Generiskt VMS

En översikt

LARS BERGLUND GUSTAF OLSSON

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

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

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

www.foi.se

FOI-R--3408--SE
ISSN 1650-1942 Januari 2012

Lars Berglund Gustaf Olsson

Generiskt VMS

En översikt

Titel	Generiskt VMS - En översikt
Title	Generic EW Defensive Suit - An overview

Rapportnr/Report no	FOI-R--3408--SE
Sidor/Pages	30 p
Månad/Month	Januari
Utgivningsår/Year	2012
ISSN	ISSN 1650-1942
Kund/Customer	FM
Projektnr/Project no	E54013
Godkänd av/Approved by	Jonas Palm

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Sensor- och TK-system
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Sensor and EW Systems
Box 1165
SE-581 11 Linköping

Sammanfattning

Denna rapport är utgiven inom ramen för projektet VMS Marin Miljö inom FoT-område Telekrig. Rapporten beskriver hur ett generiskt Varnar- och Motverkanssystem (VMS) bör vara uppbyggt och vilka funktioner det behöver ha.

Med generiskt VMS avses här en generell systemuppbyggnad av VMS som ska kunna appliceras på alla typer av plattformar. Huvudsakligt fokus ligger på enskild plattform.

Rapporten vänder sig till de som arbetar med eller ska arbeta med VMS.

Det generiska VMS:et är indelat i tre huvudkomponenter, sensorsystem, logikenhet samt motverkanskanaler. Som motverkan inkluderas även ”hard kill” funktionen för att kunna erhålla ett optimalt VMS.

För att kunna få ett mer optimalt VMS har följande områden identifierats som kommer att kräva ett fördjupat arbete vad avser VMS.

- Integration med ledningssystem
- Operatörsstyrda sensorsystem
- Biblioteksfunktioner
- Omhändertaget hot
- Insatsuppföljning

Syftet är att den framkomna beskrivningen i rapporten ska kunna tjäna som en ”road map” för kommande VMS.

Nyckelord: VMS, sensorer, motverkan, motmedel, telekrig

Summary

This report is published by the FOI project" Defensive Aid Suit in Maritime Environment" in the research area of Electronic Warfare. The report describes frame and function for the parts needed for a generic Defensive Aid Suit (DAS).

By generic DAS a general description of the building blocks and functions that defines DAS. The generic DAS should be applicable to all types of platforms.

Main focus is on single platform. The report should be read by those who are working with or those who are about to start work with DAS.

The generic DAS consists of three major parts, sensor systems, logic unit and counteraction systems. In counteraction systems both soft kill and hard kill are included in order to achieve an optimized DAS.

Some areas of research have been identified that requires more studies in order to get a DAS that is fully functional. These areas are:

- Integration with the Command and Control System
- Sensor systems handled by operators
- Library functionality
- When is a threat considered taken care of depending on counter action
- Evaluation of chosen counteraction

The purpose with this report is to serve as a guide for personal working with questions related to DAS.

Keywords: DAS, sensors, counter action, countermeasure, EW

Innehåll

1 Inledning

Denna rapport är utgiven inom ramen för projektet VMS Marin Miljö inom FoT-område Telekrig, och bygger på det arbete som gjorts i ett tidigare FoT-projekt ”*Framtida behov inom VMS”* avseende generiskt koncept för Varnar- och MotverkansSystem (VMS). Med generiskt VMS avses här en generell systemuppbyggnad av VMS som ska kunna appliceras på alla typer av plattformar. Rapporten vänder sig till de som arbetar med eller ska arbeta med VMS.

1.1 Bakgrund

En viktig del inom telekriget är VMS som plattformsskydd. Den klassiska bilden av VMS är ett system som är avsett för en plattforms egenskydd. I första hand skall det möta och avvärja hot som helt plötsligt och i vissa fall oförväntat ”dyker” upp. Dagens VMS är till mycket stor del baserat på telekrig. Detta innebär att fysisk bekämpning av en robot enligt denna traditionella definition faller utanför begreppet VMS.

VMS-funktionen, betraktad i ett förbandsperspektiv, kräver att synen på VMS vidgas. Från att enbart betraktas som ett system med syfte att ge ökad överlevnad för enskild plattform till ett system som medför ökad överlevnad för förbandet.

