelerat med objektets rörelse, t. ex. kan beteenden som ”springer”, ”går” och ”kastar” vara relevant att kunna bestämma.

För att uppnå dessa förmågor krävs utveckling av metoder för association, följning och klassificering utgående från sensordata. Beroende på specifika krav, kan metoder för beteendebestämning i sensordata krävas. En del av dessa metoder är specifika för respektive sensor medan andra är mer generella. Uppräkningen av förmågor ovan är gjord i stigande svårighetsgrad med avseende på de metoder som måste användas för att uppnå förmågan. Förutsatt bra sensordataunderlag är de första förmågorna lättare att uppnå än de sista. Sensordataanalysen sker i två steg; ett steg där analys sker för varje enskild sensor och ett annat steg där sammanvägning sker. Uppgiftsfördelningen mellan dessa två steg är en praktisk fråga som avgörs under projektets gång. Sensordataanalysen är en automatisk process.

## 5.2 Händelseanalys

Händelseanalys är den analys som sker för att bestämma vilka händelser som inträffar runt anläggningen och är det steg i datafusionsprocessen som följer efter sensordataanalysen. Den ger svar på frågorna vem, vad, hur och när. Mer formellt beskriver en händelse den aktivitet som utförs, den aktör som utför aktiviteten, den plats aktiviteten utförs på (i respektive anläggning) och det tidsintervall aktiviteten utförs. Händelsens aktör beskriver vilket objekt som är inblandat (dess unika systemidentifierare) tillsammans med dess klassificering. Aktiviteten beskriver objektets beteende, rörelse och position över tiden och i förhållande till anläggningen. Exempel på aktiviteter är ”fotograferar anläggningen”, ”observerar anläggningen” eller ”går runt staketet”.

Händelseanalys är en grundläggande förutsättning för intelligent övervakning. Detta gäller speciellt då övervakningen ska ske i områden där människor och fordon kan röra sig relativt fritt. Många övervakningssystem idag bygger sin varningsstrategi på enkla regler som låter systemet varna då ett objekt befinner sig i en viss sensors täckningsområde. En sådan strategi är inte tillräcklig då människor kan ha legitima skäl att befinna sig i sensorernas täcknings-områden. I detta fall måste övervakningssystemet ha en förmåga till att bedöma objektets typ och aktivitet noggrant innan varning kan utfärdas. Det kan också vara viktigt att systemet kan agera olika i olika delar av en sensors täckningsområde. Detta gäller speciellt i de fall där en sensor samtidigt täcker delar av anläggningen som är väsentligt olika i något avseende, t.ex. då en sensor täcker ett område både innanför och utanför ett staket. Syftet med händelse-analysen är att skilja de händelser som verkligen är intressanta att uppmärksamma från normala händelser och därmed möjliggöra en mer flexibel hantering av människor och fordon i övervakade områden.

Händelseanalysen har förmåga att:

- Bestämma var i relation till anläggningen objekten befinner sig, t. ex. utanför staketet eller innanför staketet. Detta avgör händelsens plats.
- Bestämma objektets rörelse och beteende i förhållande till anläggningen.
- Bestämma objekts rörelse och beteende över längre tidsperioder, dvs. bestämma deras aktiviteter.

- Bestämma vilka objekt som kan höra samman. Med detta avses att bestämma vilka människor som tillhör ett visst fordon, samt att bestämma vilka individer som rör sig som en grupp vid anläggningen.
- Bestämma vilka viktiga händelser som inträffat.
- Bestämma vilka enskilda händelser, eller sammansatta händelser, som ska ge upphov till larm eller meddelanden och vilka som inte ska det.

I händelseanalysen hanteras även viss information från andra källor än sensordataanalysen. I första hand gäller detta information om anläggningens geometri, dvs. huvudsakligen en karta över anläggningen. Ett annat exempel gäller tidsinformation som används för att, tillsammans med sensorinformation, kunna avgöra om det är rimligt med ett besök vid en viss tidpunkt. Alla händelsebeskrivningar levereras tillsammans med ett mått på hur trolig händelsen är. Detta anges i kvalitativ form, t. ex. som ”troligt”, ”mindre troligt” och ”inte troligt”. Osäkerheterna från sensordataanalysen sammanställs på ett korrekt sätt.

Händelseanalysens förmåga att avgöra om det kan vara samma objekt som observerats vid olika tillfällen kräver att metoder för association finns tillgängliga. Grundantagandet är att association ska göras i sensordataanalysen, men frågan om ny association måste göras eller inte är en praktisk fråga. Detta beror bl. a. på hur lång tid det är mellan tillfällena då objektet observeras. Dess förmåga att bestämma vilka objekt som hör samman kräver att metoder för aggregering finns tillgängliga.

Det är inte säkert att allt som händer vid anläggningen kan kännas igen och kategoriseras av systemet. Vissa händelser kommer istället att kategoriseras som ”okända händelser”. Dessa händelser kan sedan analyseras mer utförligt av en för ändamålet lämpad användare. Exakt vilka händelser som systemet ska klara att känna igen diskuteras i kapitel 7. Händelseanalysen sker automatiskt efterhand som sensordataanalysen levererar information. Då analysen bedömer att en händelse inträffar innebär detta att sensordata lagras och görs tillgänglig för djupare analys vid behov. Dessa data raderas senare om händelsen inte resulterar i ett larm eller annat meddelande en användare.

### 5.3 Situationsanalys

Situationsanalysens uppgift är att hjälpa användaren att snabbare och bättre kunna bedöma den aktuella situationen. Uppgiften gäller också att bestämma den totala situationen för flera (eller alla) anläggningar sedda tillsammans. Utgångspunkten för stödet är de händelser som utspelat sig, relevanta underrättelser och systemets kunskap om samband mellan inträffade händelser och olika situationer.

En beskrivning av situationen är, precis som en beskrivning av händelser, en beskrivning av de aktörer, aktiviteter, platser och tidsintervall som utspelar sig. Situationsanalysen skiljer sig emellertid på några punkter ifrån händelseanalysen. För det första är situationsanalys en process som utförs endast då användaren kräver detta och som kan styras av användaren.

Händelseanalysen är en automatisk process där användaren inte har möjlighet att påverka den analys som utförs. För det andra är händelserna sammanställda till en beskrivning som är lämplig för snabba säkerhetsanalyser. Till exempel skulle händelserna ”X går (nu) runt anläggning A” och ”X fotograferade anläggningen (föret)” kunna sammanställas till situationen ”Y spanar mot anläggning A”. För det tredje tas i situationsanalysen hänsyn till underrättelser, en längre tidsperiod (flera dagar, veckor eller t. o. m. månader) och till flera anläggningar.

Det exakta innehållet i situationsbeskrivningen måste avgöras i samråd med användarna, men situationsanalysen har förmåga att hjälpa användaren att bedöma:

- Om någon aktivitet pågår vid anläggningarna eller inte.

- Typen av aktivitet, dvs. om normal aktivitet pågår eller om någon avvikelse i form av inbrott, obehörig vistelse vid anläggning, spaning eller sabotage pågår. Med obehörig vistelse menas t. ex. situationer där barn eller förvirrade personer tagit sig in på anläggningen.
- Typen av aktör, dvs. om det gäller grupper eller enskilda, barn eller vuxna.
- Vilken anläggning som hotas. Vid behov kan man identifiera den speciella del av anläggningen som situationen gäller.
- Tidsintervallet då aktiviteten inträffar, inträffade eller (möjligen) är på väg att inträffa.
- Om situationen är känd eller okänd. Situationen bedöms som okänd i de fall händelser som inträffar är okända eller då situationsanalysen bedömer att någon väsentlig situation pågår vid anläggningen, men inte kan avgöra vilken det är.

Det är svårt att skilja på vissa typer av aktiviteter och aktörer med hjälp av enbart den sensorinformation som insamlats. I många fall är det underrättelseinformation och kännedomen om anläggningen som bidrar till att bedöma att den ena situationen är mer trolig än den andra. Alla situationsbeskrivningar levereras tillsammans med ett mått på hur trolig situationen är. Osäkerheterna från händelseanalysen sammanställs på ett korrekt sätt. Den väsentligaste skillnaden mellan metoder för situationsanalys gentemot metoder för händelseanalys är att metoder för situationsanalys måste kunna hantera en mycket större mängd information. Samtidigt finns inget krav på att situationsanalys ska göras automatiskt, kontinuerligt och i realtid, varför resultatet av analysen kan tillåtas dröja något.

Situationsanalysen ska, som tidigare nämnts, också kunna hantera vissa underrättelser. Källor till underrättelser är – trots sitt namn – inte begränsat till poliser. Det kan lika gärna röra sig om någon anställd eller en privatperson som observerat något av intresse för övervakningen av anläggningarna. Underrättelserna måste matas in i systemet av en lämplig användare. En underrättelse kan innehålla en lång rad olika typer av information och kan vara utformade på en rad olika sätt. Det finns ingen möjlighet för systemet att kunna analysera alla former av ostrukturerad information som en underrättelse kan innebära. De underrättelser som situationsanalysen kan analysera är strukturerad information av två olika typer. För det första finns underrättelser om en händelse som inträffar och om dess trolighet. Med andra ord kan i detta fall underrättelseinformation ses som en parallell källa till händelseinformation. Detta underlättar tolkning och hantering av underrättelserna. Detta kan vara samma typ av händelser som händelseanalysen hanterar, men det kan också vara andra händelser. T. ex. bör information om en stulen bil ses som en underrättelsehändelse. Bedömningen av troligheten av underrättelsen måste göras av den användare som matar in händelsen i systemet. För det andra får man via underrättelser information om den allmänna hotbilden mot olika anläggningar eller mot dess kunder. Detta påverkar också analysen av situationen genom att troligheten av att vissa situationer ska uppkomma ökar då hotbilden ökar. Specifika hot mot en viss anläggning ses i detta sammanhang som en lokal ökning av hotbilden mot denna anläggning.

Underrättelser kan också innehålla mer specifik information om t.ex. olika aktörers kapacitet, vilka aktörer som agerar i olika områden och hur vanligt det är att olika händelser leder till en viss situation. Situationsanalysen kommer dock inte att kunna analysera denna typ av information automatiskt, men den kan påverka situationsanalysen på lång sikt genom förändring av systemets kunskapsdatabaser.

Det är systemets kunskap om sambandet mellan aktören, anläggningen och aktiviteten å ena sidan och situationen å andra sidan som avgör hur händelser ska tolkas. Vid utveckling av situationsanalysen måste alla relevanta samband utredas. Dessutom måste styrkan i sambandet utredas. Med detta avses att bedöma hur troligt det är att en viss situation uppstår, givet de händelser som kan inträffa. Förhandskunskap om t. ex. de aktörer som rör vid en anläggning, om hur ofta en viss situation uppstår eller om vid vilka tider en situation normalt uppstår kan utnyttjas.

Systemets förmåga att dra slutsatser om situationen försvåras av att det finns samband som inte är kända vid utvecklingstillfället och av att datainsamling och analys kan vara otillräcklig för att identifiera alla relevanta händelser. Problemet med okända samband kan åtgärdas med automatisk inläring av samband, men detta ingår inte i detta systemkoncept.

## 5.4 Konsekvensanalys

Konsekvensanalysens uppgift är att hjälpa användaren att förstå konsekvensen av olika situationer. Den ger alltså stöd till att bedöma konsekvensen av de situationer som situationsanalysen resulterat i, dvs. situationer där aktiviteten rör inbrott, sabotage, etc.. Beroende på ambitionsnivå kan detta vara både triviale och mycket svårt. Om analysen begränsar sig till konsekvensen för anläggningen, är konsekvensen av olika händelser och situationer i många fall uppenbar. Att sabotage medför att anläggningen riskerar att skadas är självklart. Konsekvensanalysen kan ge stöd till mer kvalificerad bedömning av konsekvenser. Anledningen till att konsekvensanalys behövs är att det kan t.ex. vara svårt att bedöma alla konsekvenser av ett sabotage. Vad är egentligen risken att en viss typ av sabotage leder till ett elavbrott? Vilka kommer i så fall att drabbas? Hur hårt kommer de att drabbas? Det exakta innehållet i konsekvensanalysen för detta systemkoncept kommer att bestämmas i samråd mellan FOI och aktuella intressenter och specificeras inte i denna rapport. Ett viktigt skäl till detta är att konsekvensanalysen kan komma att hantera känslig information.

Utgångspunkten för konsekvensanalysen är resultatet av situationsanalysen, samt relevanta underrättelser och systemets inbyggda kunskap. Avsikten är att konsekvensanalysen ska stötta användarens bedömning av konsekvenser givet exempelvis kunskap om:

- Det finns några speciella kunder till anläggningen som drabbats av ett elavbrott.
- Hur stort område eller hur många kunder som drabbas av ett avbrott.
- Det finns personal i närheten av anläggningen.
- Det finns något speciellt att stjäla eller skada vid en anläggning, t. ex. om stöldbegärligt material för ombyggnad eller reparation finns vid anläggningen.
- Hur lång tid det tar att ersätta distribution eller produktion på olika anläggningar.
- Olika aktörers kapacitet och inställning.
- Det område anläggningen är belägen i.

Tanken är att all information som är relevant automatiskt ska göras enkelt tillgänglig för användaren då en situation uppkommer vid en anläggning. Med hjälp av denna information ska användaren själv kunna bedöma eventuella konsekvenser. I sin enklaste form sker detta genom att relevanta dokument hittas och görs enkelt tillgängliga för användaren. Vilken information som kan göras tillgänglig i systemet beror på vilken information ägaren av systemet anser vara lämplig att ha tillgänglig på detta sätt.

Konsekvensanalysen kommer dessutom att ge stöd för bedömning av hur allvarlig en konsekvens är, i fortsättningen kallad konsekvensnivå. Detta rör sig om en översiktlig bedömning som presenteras tillsammans med relevant information. En sådan bedömning måste ske i samverkan mellan FOI och aktuella intressenter. FOI bidrar i första hand med en metod för att bedöma och gradera konsekvensnivån. I arbetet med att bedöma konsekvens-nivån tas hänsyn till typen av situation, vilka det är som utför aktionen, hur många de är, anläggningens karaktär och när situationen uppstår. Vilka som utför aktionen kan påverka konsekvensnivån om man känner till deras kapacitet och inställning.

Konsekvensen av händelser är olika för olika inblandade. Framför allt rör det sig här om konsekvenserna för Svenska Kraftnät, individer som är involverade i situationen, den del av samhället som får sin elförsörjning genom anläggningen, samt eventuellt vissa speciella företag, myndigheter eller andra organisationer. Precis som för situationsanalysen utförs

konsekvensanalysen endast då användaren kräver detta. Konsekvensanalysen ger inte förslag på egna aktioner för användaren, dvs. förslag på vad som ska göras nu och hur man i så fall gör detta. Sådant stöd ges av systemkomponenter som beskrivs i kapitel 6.

## 5.5 Dataosäkerhet

De resultat som sensordataanalysen producerar innehåller alltid osäkerheter. Osäkerheten härrör från fysikaliska begränsningar i sensorns upplösning, hur länge och hur ofta som sensorerna registrerat objektet samt på approximationer och antaganden om objekten i signal- och bildbehandlingen, se mer i [Jungert & Lantz, 2006]. För att användaren ska kunna ta hänsyn till osäkerheterna kommer systemet ge möjlighet att presentera osäkerheten i resultatet tillsammans med resultaten från sensordataanalysen. Händelseanalysen måste kunna propagera och hantera sensordatas osäkerhet på ett korrekt sätt då den bestämmer vilka händelser och kombinationer av händelser som inträffar. Detta styr i hög grad osäkerheten om vilka händelser som inträffar. Detsamma gäller för situationsanalysen. I situationsanalysen hanteras osäkerheter genom att framställa flera alternativa hypoteser om situationen och hypotesernas trolighet. Det är då användarens ansvar att bedöma situationen. Om användaren inte är säker på sin bedömning, givet det underlag som han/hon får presenterat, kan användaren begära mer information från systemet.

## 5.6 Sensorstyrning

Sensorstyrning handlar om att styra in eller justera sensorer så att de så bra som möjligt registrerar det som sker inom ett visst område. Sensorstyrning kan ske automatiskt eller manuellt. Sensorstyrningen används för att automatiskt bestämma uppgiftsfördelningen i sensorsystemet. Sensorsystemets olika uppgifter inkluderar att söka efter nya objekt, följa objekt och att klassificera okända objekt. Olika sensortyper agerar olika då de ska utföra dessa olika uppgifter. Sensorstyrningen har förmåga att välja hur mycket tid varje sensor ska ägna sig åt alla aktuella uppgifter i den närmaste framtiden. För en enskild sensor inkluderar detta att välja tidsfördelningen mellan att följa ett känt objekt eller att söka efter nya objekt. Dessutom kan sensorstyrningen avgöra vilken sensor som ska följa ett objekt då det förflyttar sig. Sensordata- och händelseanalysen levererar styr signaler om var intressanta händelser sker, så att sensorerna kan riktas in mot de mest intressanta fenomenen. På de högre nivåernas analys, situations- och konsekvensanalys, sker ingen automatisk sensorstyrning. I de fall användaren vill styra sensorerna har han/hon prioritet över den automatiska sensorstyrningen.

## 6. Systemarkitektur för intelligent övervakning

I detta kapitel presenteras den systemarkitektur som föreslås. Systemarkitekturen bygger på de behov som identifierats i kapitel 2 och 3, och de analys- och sensorförmågor som diskuterades i kapitel 4 och 5. I detta kapitel kommer begreppet tjänst att beskrivas tillsammans med den tjänstebaserade arkitektur som utgör en central del av systemkonceptet. Vidare kommer tjänster nödvändiga för användarna att presenteras liksom behovet av beslutsstöd av olika slag. Målsättningen är en systemarkitektur som kan utnyttjas för övervakning av olika typer av skyddsobjekt.

Moderna systemlösningar för tillämpningar inom övervakningsområdet har stor potential att effektivisera och öka förmågan att övervaka. Utan en väl genomarbetad arkitektur för dessa system finns risk att de blir alltför komplexa och inflexibla. Inom utvecklingen av framtida ledningssystem, vilket övervakningssystem är en speciell tillämpning av, kommer detta att hanteras med stöd av en tjänstebaserad systemarkitektur. System och systemkomponenter kommer att interagera genom tjänster. Tjänsterna kan vara organiserade hierarkiskt, dvs. tjänster på olika nivåer kan anropa varandra för att utföra vissa uppdrag. En tjänst i ett övervakningssystem kan nyttjas för att inhämta information i en viss situation och för ett visst ändamål. En annan tjänst kan användas för att analysera den inhämtade informationen.

En tjänstebaserad systemarkitektur medger en modulär systemstruktur. System som istället har en monolitisk struktur blir alltför komplexa för att effektivt kunna realiseras och underhållas, samt att de är svåra att anpassa till förändrade situationer. Utöver detta finns det krav på att kunna återanvända tidigare utvecklad programvara. Modulariteten medger en viss typ av oberoende av vilken sensor som används, s. k. sensoroberoende. Detta hänger samman med att systemkomponenter och moduler enbart har svaga bindningar. Systemet som helhet blir därmed oberoende av exakt vilka typer av sensorer som används, antalet anslutna sensorer samt att sensorer kan bytas mot andra utan att detta påverkar övriga delar av systemet. De resultat som kan genereras av systemet är däremot inte oberoende av sensorerna. Sensorernas förmåga påverkar systemets förmåga.

Utöver modularitet medger tjänstebaserade systemarkitektur er möjligheten till evolutionär utveckling av systemet och en fokusering på den nytta som systemet skall generera. Tjänstearkitektur ger också system med högre flexibilitet, vilket medger anpassning av systemet till förändrade behov och situationer. Nyttjande av standardiserade gränssnitt mellan systemkomponenterna, i detta fall tjänsterna, medger interoperabilitet med externa system, samt ett ökat leverantörsberoende med avseende val av systemets komponenter.

### 6.1 Tjänstebegreppet

Begreppet tjänst har ingen entydig definition och används inom ett flertal områden med vitt skilda betydelser, exempelvis (1) en befattning med formaliserade arbetsuppgifter och kvalifikationskrav, (2) utövandet av ett arbete och (3) en handling som är till nytta för någon annan [Stenumgaard, 2004]. Inom områdena systemarkitektur, informationssystem och informationsteknologi används begreppet tjänst numera flitigt och har blivit något av ett modeord. Begreppet IT-tjänst har lanserats som "the typical outcome of people's activities using IT tools according to the precisely defined process". Inom IT-området anses en tjänst vara en funktion som tillhandhålls till en specificerad kvalitet och kostnad [Rodosek, 2003]. Inom telekommunikationsområdet ses tjänster som förmågor att utbyta information som tillhandahålls kunder av tjänsteleverantörer [Gozdecki, 2003].

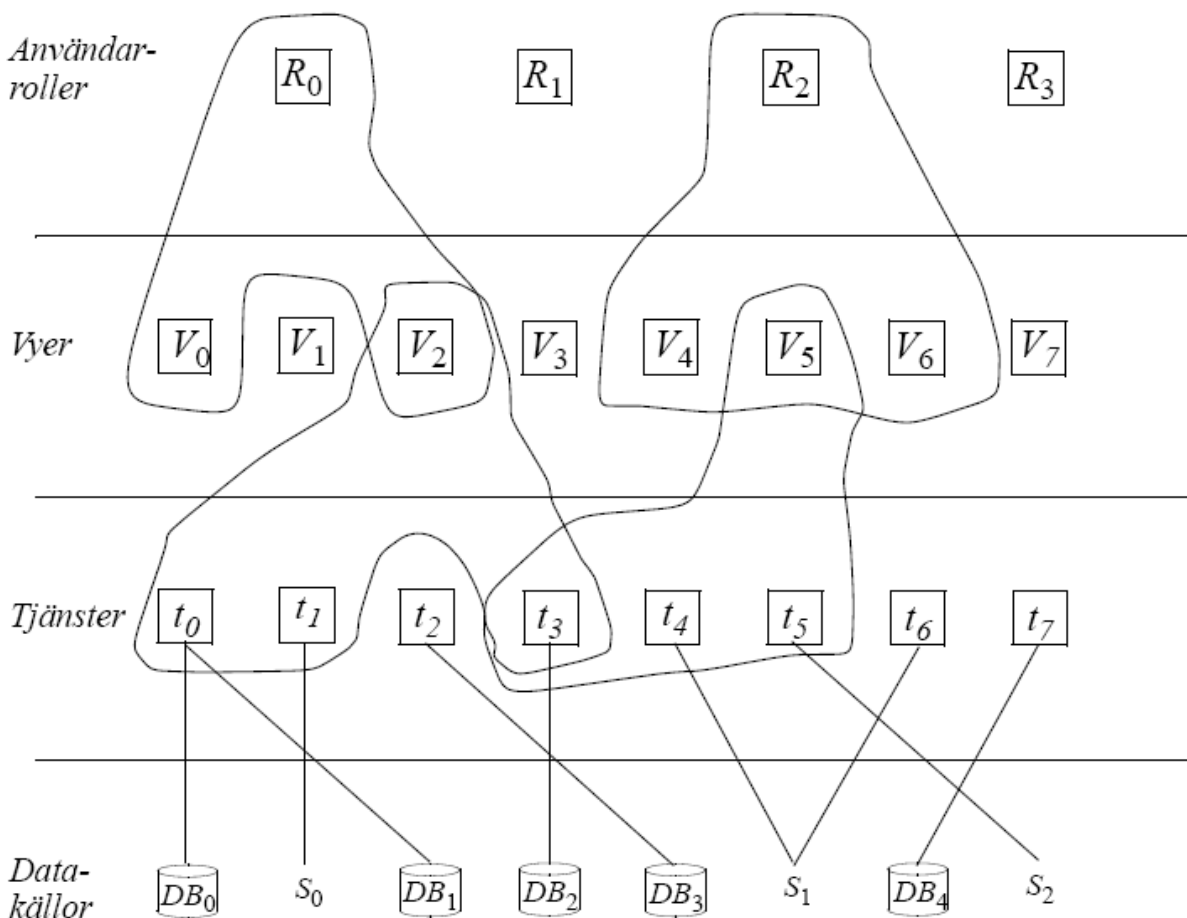
Arkitekturen Service Oriented Architecture (SOA) har sprungit ur ett försök att skapa lösare kopplingar mellan olika programvarukomponenter. En tjänst i SOA definieras som "a unit of work done by a service provider to achieve desired end-results for a service consumer" [He, 2003]. Inom den svenska Försvarmakten har en generell definition av begreppet *tjänst*, starkt influerad av