Denna vidgade syn kan ge VMS en mer offensiv roll vilket också medges om VMS för förband utnyttjas på ett riktigt och genomtänkt sätt. Här kan VMS innefatta motverkan i form av fysisk bekämpning med egna hard kill-system.

Under ett tidigare FoT-projekt *VMS Internationella Insatser* genomfördes studier som visade på stora svårigheter att kunna utnyttja ett delsystem från ett VMS för en typ av plattform till en annan.

Främsta orsaker till detta är olika plattformars krav vad avser vikt, utrymme, installation etc. Plattformarna verkar dessutom i olika insatsmiljöer med varierad hotbild avseende såväl våglängdsområde som stridsavstånd. Detta ställer i sin tur olika krav på reaktions-tider, sensorers täckningsområde, upplösning och räckvidd samt olika typer av motverkan.

Tankar väcktes på att finna ett koncept för hur ett generellt VMS bör vara uppbyggt.

1.2 Introduktion

Idéen är att ett generiskt VMS-koncept ska kunna stå som modell för ett framtida försvarsgrens- och plattformsgemensamt VMS. Då plattformar ska kunna samverka i tillfälligt sammansatt förband (stridsgrupp) finns behov av att samordna VMS åtgärder. Detta ställer krav på fungerande kommunikation (tal och data) och kompatibla ledningssystem med lägesinformation som kan presenteras och behandlas på ett sätt som är ändamålsenligt.

Ett sådant förslag till försvarsmaktsgemensamt VMS-koncept bör baseras på en gemensam grundfilosofi. Vidare skall hänsyn tas till att plattformars VMS ska kunna anpassas för såväl enskilt uppträdande som förbandsuppträdande. Denna anpassning ska kunna ske dynamiskt. Det försvarsgemensamma VMS-konceptet bör baseras på en modulärt uppbyggd arkitektur med flexibel konfigurering som kan anpassas efter aktuell insatsmiljö (uppdrag, hotbild, atmosfärsförhållanden etc.).

Denna rapport beskriver ett förslag på ett generiskt VMS uppbyggnad och funktioner, med huvudsakligt fokus på enskild plattform.

2 Översiktlig systembeskrivning

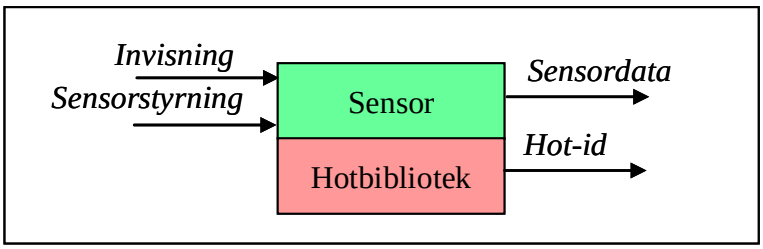
Det föreslagna VMS-konceptet bygger på tre delkomponenter:

- Sensorsystem
- Motverkanskanaler
- Logikenhet

Delkomponenterna bör så långt det är möjligt ha försvarsmakts-gemensamma gränssnitt och protokoll för att underlätta framtida integration.

2.1 Sensorsystem

Med sensorsystem avses i denna rapport ett system som innehåller en eller flera sensorer med tillhörande sensorstyrning, signalbehandling och eventuellt hotbibliotek. Sensorsystemet levererar sensordata och/eller hotinformation via försvarsgrensgemensamt gränssnitt och protokoll. I begreppet sensorsystem ingår varnare, en funktion i ett sensorsystem kan vara varning.



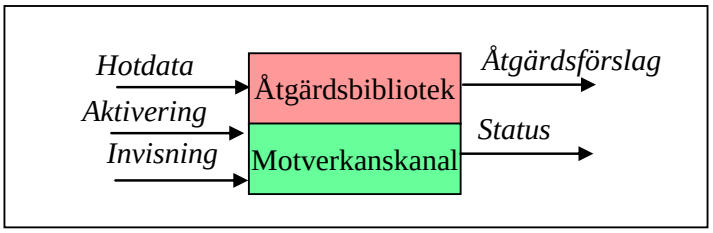
Figur 2.1 *Schematisk beskrivning av ett sensorsystem innehållande sensor och hotbibliotek, samt in och utsignaler.*

Invisning (geometrisk orientering) och styrning (inställning av parametrar) av sensorsystem ska kunna ske baserat på data från annat sensorsystem eller av operatör. Sensordata kan bestå av parameterdata, riktning och avstånd, upptäcktstid etc. I de fall då sensordata kan matchas mot data i hotbiblioteket kopplas ett hot-id till sensordata. Detta kan bestå av signal-id, hottyp, hotklass (t.ex. fientligt, eget, okänt).