definitionen inom SOA, tagits fram; denna definition är avsedd att användas för att möjliggöra integration av olika system [Jönsson, 2003]. Enligt denna definition är en tjänst en abstraktion av hur en producent kan åstadkomma *nytta* för en konsument, utan att beskriva hur detta genomförs. Nyttan åstadkoms genom att producenten levererar en prestation, vilken ger effekt hos/för konsumenten. Tjänster skall beskrivas oberoende av hur de är implementerade; manuellt, tekniskt eller genom kombinationer av dessa. Beskrivningen av en tjänst skall förklara hur konsumenter gör för att få tillgång till tjänsten och vad som produceras, det vill säga vilken effekt som erhålls. Vidare skall beskrivningarna specificera de relevanta egenskaper och med stöd av dessa egenskaper kan konsumenterna välja vilken realisering av tjänsten som passar dem bäst. Tjänsten utgör därmed en fasad mellan producenter och konsumenter. Konsumenter behöver inte ha kännedom om vilka producenter som tillhandhåller olika tjänster, utan kan söka efter de tjänster som passar bäst baserat på deras beskrivningar.

I det system som föreslås här är konsumenterna användare knutna till driftcentralen. Producent är i detta fall sensorsystemet eller någon annan komponent som utför informations-bearbetning eller -insamling. En tjänst kan därför i detta sammanhang definieras som den bearbetning och insamling av information övervakningssystemet utför som resultatet av ett specifikt anrop. Detta anrop kan ske av en användare eller av andra tjänster.

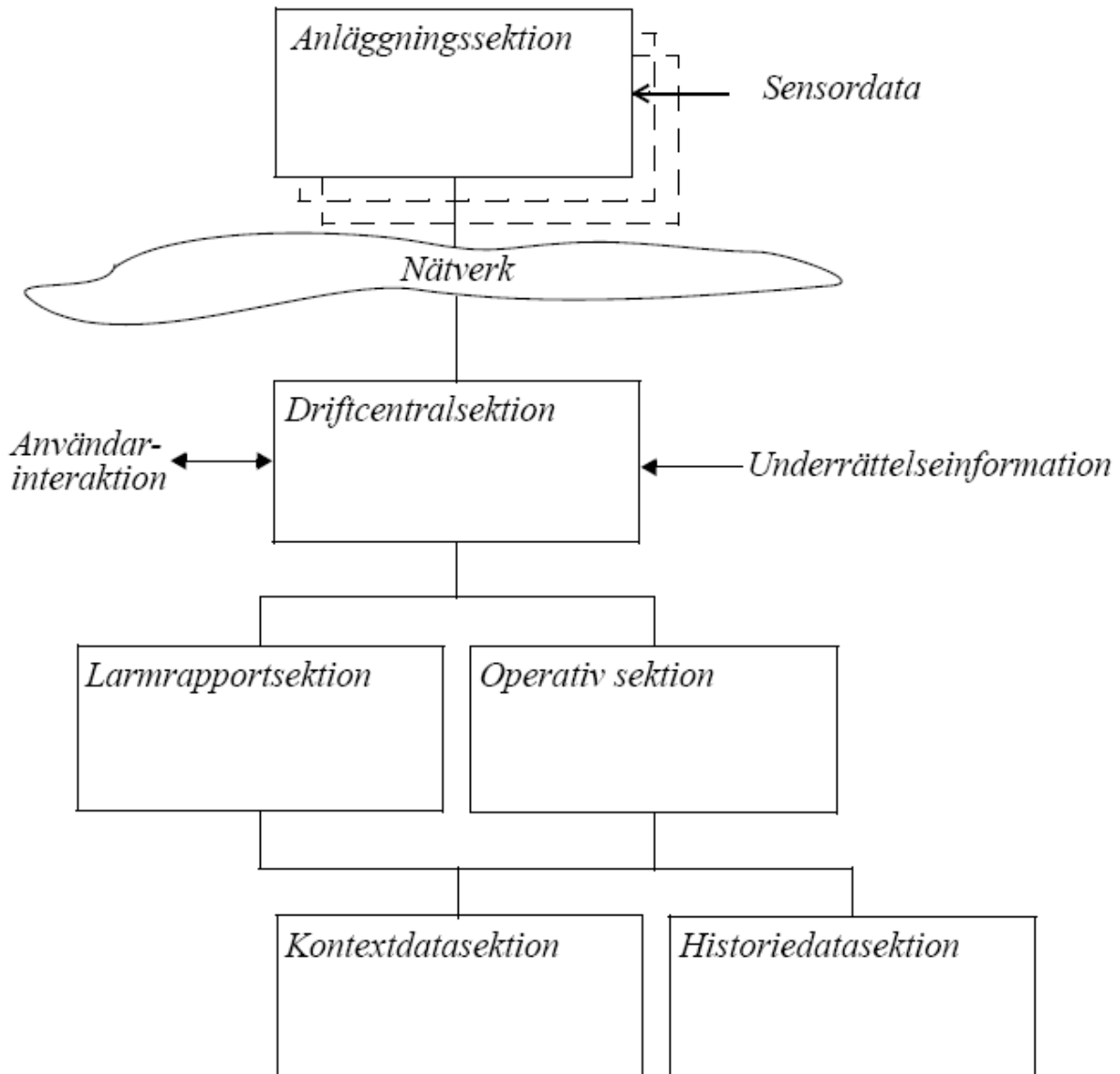
## 6.2 Vyer och användarroller

En vy utgörs av information som visualiseras för användare, samt av ett antal fördefinierade tjänster. Den information som presenteras kan utnyttjas för att beskriva situationen vid en anläggning för användarna. En instans av en vy innehåller den information som tjänsterna knutna till vyn har producerat och presenterar vid en given tidpunkt. Instansen uppdateras successivt allteftersom ny information kommer in, vilket har till följd att nya vyinstanser skapas i samma takt. Inaktuella vyinstanser sparas i Historiedatavyn så snart de blir inaktuella.



Figur 6.1. Systemstruktur i fyra lager för tjänstebaserade övervakningssystem.

Genom att användarna endast kan avropa de tjänster som är knutna till de vyer som de tilldelats medför detta att användarna endast har tillgång till ett begränsat antal operationer som de kan genomföra. Under vissa omständigheter är detta nödvändigt, exempelvis om användarna saknar behörighet för att ta del av viss information. I andra situationer kan det vara nödvändigt att kunna tilldela vissa användare ytterligare befogenheter. De ges då möjlighet att nyttja ett antal ytterligare tjänster som integreras i systemet. Därigenom är det möjligt att anpassa systemet till olika situationer och tillgängliga datakällor så som sensorer och databaser.



Figur 6.2. Strukturen för övervakningssystemet med dess sex olika tjänstesektioner samt de vägar för informationsflöde som kan förekomma.

Olika kategorier av användare har olika behov av så väl tjänster som visualiseringar. Användare har olika arbetsuppgifter, vilka kräver olika förmågor av systemet. Med utgångspunkt från användarnas arbetsuppgifter är det möjligt att identifiera ett antal olika roller som är anpassade till de olika användarkategoriernas behov. En given roll har ett antal vyer knutna till sig där varje vy innefattar ett antal tjänster. Till tjänsterna finns ett antal datakällor. Systemstrukturen kan beskrivas i fyra nivåer som illustrerar hur en användarroll kan ha olika vyer knutna till sig, som i sin tur har ett antal tjänster knutna till sig. Tjänsterna kan i sin tur avropa olika datakällor (figur 6.1). I den tillämpning som beskrivs i denna rapport har två roller identifierats:

- operatörsrollen,
- analytikerrollen.

Operatören hanterar förekommande larm och kan följa vad som pågår vid de olika anläggningarna. Analytikern har till uppgift att följa upp och analysera vad som sker över tiden viden eller flera anläggningar.

### 6.3 Systemöversikt

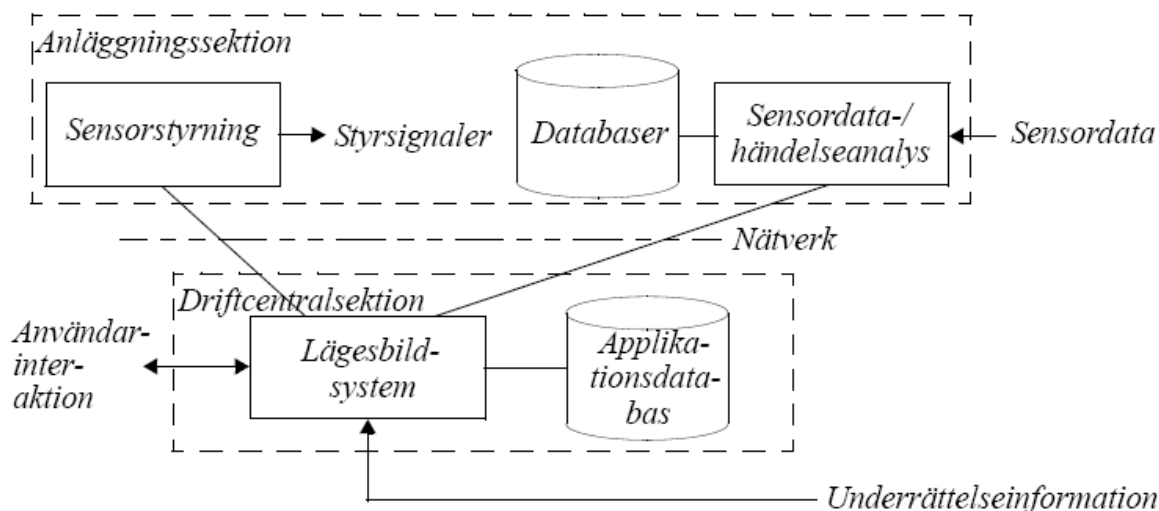
Grundstrukturen för övervakningssystem utgörs väsentligen av sex olika delar, s. k. sektioner, där varje sektion innehåller minst en vy med dess underordnade tjänster (figur 6.2). Av dessa sex sektioner återfinns fem i driftcentralsystemet. Den sjätte sektionen, Anläggningssektionen, är multipel och kommer att återfinnas vid varje anläggning. Till varje Anläggningssektion kopplas ett antal sensorer, samt grundläggande förmåga till sensordata- och händelseanalys. Information kan flöda mellan sektionerna i båda riktningar i enlighet med de relationer (linjer) som finns i figur 6.2. Den information som utbyts mellan sektionerna är resultatet av olika tjänsteanrop. Vidare finns också i Anläggningssektionen en modul för sensorstyrning genom vilken operatörerna kan styra en sensor från kontrollrummet.

Driftcentralsektionen omfattar hanteringen av övervakningssystemet, interaktionen med användarna, samt inhämtning och analys av underrättelseinformation. Den Operativa sektionen hanterar lägesbeskrivningar för aktuella larm. Med lägesbeskrivning menas i detta sammanhang en beskrivning av vad som sker vid en anläggning där ett larm inträffat. En sådan lägesbeskrivning kan innehålla information om vad larmet består av, t. ex. inblandade personer, fordon och andra objekt som ingår i larmet.

Larmrapportsektionen innehåller en vy som visar förekommande larm och som innehåller bland annat tjänster som automatisk aktiveras och som är nödvändiga vid larm. De båda övriga sektionerna, Kontextdatasektionen och Historiedatasektionen har till syfte att stödja verksamheten. Kontextdatasektionen skall förse användarna med grundläggande information om den anläggning som ett inkommet larm avser, dvs. en karta över anläggningen och dess omgivning. Historiedatasektionen har till uppgift att ta hand om och lagra information som skapats under ett larm, t. ex. inaktuella vyinstanser. Avsikten med Historiedatasektionen är att det skall vara möjligt för en analytiker att i efterhand analysera en eller flera händelser för att avgöra om det finns några samband mellan dessa, exempelvis om någon person visat sig på platsen vid flera tillfällen och därvidlag uppträtt på något avvikande.

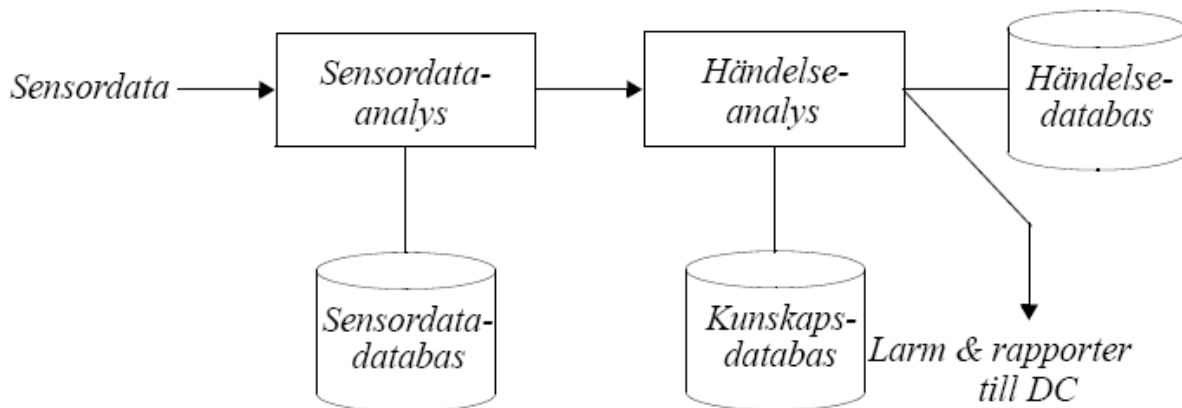
### 6.4 Systemsektioner

I detta avsnitt beskrivs de mest centrala strukturerna av systemet i detalj; främst med avseende på de olika vyer som finns integrerade i de olika sektionerna. De viktigaste sektionerna i övervakningssystemet är Driftcentralsektionen, Anläggningssektionerna och den Operativa sektionen.

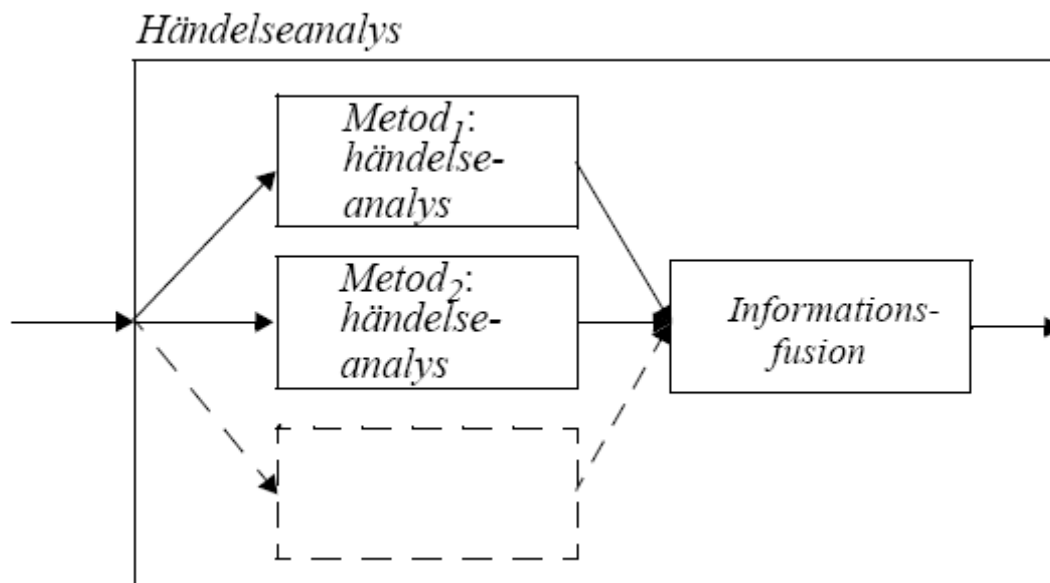


Figur 6.3. Anläggnings- och Driftcentralsektionerna sammankopplade i nätverk.

Anläggnings- och Driftcentralsektionernas strukturer framgår av figur 6.3. Dessa båda sektioner är direkt anslutna till övervakningssystemets nätverk. I Anläggningssektionen finns stöd för analys av inkommande sensordata samt ett antal databaser i vilken dessa data successivt lagras och sparas under given tid. Resultatet av gjorda analyser lagras också efterhand som de är klara. Det senare sker emellertid endast för information om händelser som systemet anser viktiga i något avseende. Vid sidan av sensor- och händelseanalysen finns i Anläggningssektionen också en modul för sensorstyrning vilket också framgår av figuren. Dataanalysen kan delas i två delar (figur 6.4): en som analyserar data som kommer in från sensorerna vid den aktuella anläggningen för att upptäcka relevanta händelser, samt ett senare steg som analyserar dessa händelser i avsikt att hitta sammansatta händelser som kan ge upphov till larm. Till stöd för händelseanalysen finns en kunskapsdatabas, för att avgöra vilken typ av händelse som pågår. För att åstadkomma säkrare och tillförlitligare bedömningar krävs troligen att händelseanalysen utgörs av flera metoder. Händelseanalysen kan baseras på analyser med olika metoder som exekveras parallellt och som därefter vägs samman i ett informationsfusionssteg (figur 6.5).



Figur 6.4. De olika analysstegen i Anläggningssektionen som kan medföra att ett larm skickas till driftcentralen.



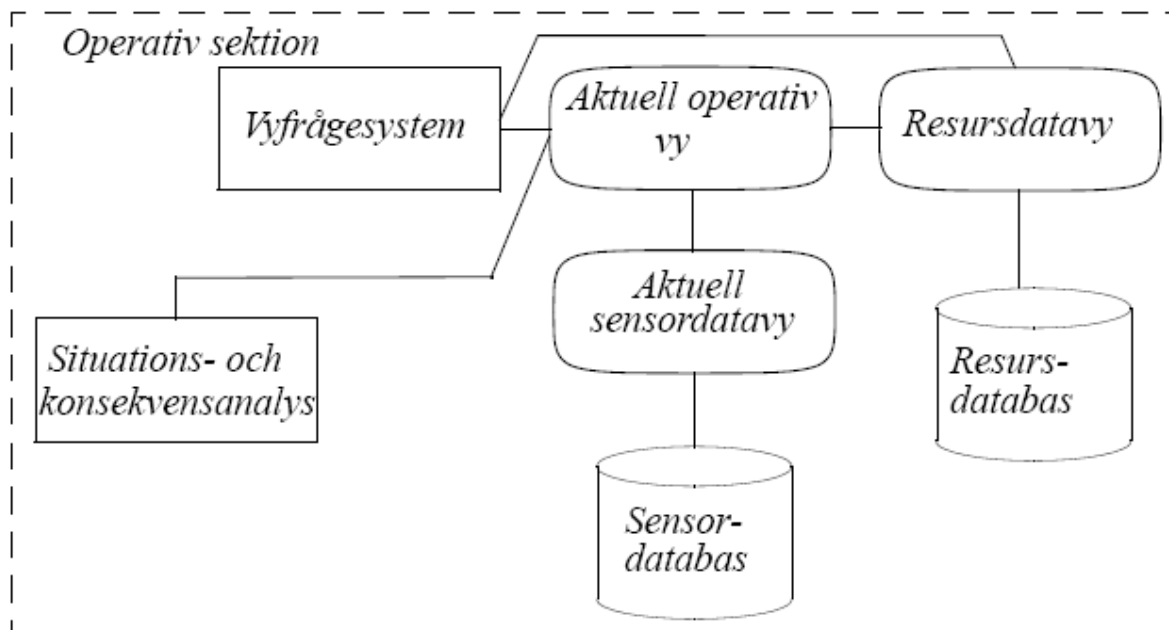
Figur 6.5. Parallell analys med olika metoder för säkrare händelseanalys.

Driftcentralsektionen består av två huvuddelar; en applikationsdatabas och ett lägesbildsystem. I applikationsdatabasen lagras information från de olika anläggningarna som senare kan hämtas automatiskt av systemet eller av användarna med hjälp av tillgängliga tjänster i den Operativa sektionen. Vidare finns i denna sektion också ett användargränssnitt genom vilket användarna kan

utnyttja systemets olika vyer. Denna del av systemet kallas lägesbildssystemet, som tillhandahåller en tjänst i det tjänstbaserade övervakningssystemet.

I den Operativa sektionen kommer även tjänster för att direkt styra sensorerna vid anläggningar att finnas. Detta krävs för att operatörerna visuellt skall kunna undersöka vad som pågår vid en anläggning där larm genererats.

Kontextdata- och Historiedatasektionerna är av enklare natur. Kontextdatasektionen innehåller en databas för lagring av anläggningsinformation. Denna består bl. a. av kartor över anläggningarna, samt information om var sensorerna är placerade i de olika anläggningarna, deras typ och deras övriga egenskaper. Historiedatasektionen har en liknande struktur, här lagras successivt information som senare kan användas för vidare analys.