Sensorsystem med liknande funktioner, för olika plattformar, bör arbeta enligt liknande signalbehandlingsprinciper i syfte att underlätta korrelation av sensorinformation inom förband. T.ex. bör radarvarnare utnyttja samma princip för pulssortering. Dessutom förenklas FM biblioteksproduktion. Internationella operationer i nya områden kräver att hotbiblioteken kan uppdateras med korta omloppstider.

2.2 Motverkanskanaler

Motverkanskanaler avser system för motverkan mot detekterade hot. Exempel på motverkanskanaler är fysisk bekämpning (pjäs, lv-robot, kanon/ksp), motmedelskastare/fällare och störsändare. Motverkanskanalen kan utnyttjas tillsammans med manöver (fart, riktning) för att öka effekt av insatsen. I systemet kan ingå signaler för styrning, statusövervakning och aktivering samt ett åtgärdsbibliotek för optimering av insats. Åtgärdsbiblioteket utnyttjar tillgängliga hotdata, vind, data för egna plattformar för beräkning av optimal motåtgärd med tillhörande utfallssannolikhet. Den beräknade optimala motåtgärden kan inkludera manöver.



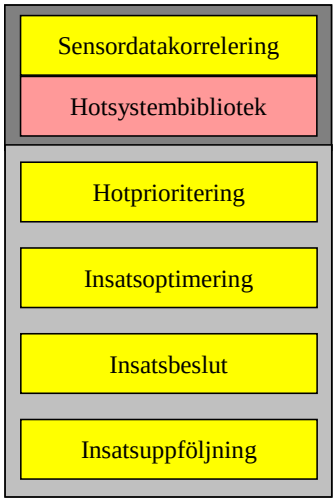
Figur 2.2 *Schematisk beskrivning av ett motverkanssystem innehållande motverkanskanal och åtgärdsbibliotek, samt in och utsignaler.*

Godkänns åtgärdsförslaget invisas och aktiveras motverkanskanalen. Invisning (geometrisk orientering) och/eller aktivering av motverkanskanalen ska kunna ske baserat på data från annat sensorsystem eller av operatör. Motverkanskanalen skall kunna rapportera status med avseende på tillgänglighet, utförd insats och felfunktion.

Samtliga tillgängliga motverkanskanalers åtgärdsbibliotek skall lämna värden på utfallssannolikhet. Dessa jämförs för att välja optimal motverkanskanal. I likhet med hotbibliotek för sensorer krävs att åtgärdsbiblioteken skall kunna uppdateras med korta omloppstider, genom FM försorg.

2.3 Logikenhet

Logikenheten skall vara länken mellan sensorsystemen och motverkanskanalerna samt utgöra gränsyta mot eventuellt ledningssystem. Logikenheten består av följande delar: sensordatakorrelering, hotprioritering, insatsoptimering, insatsbeslut och insatsuppföljning, enligt figur nedan.



Figur 2.3 *Schematisk uppbyggnad av logikenheten. Sensordatakorrelering med tillhörande hotsystembibliotek kan antingen ingå i ledningssystemet eller i logikenheten VMS.*

Sensordatakorrelering inhämtar data (sensordata) och information (hot-id) från plattformens egna sensorer samt eventuellt samverkande enheter (det senare kräver fungerande kommunikation). Inhämtad data och information fusioneras och korreleras mot hotsystembiblioteket. Detta innehåller data för aktuella plattformar och system (egna och andra) i operationsområdet, bl.a. sensorers hot-id, hastighet, räckvidder. Korreleringen syftar till att skapa en tydligare lägesbild samt en säkrare klassificering av eventuella hot. Data ut från sensorkorreleringen är upptäckta hot med tillhörande sensordata och hotsystem-id (obs att hotsystem-id inte behöver vara samma som hot-id).

Hotprioriteringens uppgift är att sammanställa och prioritera upptäckta hot. Syftet är att prioritera i vilken ordning hoten skall motverkas. Prioriteringen kan bygga på predikterad

ankomsttid till antingen egen plattform eller angivet skyddsobjekt vid förbandsuppträdande alternativt vilken skadeverkan hotet kan ge. Resultatet från hotprioriteringen är en lista av aktuella hot (med tillhörande information) i prioritetsordning.