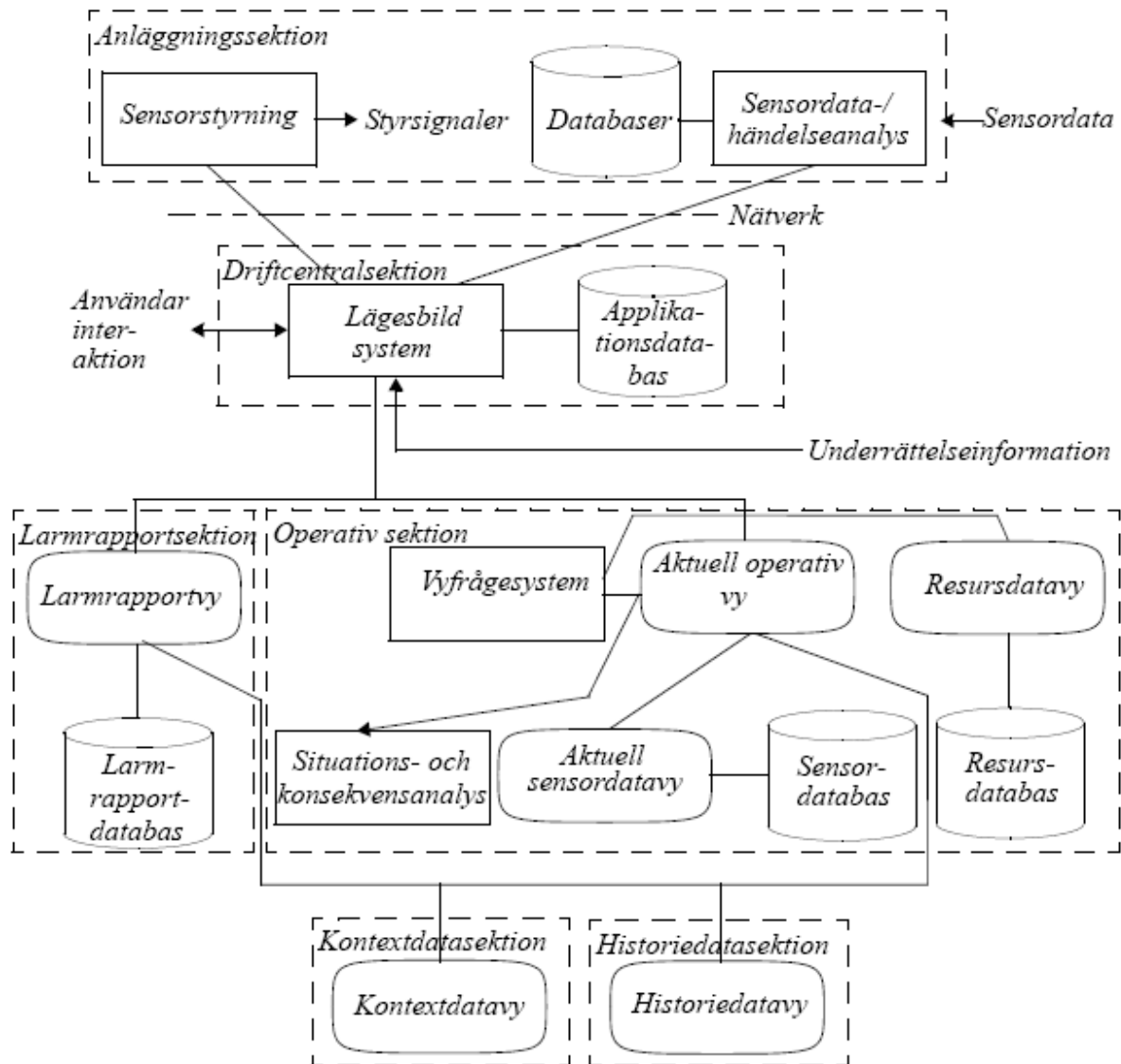


Figur 6.6. Den Operativa sektionen, dess vyer och beslutstöd.

## 6.5 Rollstruktur

Övervakningssystemet kan, som redan nämnts, hantera ett antal olika roller. De delsystem som skapas för att passa de olika rollernas behov har olika egenskaper (figurerna 6.7 och 6.8). Detta sätt att modulärt bygga upp olika delsystem ger hög flexibilitet och anpassnings-barhet till olika rollers behov, uppkomna situationer och tekniska förutsättningar att samla in information. Således kommer det att vara möjligt att utveckla och infoga anpassade tjänster för varje typ av anläggning, t. ex. ett ställverk, en kärnkraftsanläggning eller ett vatten-kraftverk. Detta gäller även andra typer av skyddsanläggningar, som behöver övervakas på liknande sätt.

Arbetsprincipen för de rollbaserade systemen är att användarna arbetar i en speciell, aktiv vy som över tiden kan variera med hänsyn till den pågående verksamheten. Den aktiva vyn visar den information som är knuten till den vid aktuella tidpunkten, t. ex. en visualisering av läget vid den anläggning som ett pågående larm avser. När behov av annan information uppstår kan användarna växla till en annan vy med hjälp av de i den aktiva vyn befintliga tjänsterna. Vissa kompletteringstjänster till detta förfarande finns, exempelvis kommer det i vissa situationer inte att vara nödvändigt att växla till en annan vy om det finns tjänster som indirekt kan anropa den eftersökta informationen från den aktiva vyn. Dessutom kan det också finnas vyer som kan styras av någon annan vy, ett exempel på detta är Aktuella sensordatavyn som kan styras från Aktuella operativa vyn. figurerna 6.7 och 6.8 visar hur de kompletta rollsystemen för respektive operatörs- och analytikerrollerna är uppbyggda.



Figur 6.7. Operatörsrollen för övervakningssystemet.

För operatörsrollen finns kompletta vyer i Larmrapportsektionen och i den Operativa sektionen medan Kontextdatasektionen och Historiedatasektionen saknar vyer, vilket medför att operatörerna inte direkt kan komma åt tjänsterna i dessa vyer. Dessa nås indirekt från Aktuell operativ vy i den Operativa sektionen och då endast för vissa speciella och begränsade ändamål. Detta begränsar givetvis vad operatörerna kan göra men medför inga begränsningar med avseende på deras primära arbetsuppgifter som är att hantera olika larm.

Larmrapportvyn, som återfinns i Larmrapportsektionen, är endast aktiv då larm eller annat meddelande inkommer till driftcentralen. Larm och meddelanden anger vad som hänt, var och när. När detta inkommer startar Larmrapportvyn automatiskt ett antal tjänster som aktiverar den Operativa sektionen, laddar ner information om den aktuella anläggningen från Kontextdatabasen och överför sensordata från den larmade anläggningen till Aktuell sensordatavvy om sådan information föreligger. Härigenom visualiseras information som visar på vad som pågår vid anläggningen.

I Aktuell operativ vy kan operatörerna se var händelsen registrerats och vilka sensorer som gjort registreringen. Vid behov kan operatörerna växla mellan tillgängliga sensorer och betrakta lämpligaste sensordata i Aktuell sensordatavvy. Så snart operatörerna anser sig ha tillräcklig information om det aktuella larmet kan de besluta om vilka åtgärder som skall vidtas. Detta kan innebära att någon måste skickas till den aktuella anläggningen för att vidta åtgärder; t. ex. kan

detta vara att släppa in polis eller räddningstjänst. För detta behöver operatörerna tillgång till telefonnummer till olika individer och organisationer. Denna typ av information finns tillgänglig i Resursdatabasen som kan nås via Resursdatavyn. Detta kan ske på två sätt: (1) antingen genom att operatörerna växlar över till Resursdatavyn och hämtar den eftersökta informationen eller (2) att de genom en indirekttjänst i Aktuell operativ vy hämtar den eftersökta informationen utan att växla vy.

## 6.6 Vyrelaterad information

I detta avsnitt beskrivs vilken information som presenteras i respektive vy. Viss information är direkt relaterad till larm.

### **Larmrapportvyn (LRV)**

Larmrapportvyn (LRV) innehåller information direkt relaterad till aktuella larmrapporter och meddelanden.

### **Aktuell operativ vy (AOV)**

Aktuell operativ vy (AOV) visar information om den anläggning för vilket larm har genererats. Informationen består främst av en kartbild över aktuell anläggning, dess omgivning och vilka sensorer som är aktiva samt deras lägen. I det fall någon meddelar att de vill komma in i anläggningen skall deras uppgifter kollas mot Resursdatavyn. Förutom den information som skapas vid ett larm kan också underrättelseinformation automatiskt inhämtas och föras över till denna vy.

I AOV kan också lägesinformation föras in i kartan över området. Denna information kan avse objekt som kan utgöra ett hot mot anläggningen som larmet avser. Detta kan också vara personer som betar sig på ett hotfullt sätt eller som är ute på något slags spaningsuppdrag eller personer i fordon som är ute på spaning.

### **Kontextdatavyn (KXV)**

Kontextdatavyn (KXV) innehåller främst kartor över samtliga anläggningar och deras omgivningar. Annan information utgörs av aktuella sensorer som finns placerade vid de olika anläggningarna, deras typ och position som kan vara både i och utanför anläggningen. **KXV** kan också innehålla andra attributvärden som tillhör anläggningen.

### **Historiedatavyn (HDV)**

Historiedatavyn (HDV) innehåller information relaterad till tidigare larm, dvs. instanser ur Larmrapportvyn och Aktuell operativ vy samt tillgängliga sensordata från Sensordatavyn. Dessa vyinstanser skall vara komprimerade och behöver inte innehålla *explicit kontext* information utan bara referenser till den anläggning som larmet avsåg. Operatörerna kan inte komma åt data i Historiedatavyn annat än i begränsad omfattning och då endast sådan information som avser ett pågående larm, som redan överförs till Historiedatavyn. För att i ett aktivt skede komma åt historisk information om ett pågående larm måste operatören avropa tjänsten backa tillbaka till någon tidigare tidpunkt eller tidsintervall. Information som har blivit inaktuell överförs automatiskt till Historiedatavyn från främst Aktuell operativ vy och från Larmrapportvyn.

### **Resursdatavyn (RDV)**

Resursdatavyn (RDV) innehåller information som handleder operatörer och analytiker under en given situation. Sådan information kan delges i form av en handbok som även kan ses som ett policydokument. Handhavandet av detta dokument sker genom avrop av en tjänst. Handboken skall ge användarna vägledning så att dessa kan hitta lämplig information och få råd med avseende på vilka åtgärder som bör vidtas i det aktuella läget.

Exempel på annan information som skall finnas tillgänglig kan vara information om personal som har behörighet att gå in i en anläggning. Samt information om personal som i händelse av larm

skall skickas ut till platsen för att släppa in polis eller räddningstjänst samt också för att undersöka om personal, som gått in under dagen, men inte kommit ut ur anläggningen igen, inte ligger skadade i anläggningen. Denna personalinformation skall innehålla telefonnummer och dylikt. Telefonnummer till polis, räddningstjänst och andra verk, myndigheter och företag bör också finnas lagrade här.

### **Aktuella sensordatavyn (SDV)**

Aktuella sensordatavyn (SDV) används för att visualisera sensordata från olika sensordatakällor och styrs från den Aktuella operativa vyn. Vid larm aktiveras den automatiskt och aktuella sensordata visualiseras i vyn. Historiska sensordata lagras så länge larmet pågår i sensordatabasen och överförs efter hand som de blir inaktuella till Historiedatavyn. Data i SDV kan bara komma åt av dem som har analytikerrollen. Operatörerna skall bara kunna komma åt sådana sensordata som kan associeras med det pågående larmet och inte till avslutade ärenden.

### **6.7 Definierade tjänster**

Tjänster finns av tre olika huvudtyper, automatiska som aktiveras vid t. ex. ett larm, analytiker- och operatörstjänsterna som avropas av respektive användarkategori. Tjänsterna kan vara synkrona, då konsumenter direkt erhåller effekt av den utförda tjänsten. De kan även vara asynkrona, så kallade prenumerationstjänster, där leverans sker fortlöpande tills dess att prenumerationen avbeställs. Stödtjänster är tjänster som inte levererar resultat till användaren, utan har till uppgift att internt stödja systemets funktion. Asynkrona tjänster är speciellt användbara i övervakningssammanhang, där sensorer och sensorsystem kontinuerligt kan leverera data och information till de användare som har ansvar för övervakningen. Denna informationsöverföring kan genom prenumeration ske automatiskt så länge detta krävs för att säkerställa övervakningen. Därigenom blir det möjligt att automatiskt starta tjänster som hämtar in aktuella sensordata och presenterar dessa för användaren. Det blir också möjligt att skifta sensor, vilket medför att den tidigare använda sensorn slutar överföra information och att den nya tar vid. Vid sidan av dessa tjänster föreligger också behov av en mängd olika stödtjänster som kommer att diskuteras nedan. I detta avsnitt beskrivs de tjänster som har definierats för de olika vyerna.

## **Initieringstjänster i övervakningssystemet**

### **Automatiska tjänster**

- Vid larm, aktivera LRV och för in information om det nya larmet i vyn.

### **Analytikertjänster**

- initiera analytikerrollen genom initiering av vyerna LRV, AOV, KXV, HDV, RDV, SDV.

### **Operatörstjänster**

- initiera operatörsrollen, vilket kan göras även om inget larm pågår, genom initiering av vyerna LRV, AOV, RDV, SDV.

## **Tjänster i Larmrapportvy (LRV)**

### **Automatiska tjänster**

- När nytt larm går, aktivera AOV (om inget annat larm är under beredning).
- Initiera nytt larm i Historiedatabasen samt i Larmrapportdatabasen då nytt larm går.
- Vid avslutat larm ta ur Larmrapportdatabasen bort och föröver kvarvarande information till Historiedatabasen (från AOV).

### **Operatörstjänster**

- Växla till annat aktivt larm eller växla till nytt larm (avser de fall då flera larm pågår samtidigt och innebär också växling av övriga vyer). Innefattar: aktivera AOV, hämta kontextdata om nytt larm, öppna ASV för presentation av nya sensordata.
- Avsluta larm resulterar i att samtliga resterande information överförs till Historiedatabasen.

- Backa tillbaka till tidigare händelser.

### **Analytikertjänster**

- Sök reda på tidigare larm för analys från HDV.
- Aktivera tidigare larm.
- Backa tillbaka till tidigare händelser.
- Aktivera beslutsstödshjälpmedel för fusion.

## **Tjänster i Aktuell operativ vy (AOV)**

### **Automatiska tjänster**

#### *Vid aktivering av larm:*

- Hämta kontextdata från Kontextdatabasen (över larmat objekt).
- Hämta och öppna aktuella sensordatabilder i SDV.
- Aktivera SDV för aktuella sensordata.

#### *Vid pågående larm*

- Uppdatera AOV med nya data från applikationsdatabasen när sådana data inkommer.

#### *Vid inpassage*

- Kontrollera personuppgifter mot Resursdatavyn (RDV).

#### *Vid uppdatering av aktuell vy*

- Spara gamla vyinstanser i HDV-databasen.

### **Operatörstjänster**

- Visa eftersökta uppgifter i Resursdatavy (RDV).
- Visa Larmrapportvy (LRV).
- Visa SDV.
- Hämta nya data från applikationsdatabasen (uppdatera AOV).
- Växla till annan vy (LRV eller RDV).
- Visa attributvärden för specificerade (utpekade) objekt i AOV.
- Koppla upp angiven sensor i SDV.
- Styr (zoom, pan, tilt) aktuell rörlig sensor och visa i SDV (avser andra sensortyper än videokamera).
- Zoom i aktuell vyinstans (avser kartbild över anläggning).
- Pan i aktuell vyinstans (avser kartbild över anläggning).
- Backa tillbaka till vyinstans för pågående larm (hämtas från Historiedatabasen och avser given tidpunkt eller tidsintervall).

### **Analytikertjänster**

- Visa eftersökta uppgifter i Resursdatavy (RDV).
- Visa Larmrapportvy (LRV).
- Visa SDV.
- Växla till annan vy (Larmrapportvy, Historydatavy, Kontextdatavy eller Resursdatavy).
- Sök i Historiedatabasen efter speciell instans samt för över denna till AOV.
- Visa attributvärden för specificerat (utpekat) objekt i AOV.
- Aktivera vyfrågespråket.
- Koppla upp angiven sensor i SDV.
- Styr aktuell rörlig sensor och visa i SDV (avser andra sensortyper än videokamera).
- Zoom i aktuell vyinstans (avser kartbild över anläggning).
- Pan i aktuell vyinstans (avser kartbild över anläggning).
- Backa tillbaka till vyinstans för pågående larm (hämtas från Historiedatabasen).

## Tjänster i Kontextdatavy (KXV).

### Analytikertjänster

- Presentera kontextdata för given anläggning.
- Sök i Kontextdatabasen efter data om viss anläggning.
- Växla till annan vy (AOV, RDV, HDV eller LRV).
- Överför aktuell KXV-instans till AOV.
- Zoom i aktuell vyinstans (avser kartbild över anläggning).
- Pan i aktuell vyinstans (avser kartbild över anläggning).

## Tjänster i Historiedatavyn (HDV)

### Analytikertjänster

- Återaktivera gammalt inaktivt/avslutat larm.
- Visa Historiedatavy från given tidpunkt för aktiverat larm.
- För över aktuell vyinstans till AOV.
- Växla till annan vy (AOV, LRV, KXV eller RDV).
- Zoom (AOV-typ).
- Pan (AOV-typ).

## Tjänster i Resursdatavyn (RDV)

### Operatörs- och analytjänster

- Hämta information om personer och organisationer (montörer, polis, räddningstjänst, etc.).
- Öppna handboken.

## Tjänster i Aktuell sensordatavy (SDV)

SDV saknar egna tjänster, dvs. vyn styrs från AOV.

### 6.8 Beslutsstöd

Till systemet kan knytas beslutsstödssystem som kan vara av olika komplexitet. Dessa beslutsstöd ses ur systemets synvinkel också som tjänster, anknutna främst till den Operativa sektionen. Utöver de beslutstöd som nämns här kommer det också att vara möjligt att införa andra, vilka också kan anslutas till andra sektioner såsom t. ex. Driftcentralsektionen. Detta är möjligt även om det inte finns några sådana tjänster i detta förslag. Åtkomst av beslutstöds-tjänster sker via den sektion som är värd för dessa beslutstöd. Nedan presenteras några olika beslutsstöd som är lämpliga för detta övervakningssystem.

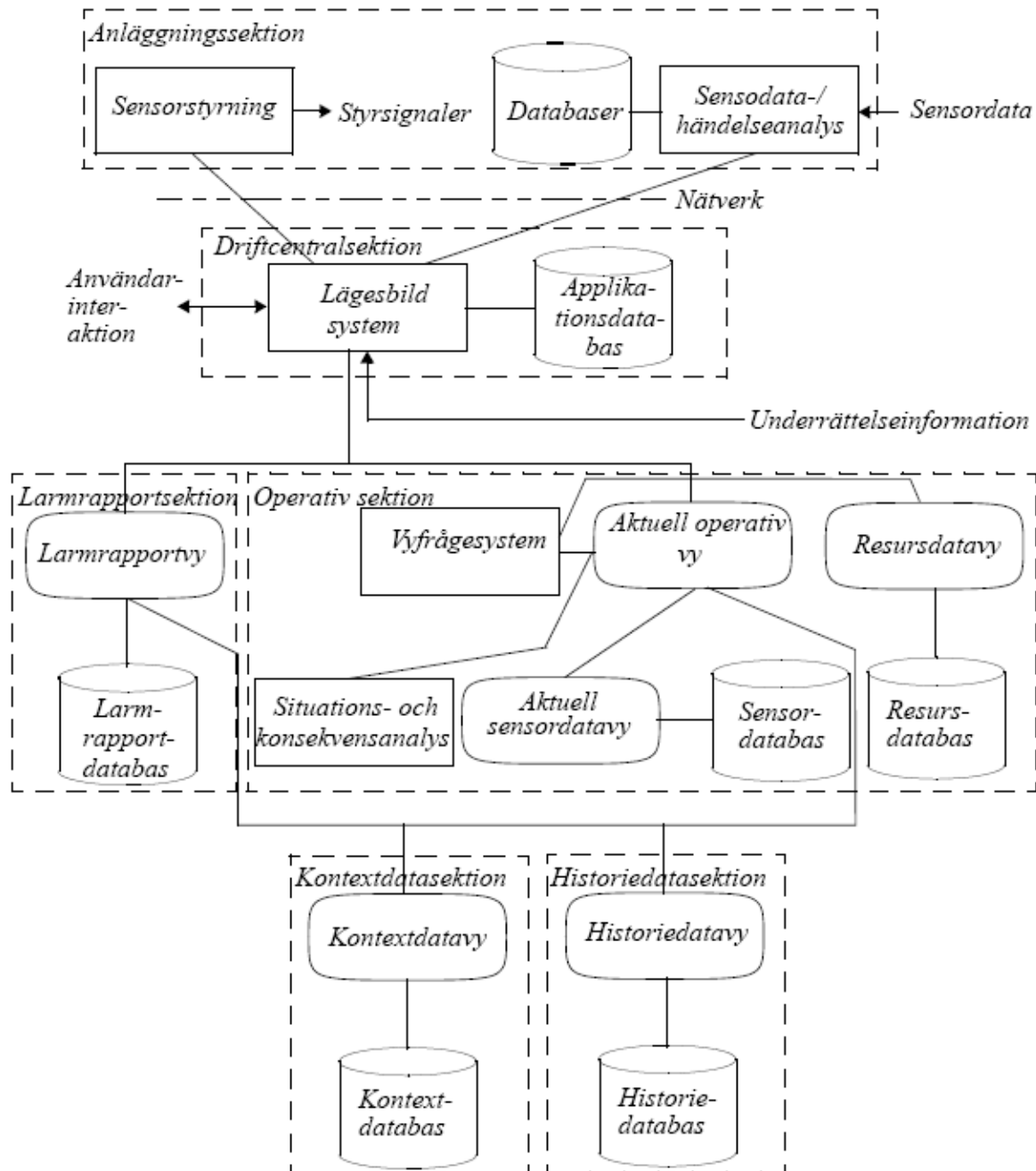
#### 6.8.1 Vyfrågespråk

Frågespråk utnyttjas främst för att ge användare möjlighet att välja vilken information som ska bearbetas eller visualiseras. Ett frågespråk är nödvändigt då det finns stora datamängder att hantera. Språket väljs så att det är möjligt för användarna att formulera tydliga sökvillkor, varefter information som uppfyller dessa kan samlas in. För ovana användare kan det vara svårt att snabbt precisera dessa villkor. I denna tillämpning kommer därför att väljas en ansats av något förenklad typ, som gör det möjligt för operatörerna att plocka fram eftersökt information på ett mer objektorienterat sett utan att användaren skall behöva precisera några mer komplexa sökvillkor. Därför väljas en sökmetod som är förenklad och visuell till sin natur. Detta gör det möjligt för operatörerna att klicka på aktuella objekt och enkelt få fram attribut- och statusvärden för dessa objekt. Detta kan innefatta allt mellan anläggningsobjekt till sensorer. För analytiker som kommer att arbeta under andra förhållanden och som har behov av att analysera mer omfattande information är det nödvändigt att komplettera med möjligheten att ställa mer komplexa sökvillkor.

Oberoende av vilken ansats som väljs skall frågespråket kunna utnyttjas för att ställa frågor om den information som samlats in. Den frågeteknik som ska användas kallas för *dynamic queries* och är både enkel och kraftfull, se t. ex. [Ahlberg, 1992], [Burigat & Chittaro, 2007].

### 6.8.2. Vyfrågespråk för dataanalys

För operatören och analytikern finns, som kan ses i figur 6.7 och 6.8, olika tjänster tillgängliga. Situations- och konsekvensanalysen är tjänster som erbjuds enbart till analytikern. Händelseanalysen utgör grunden för analytikerns situationsanalys. I detta konceptförslag finns ingen tjänst för situations- eller konsekvensanalys för operatören. Den dataanalys operatören har tillgång till är den automatiska händelseanalysen.



Figur 6.8. Delsystem anpassat till analytikerrollen i övervakningssystemet.

I kapitel 5 nämns att användaren kan påverka situations- och konsekvensanalysen. Detta sker genom de frågor som användaren ställer till systemet genom frågespråket. Genom frågespråket – och enbart genom frågespråket – kan användaren bestämma vilken information som ska behandlas. Tjänsterna för situations- och konsekvensanalys måste därmed kunna styras genom

frågor. Situations- och konsekvensanalysen erbjuder alltså inte användaren några direkta tjänster, utan dessa erbjuds via frågespråket.

Användaren efterfrågar och styr genom frågespråket de platser, tidsintervall, aktörer eller aktiviteter som ska analyseras. Dessutom styrs de egenskaper (t. ex. längd och storlek) och statusvärden (t.ex. hastighet) som analyseras hos aktörerna. I detta konceptförslag ingår inte att användaren genom frågespråket kan ställa frågor om framtiden. Beroende på aktuella intressenters specifika krav kan detta också inkluderas. I detta fall måste frågespråket och situations- och konsekvensanalysen kunna föra resonemang både med händelser som har inträffat och med hypotetiska händelser som skulle kunna inträffa.