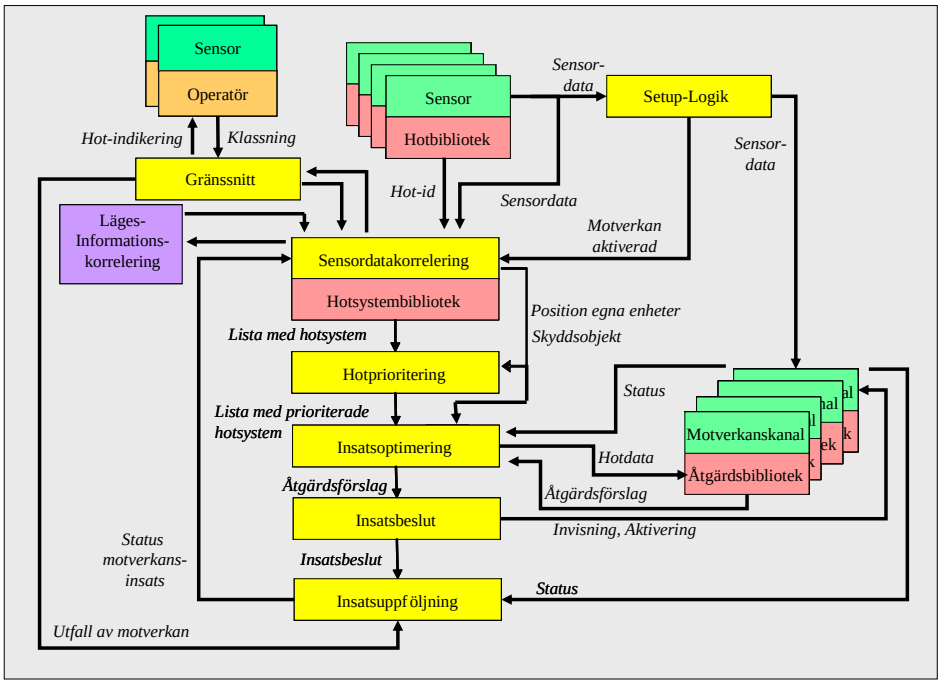
Insatsoptimering har till uppgift att utgående från aktuell hotprioritering optimera och presentera förslag till plattformens eller förbandets motåtgärder. För aktuell hotsituation inhämtas status från tillämpliga motverkanskanaler. Om tillämpliga motverkanskanaler är tillgängliga skickas hotinformation för beräkning av utfallssannolikhet för respektive motverkanskanal. Dessa utfallssannolikheter jämförs och den med högsta utfalls-sannolikhet väljs och presenteras som insatsförslag.

En viktig faktor som styr insatsoptimeringen är plattformens eller förbandets handlingsregler för att kunna hantera aktuella hotsituationer. Styrande för handlings-reglerna är bl.a. ROE, uppdrag, insatsmiljö etc. Dessa handlingsregler måste kunna anpassas dynamiskt och ingå som en del i uppdragsplanering. I insatsoptimeringen skall det finnas möjligheter att välja huruvida insatsbeslut skall aktiveras manuellt, semiautomatiskt eller automatiskt.

I insatsbeslut effektueras föreslagen motverkansåtgärd. Detta kan innebära styrning av såväl sensorer som motverkanskanaler samt manöver. Beslutet kan effektueras manuellt (operatör väljer mellan flera förslag), semiautomatiskt (föreslagen åtgärd bekräftas av operatör) eller automatiskt. I samband med effektuering skickas åtgärdsförslaget vidare till eventuell uppföljning med aktuellt hot markerat som ”under åtgärd” med vald motåtgärd.

I insatsuppföljning hanteras felfunktioner hos motverkanskanalerna genom en kontinuerlig uppföljning av pågående insatser. Vid felfunktion skickas status till hotprioritering för eventuell förnyad insats med annan motverkanskanal. I en framtida funktion kan uppföljning kompletteras med sensorinformation för motverkansbedömning, för att avgöra om insatt motverkan hade tillräcklig effekt eller om det behövs en ny insats.

I figuren nedan redovisas principen för ett generellt VMS baserat på texten ovan.