### **6.8.3. Visualisering av dataanalys**

Visualisering av analysresultat sker i en karta över den aktuella anläggningen. De tjänster som finns för detta medger att man klickar på objekten (fordon eller person) och sedan får reda på aktuell information, dvs. deras typ, samt deras aktivitet, egenskaper och statusvärden, och hur säker denna information är med ett trolighetsmått. Dessutom finns möjlighet att samtidigt spela upp olika händelseförlopp vid enskilda eller olika anläggningar.

Visualiseringen av konsekvensanalysen är starkt beroende av den information som aktuell uppdragsgivare finner relevant. Av detta skäl är det inte möjligt att specificera konsekvensanalysens visualisering mer utförligt i detta läge.

Analytikern kan styra hur säker analysen måste vara för att presenteras för användaren och vissa former för visualisering av analysen. Detta inkluderar t. ex.:

- Hur många alternativa hypoteser om situationen eller möjliga konsekvenser som får presenteras.
- Hur osäkra händelser och situationer som ska presenteras eller larmas för.

## 7. Förmågor för intelligent övervakning

Detta kapitel presenterar tre scenarier som kan användas för att demonstrera övervakningssystemets förmågor till tidig och tillförlitlig upptäckt av hot mot skyddsanläggningar. Förutom händelseförloppen i scenarierna beskrivs de förmågor som övervakningssystemet måste ha för att hantera detta.

Scenario 1 beskriver spaning till fots mot en anläggning. En person X kommer till en viss anläggning vid två olika dagar. Vid det första tillfället går X runt staketet och stannar vid några tillfällen och observerar anläggningen. Två dagar senare återkommer X och fotograferar anläggningen. Avsikten är att systemet ska känna igen dessa händelser och larma om att spaning mot anläggningen förekommer.

Scenario 2 beskriver också spaning mot en anläggning, men i detta fall sker spaningen från ett fordon. En bil kommer till anläggning vid två olika dagar. Vid det första tillfället lämnar ingen bilen. Vid det andra tillfället går en person ut ur bilen och fram till grinden. Bilen är stulen. Avsikten är att systemet ska larma om att spaning mot anläggningen förekommer.

Scenario 3 beskriver en familj med barn och hund som kommer till en anläggning. Familjen har picknick en bit från anläggningen. Familjens barn och hund leker sedan en stund nära staketet. I detta fall ska systemet inte larma.

Tabellerna nedan beskriver de olika stegen i scenarionas händelseförlopp och de händelser som systemet registrerar. Dessutom beskrivs hur systemet ska agera då händelsen inträffar. Dessa olika sätt att agera finns:

- A0 – händelsen lagras lokalt och delges inte operatören.
- A1 – händelsen delges operatören för kännedom.
- A2 – larm skickas till operatören, för att initiera någon form av agerade.

Tabellernas information om systemagerande ska ses som ett förslag på hur systemet ska agera då dessa händelser inträffar. Exakt vilka händelser som ska presenteras för operatören och vilka som ska ge upphov till larm måste utredas vidare.

### 7.1 Scenario 1

Tabell 2: Scenario 1, del 1, kl. 16.27, 14 maj.

Steg	Händelser	Systemagerande
En röd Volvo närmar sig anläggningen och stannar i dess närhet.	Ett fordon Z närmar sig anläggningen. Fordon Z stannar vid plats p0.	A0
En man lämnar Volvon och går i riktning mot anläggningen.	En person X går emot anläggningen.	A0
Mannen är ca. 180 cm lång, bär grön rock och är flintskallig. Han kommer fram till anläggningens staket.	X kommer fram till staketet vid plats p1.	A0 X attribut registreras.
Han går längs staketet cirka 150 m. Han stannar under vandrigen två gånger och tittar in mot anläggningen.	X går runt staketet från plats p1 till plats p4. X observerar anläggningen vid plats p2. X observerar anläggningen vid plats p3.	A1
Mannen viker av och försvinner från anläggningen.	X går bort från anläggningen vid plats p4.	A0

Volvo startar och avlägsnar sig från anläggningen.	Fordon Z startar vid plats p0. Fordon Z åker ifrån anläggningen.	A0
--	---	----

Tabell 3: Scenario 1, del 2, kl. 00.16, 16 maj.

Steg	Händelser	Systemagerande
Samme man som besökte anläggningen två dagar tidigare går fram till staketet vid anläggningen.	En person Y kommer fram till staketet från väster vid plats B.	A0 Y attribut registreras.
Mannen tar fram en kamera och fotograferar anläggningen.	Person Y fotograferar vid plats B.	A1
Han följer sedan staketet cirka 50 m norr ut.	Person Y går runt staketet 50 m till plats C.	A1
Han tar sedan ytterligare fotografier här.	Person Y fotograferar vid plats C.	A1
Efter att ha slutfört fotograferingen avviker mannen från anläggningen och avlägsnar sig.	Person Y går ut från staketet till väster från C.	A0
Analytikern ställer en fråga till systemet om aktivitet vid anläggning A efter de meddelanden som inkommit.	Spaning mot anläggningen förekommer.	A2 Analytikern känner igen personen från två dagar tidigare.

### Sammanfattning:

I del 1 rapporteras en händelse till operatören, men inget larm. Händelseförloppet bedöms inte så allvarligt i det läget. Tre händelser rapporteras till operatören i del 2. Ingen av dessa händelser föranleder heller något larm. Vid analytikerns analys av dessa rapporterade händelser vid den aktuella anläggningen framkommer att en person har varit på platsen och gett upphov till sammanlagt fyra rapporterade händelser. En lämplig åtgärd vidtas av analytikern.

### Förmågor som visas:

Händelseförloppet visar systemets förmåga att:

- Upptäcka och lokalisera fordon.
- Upptäcka och följa en människa i anläggningens närområde.
- Följa en person mellan olika sensorers täckningsområden.
- Associera människor med fordon.
- Upptäcka fotografering mot anläggningen.
- Dra slutsatsen att spaning pågår mot anläggningen.

## 7.2 Scenario 2

Tabell 4: Scenario 2, del 1, kl. 23.46, 23 november.

Steg	Händelser	Systemagerande
En blå Volvo kommer körande längs tillfartsvägen till anläggningen.	Ett fordon Z närmar sig på tillfartsvägen.	A0
Bilen stannar framför grindarna med helljuset på i riktning mot grindarna. Ingen lämnar fordonet.	Fordonet Z stannar vid plats p0.	A0
Efter några minuter startar fordonet på nytt.	Fordonet Z startar vid plats p0.	A0

Fordonet vänder och kör åter ut via tillfartsvägen.	Fordonet Z kör längs tillfartsvägen från anläggningen.	A0
---	--	----

Tabell 5: Scenario 2, del 2, kl. 00.23, 24 november.

Steg	Händelser	Systemagerande
Samma blå Volvo kommer körande längs tillfartsvägen.	Ett okänt fordon Z kommer körande på tillfartsvägen.	A0
Bilen stannar framför grindarna med helljuset på och riktat in mot anläggningen. Bilen har registreringsnumret IQV 123.	Fordonet Z stannar vid plats p1.	A0 Fordonets attribut registreras.
En person går ur bilen och fram till grinden för att studera anläggningens lås.	En person X går ur bilen. Person X går fram till plats p2 (p2=grinden).	A0
Föraren går in i bilen igen.	Person X går tillbaka till bilen. Person X går in i bilen.	A0
Efter någon minut startas fordonet.	Fordon Z startar.	A0
Fordonet lämnar området via tillfartsvägen.	Fordon Z kör längs tillfartsvägen från anläggningen.	A0
Analytikern ställer en fråga till systemet om aktivitet vid anläggning A efter de meddelanden som inkommit. Han/hon studerar bilens registreringsnummer. Registreringsnumret visar sig tillhöra en stulen bil.	Bilen är troligen samma som besökte anläggningen tidigare. Fordonet med registreringsnummer IQV 123 är stulet.	A2 Fordonstypen denna dag associeras med fordonstypen dagen före.

### Sammanfattning:

Det finns inget skäl för ett fordon att vara vid denna anläggning på natten, varför systemet meddelar detta i del 1. Fordonet visar sig på nytt en dag senare. Vid detta tillfälle registreras fordonet tillräckligt väl för att registreringsskylten ska vara synlig. Fordonet visar sig vid senare analys av analytikern vara stulet.

### Förmågor som visas:

Händelseförloppet visar systemets förmåga att:

- Upptäcka och följa människor när de går ut ur och in i ett fordon.
- Upptäcka att det är samma fordonstyp som uppträder vid olika besökstillfällen.
- Upptäcka och lokalisera ett fordon på tillfartsvägen och i fjärrområdet.
- Dra slutsatsen att spaning mot anläggningen förekommer.
- Hantera information av underrättelsekaraktär, i detta fall information om att registreringsskyltarna på fordonet tillhör en stulen bil.

## 7.3 Scenario 3

Tabell 6: Scenario 3, kl. 12.20, 16 juni.

Steg	Händelser	Systemagerande
En familj på fyra personer, två vuxna, två barn och en hund kommer gående längs tillfartsvägen till anläggningen.	Fem individer X, Y, Z, W, V kommer gående tillsammans på tillfartsvägen. Två vuxna X, Y går till plats p0. Två barn Z, W går till plats p0. Ett djur V går till plats p0.	A0 Individernas attribut registreras och de klassificeras.
Familjen sätter sig ner en bit ifrån anläggningen och dricker kaffe. Familjen fikar under några minuter.	Personerna sitter tillsammans vid plats p0.	A0
Barnen i familjen går tillsammans med hunden runt anläggningen. Hunden springer en bit längs staketet. De vuxna sitter kvar vid platsen.	Personer Z, W och djur V springer runt anläggningen tillsammans. Personer X, Y sitter vid plats p0.	A0
Barnen återvänder till de vuxna med hunden efter att ha gått runt anläggningen.	Personer Z, W går till plats p0. Djur V går till plats p0.	A0
Familjen plockar ihop sina tillhörigheter och börjar promenera bort längs tillfartsvägen.	X, Y, Z, W, V går iväg tillsammans på tillfartsvägen.	A0

**Sammanfattning:**

Två vuxna, två barn och en hund vistas utanför en anläggning, men utför ingen handling som leder till meddelande eller till larm. Vistelsen dokumenteras och inga åtgärder vidas.

**Förmågor som visas:**

Händelseförloppet visar systemets förmåga att:

- Upptäcka och följa en grupp av människor och djur i fjärrområdet.
- Bestämma att de som finns på platsen tillhör samma grupp.
- Dra slutsatsen att situationen inte är hotande.
- Särskilja barn från vuxna.
- Särskilja människor från djur.

## 8. Systemutveckling och -integration

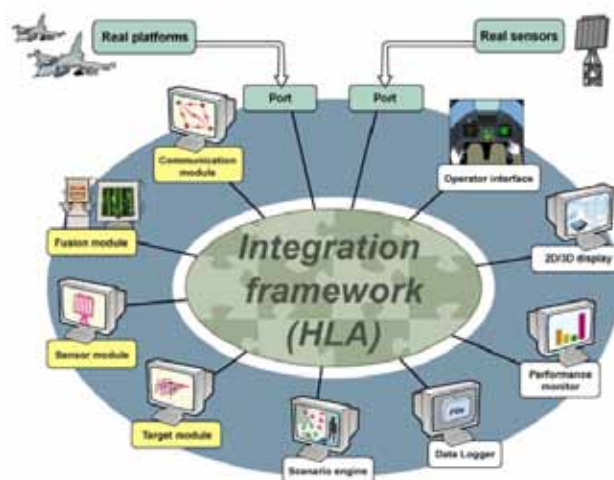
Detta kapitel beskriver ramverket MOSART samt hur detta kan nyttjas som en systemutvecklingsmiljö och som nätverk för systemintegration.