Figur 2.4 *Generell struktur som kan användas för alla typer av plattformar med eller utan ledningssystem för att underlätta samverkan mellan olika plattformar och förband. Observera att i figuren visas samma motverkanskanal på två ställen för att tydliggöra dataflödet. Notera att insatsbeslutet kan komma att styra invisning av sensorer som i sin tur ger invisning av motverkanskanal.*

3 Ingående biblioteksfunktioner

Det finns tre stycken biblioteksfunktioner i generiskt VMS. Dessa är:

- Hotbibliotek
- Hotsystembibliotek
- Åtgärdsbibliotek

Hotbibliotek är kopplat till respektive sensorsystemen och hotsystembibliotek är kopplat till sensordatakorreleringen. Åtgärdsbibliotek är kopplade till respektive motverkanskanal. En något fylligare beskrivning ges nedan.

I beskrivningarna av hotbibliotek och hotsystembibliotek används begreppen hottyp, hotklass samt hotsystem. Med hottyp avses t.ex. robotsystem. Med hotklass avses vilken klass av hottyp som avses såsom t.ex. trådstyrd, laserutpekare, laserledstråle eller ”fire and forget”. Med hotsystem avses det specifika systemet t.ex. TOW, Hellfire eller motsvarande.

3.1 Hotbibliotek

Till varje sensorsystem i VMS kopplas ett hotbibliotek. Hotbibliotekets uppgift är, att utgående från de parametrar som sensorsystemet har detekterat, typbestämma, klassificera alternativt identifiera det detekterade objektet/systemet.

Värt att notera att hur väl ett hotbibliotek kan stötta ett sensorsystem beror dels på hur själva sensorsystemet kan extrahera data från mottagna signaler dels på hur väl parametersatt själva biblioteket är.

För vissa sensorsystem kommer således hotbiblioteket endast tillåta att hottyp kan bestämmas. För andra sensorsystem kan mottagna signaler även medge inte bara hottyp utan även hotklass och hotsystem.

Observera att i hotbibliotek ska även parametrar för egna system finnas inlagda.

3.2 Hotsystembibliotek

Hotsystembibliotekets uppgift är att tillhandahålla information om de hotsystem som bedöms vara aktuella inom operationsområdet. Hotsystembiblioteket innehåller en beskrivning av hotsystemens egenskaper såsom

- Plattform
- Manöverförmåga
- Sensorer
- Vapen och verkansdelar

Innehållet i hotsystembiblioteket (data för klasser av hotsystem eller specifika hotsystem) ska matchas med sammanvägda sensordata. Syftet med hotsystembiblioteket är att stötta sensordatakorreleringen med att koppla ihop aktuell sensorinformation och klassificera och/eller identifiera vilka typer av vapensystem som används mot egen plattform eller förband. Huvudsakliga syftet är dock att förse VMS med indata för optimering av motverkansinsats.

På motsvarande sätt som i hotbibliotek är det viktigt att egna plattformar och system finns beskrivna i hotsystembiblioteket.

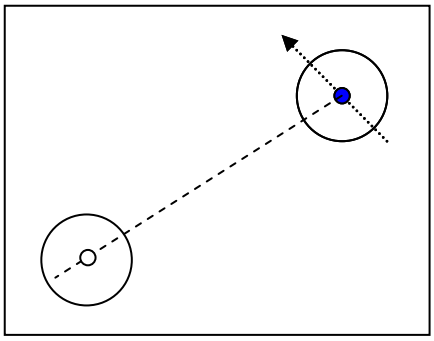
3.3 Åtgärdsbibliotek

För varje motverkanskanal (åtgärd som kan vidtas för att slå ut hotet alternativt undvika bli träffad) som en plattform har tillgång till kopplas ett åtgärdsbibliotek. Åtgärdsbibliotekets uppgift är att:

- Tillhandahålla status för motverkanskanalen
- Ge uppgift om hur lång tid som åtgår för motverkanskanalen att ”åtgärda” hotet
- Ge ett bedömt värde på hur framgångsrik åtgärden är för aktuell situation

4 Positionering

Vid enskilt uppträdande av plattform är den egna absoluta positionen (i jordfast koordinatsystem) inte av lika stort intresse som i förbandsuppträdande där hot/mållägen ska skickas vidare till andra plattformar. Det kan ändå vara av betydelse att få dokumenterad information om var plattformen blev utsatt för bekämpning.