### 8.1 MOSART

MOSART är en informationsinfrastruktur baserad på HLA (High Level Architecture), se figur 8.1 och [DMSO, 2007]. Infrastrukturen möjliggör integration av olika system så att dessa kan utbyta data och därmed interagera i en och samma process. MOSART förenklar integrationen av systemkomponenter och därigenom möjligheten att demonstrera och utvärdera deras användning och funktion i mer omfattande sammanhang. MOSART tillhandahåller program-vara för simulering och effektiv integration av egen och kommersiell programvara. Dessa programvaror kan beskrivas i fyra olika kategorier:

- programvara för integration,
- programvara för simulering av händelseförlopp,
- integrerade forskningsresultat från olika projekt,
- utgångar till yttre datakällor.

I MOSART finns ett antal stödfunktioner för simulering, t. ex. en scenarioeditor och en scenariogenerator. Vidare finns stöd för visualisering i både två och tre dimensioner, dvs. förmåga att presentera kartor i såväl hög som låg upplösning samt kapacitet för presentation av syntetiska omgivningar i 3D. Verkliga, liksom simulerade, sensordata kan också visualiseras. Det finns också stöd för loggning av pågående aktiviteter. Slutligen finns också moduler som olika forskningsprojekt har integrerat och som kan återanvändas. Bland dessa moduler finns olika datafusionsalgoritmer.

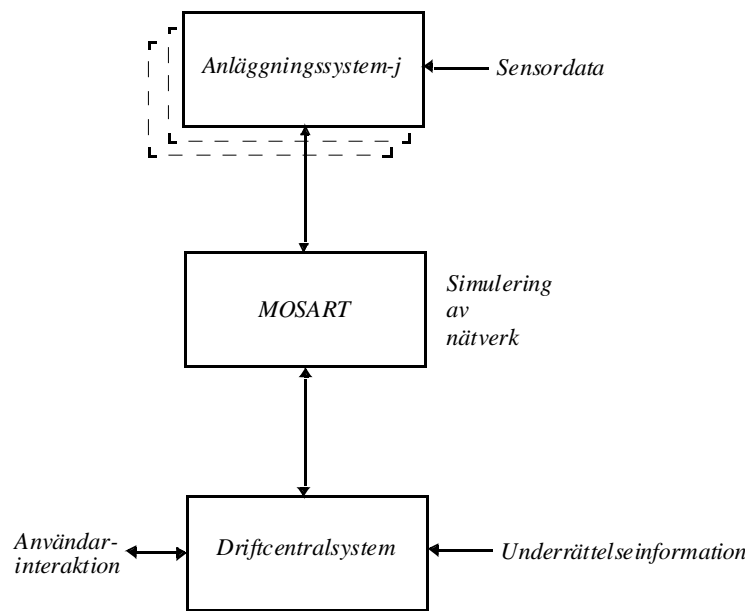


Figur 8.1. Ramverket MOSART och dess grundstruktur.

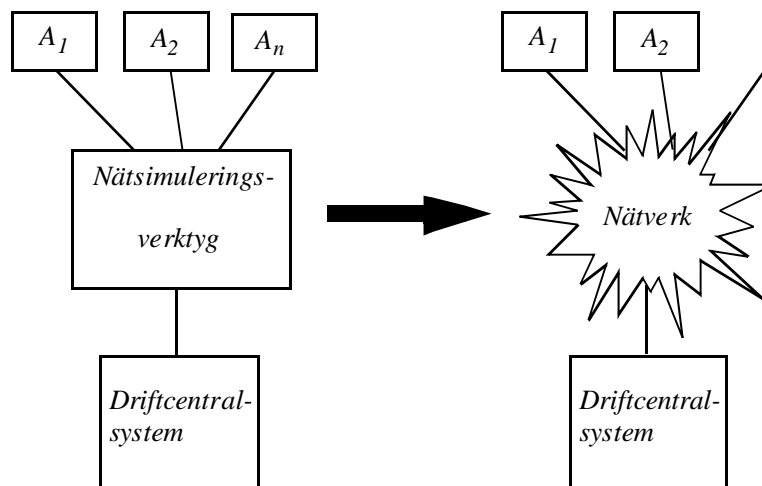
### 8.2. Systemutveckling med MOSART

Ramverket MOSART kommer genom enklare anpassningar att kunna nyttjas som den utvecklingsmiljö som de olika delarna av övervakningssystemet kommer att vara kopplat till. Dessutom kommer det att kunna användas för att simulera det nätverk ett färdigt system ska finnas i. Detta innefattar förmåga att integrera de olika systemmodulerna som utvecklas inom ramen för övervakningssystemet, samt att testa och demonstrera det slutliga systemet. De moduler som skall kopplas till MOSART utgörs främst av anläggnings- och driftcentral-systemen (figur 8.2). I demonstratorn kommer endast en modul av anläggningssystemet att ingå tillsammans med ett antal olika sensorer. Avsikten med denna arkitektur är att det senare skall vara enkelt att fasa ut nätsimuleringsdelen och koppla de olika systemdelarna direkt till det nätverk som skall användas för det slutliga övervakningssystemet (figur 8.3). Den före-slagna utvecklingsmiljön skall för anläggningssystemet också kunna utnyttjas för utveckling av algoritmer för dataanalys. Det samma

gäller även arbetet med utveckling av de moduler som ska ingå i driftcentralsystemet. MOSART kommer av denna anledning att spela en central roll vid utvecklingen av övervakningssystemet.



Figur 8.2. Utvecklingsmiljön med ramverket MOSART.



Figur 8.3. Illustration till hur nätsimuleringsverktyget skall kunna fasa ut och ersättas med det slutliga nätverket.

## 9. Sammanfattning

I denna rapport har de grundläggande principerna för ett systemkoncept för intelligent övervakning av skyddsanläggningar diskuterats. Konceptet syftar till att låta systemet samla in information om händelser vid anläggningarna med hjälp av sensorer och underrättelse-källor, samt utnyttja tekniska beslutsstöd för att ge beslutsfattaren tillgång till lämpligt beslutsunderlag. Konceptet baserar sig på:

- Övervakning utanför avspärrat område.
- Användning av multipla sensorer för övervakning.
- Sensorsamverkan.
- Automatisk identifiering av väsentliga händelser.
- En modulär, tjänstebaserad systemarkitektur.
- Generering av användaranpassat beslutsunderlag.

Systemkonceptet gör övervakning utanför avspärrat område möjlig. Huvuddelen av det system som beskrivs kan även användas för övervakning innanför avspärrat område. I detta fall finns emellertid inte samma behov av avancerade sensorer och avancerad analys som då systemet övervakar utanför avspärrat område. Övervakningssystemet omfattar delsystem för insamling av relevant information, vilket också innefattar analys av den insamlade informationen. Avsikten med analysen är att göra det möjligt att identifiera väsentliga händelser, de situationer som dessa händelser kan leda till och slutligen de konsekvenser situationen har för olika avnämare.

Väsentliga händelser är i första hand händelser som tyder på att någon planerar att genomföra någon form av intrång i, eller attack mot, en anläggning. Detta kan innefatta sådana allvarliga aktiviteter som terrorattacker, men också stöld eller vandalism. Ett system med en sådan förmåga kräver flera olika typer av sensorer som samverkar. Sensorsamverkan ger övervakningssystemet större möjligheter att klassificera objekt och följa väsentliga händelseförlopp. Därmed kan antalet falsklarm undertryckas kraftigt.

Det förslagna systemkonceptet grundar sig på moderna tekniker och metoder för komplexa informationssystem. Det ska utgöra grunden för ett tjänstebaserat övervakningssystem med målsättningen att förhindra att antagonistiska hot, stölder och vandalism iscensätts. Konceptet visar på möjligheter till anpassning till olika roller, vilket kommer att möjliggöra anpassning till olika användare med ökad effektivitet som följd. Viktiga egenskaper hos konceptets arkitektur utgörs av:

- Hög grad av modularitet med förmåga till evolutionär systemutveckling.
- Hög flexibilitet.
- Sensoroberoende.
- Robusthet mot förändring.

I konceptet är två roller identifierade. *Operatören* hanterar förekommande larm och kan följa vad som pågår vid de olika anläggningarna. *Analytikern* har till uppgift att följa upp och analysera vad som sker över tiden vid en eller flera anläggningar. Konceptet identifierar sex olika delar, s. k. sektioner. Av dessa sex sektioner återfinns fem i driftcentralsystemet; Driftcentralsektionen, Larmrapportsektionen, Operativsektionen, Kontextdatasektionen och Historiedatasektionen. Den sjätte sektionen, Anläggningssektionen, är multipel och kommer att återfinnas vid varje anläggning. Till varje Anläggningssektion kopplas ett antal sensorer, samt grundläggande förmåga till sensordata- och händelseanalys.

Det är möjligt att bygga en demonstrator som i allt väsentligt kommer att vara baserad på de grundläggande principer som finns beskrivna i denna rapport. En välstrukturerad och väldokumenterad demonstrator kommer också att kunna produktifieras med stöd av FOI. Vidare kommer man att kunna använda detta arbete som ett beslutsunderlag för att också i fortsättningen kunna förbättra sin övervakningsverksamhet, sitt systemutvecklingsarbete och sin förmåga att

upphandla ändamålsenliga system för övervakning. Ett system av detta slag, med utbytbara systemmoduler, kan enkelt anpassas till de föränderliga krav och behov som uppstår som en följd av förändrade hotbilder.

## Referenser

[Ahlberg, 1992] Ahlberg C., Williamson C. och Shneiderman B. (1992), *Dynamic queries for information exploration: an implementation and evaluation*, in 'Proc. of Conference on Human Factors in Computing Systems (CHI 92)', ACM Press, pp. 619-626.

[Burigat & Chittaro, 2007] Burigat S. och Chittaro L. (2007), *Interactive Visual Analysis of Geographic Data on Mobile Devices based on Dynamic Queries*, accepted for publication in the Journal of Visual Languages and Computing, Elsevier.

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

[DMSO, 2007] <https://www.dmsomil/public/transition/hla/>, senast besökt 2007-06-20.

[Hall & Llinas, 2001] Hall D. L. och Llinas J. (Eds.) (2001), *Handbook of multisensor data fusion*, CRC Press, New York.

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

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

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

[Jungert & Lantz, 2006] Jungert E. och Lantz F. (2006), *Intelligent skydd mot intrång i skyddsobjekt – metoder och tekniker*, FOI, Linköping, Sverige, FOI-R-1993-SE.

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

[Nastell, 2002] Nastell P. (2002), *Teknisk och Personell Bevakning, Realiserbarhetsstudie*, 2002-05-30, Slutrapport, Svenska Kraftnät, Stockholm, Sverige.

[Rodosek, 2003] Rodosek G.D. (2003), *A generic model for IT services and service management*, IFIP/IEEE Eighth International Symposium on Integrated Network Management, pp. 171-184.

[Rust, 2003] Rust R. T. och Kannan P. K. (2003) *E-service: A new paradigm for business in the electronic environment*, Communications of ACM, June, vol. 46, issue 6.

[Stenumgaard, 2004] Stenumgaard P., Wenngren G., Tullberg H., Nilsson J., Grönkvist J., Cronström P., Lindström J., Hallberg J., Hallberg N., Grahn P. och Andersson R. (2004), *Tjänstebegreppets användning inom olika tillämpningsområden*, Linköping, FOI 2004, (FOI-R--1211--SE).

[Wiss & Kindvall, 2004] Wiss Å. och Kindvall G. (red.) (2004), *FOI Orienterar om Sensorer*, nr 3, 2004, FOI, Stockholm, Sverige, ISBN 91-7056-119-2.