Figur 4.1 *Osäkerhet i egen position kommer att påverka hur noggrannheten i lägesbestämning av upptäckta mål kan göras.*

4.1 Andra plattformars position inom eget förband

Egna sensorer kan komma att detektera egenskaper eller signaler från andra egna plattformar, dessa kommer då att bilda plattformsspår i sensordatakorreleringen. För att dessa inte ska gå vidare som hot måste de kunna utpekas som egna enheter. Detta kräver information om var övriga enheterna befinner sig, vilket underlättas med t.ex. ”Blue Force tracking”.

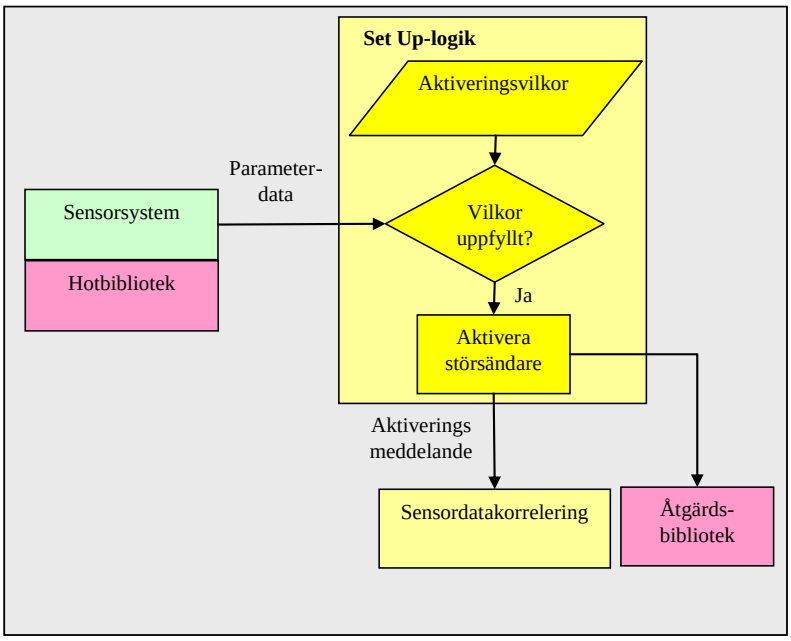
5 Set up-logik

Det kan för ett VMS vara viktigt att, i vissa fall, mycket snabbt svara på mottagen sensorinformation för att snabbt motverka det detekterade hotet. Därför bör sensorinformation kopplas via en logik, som kan anpassas och förprogrammeras inför varje uppdrag beroende på uppdrag, till en given motverkanskanal. Denna logik kallas här set up-logik.

Vanligtvis torde detta vara aktuellt vid användandet av framför allt störsändare, där en varnare/mottagare utnyttjas för att starta en störsändare. Skulle logikkedjan sensordata-korrelering, hotprioritering, insatsoptimering, insatsbeslut och motverkan utnyttjas åtgår för lång tid innan insats varför det finns risk att motverkan måste göras både mer komplicerad och kräva mer effekt.

Syftet med set up-logiken är att så snabbt som möjligt påbörja störning då ju tidigare störinsatsen påbörjas ju effektivare blir störinsatsen.

I många VMS kanske denna del av logiken inte är nödvändig medan det för andra system kan vara av yttersta vikt.



Figur 5.1 Funktionalitet hos set up-logiken.

6 Sensorsystem

Som beskrivits tidigare avses med sensorsystem ett system som innehåller en eller flera sensorer med tillhörande sensorstyrning, signalbehandling och eventuellt hotbibliotek.

Sensorsystemet ska samla in signaler/data från omgivningen och utifrån dessa skapa målspår för de mål/hot som upptäckts. Med målspår menas att konsekutiva detektioner av ett och samma objekt knyts samman till ett och samma målnummer, internt för sensorsystemet. När ett målspår etablerats kan detta sedan rapporteras vidare till sensordatakorreleringen. Så länge som sensorsystemet detekterar objektet uppdateras målspåret. För att detta ska kunnas genomföras krävs att sensorsystemet har tillgång till information om egen plattforms position. När ett hot/mål har detekterats och målspår skapats görs en korrelering mot den databas som finns i sensorsystemets hotbibliotek. När korreleringen av detekterade data har gjorts gentemot hotbiblioteket skickas en sensorrapport till sensordatakorrelering.

Ett skäl till att inte rapportera ett upptäckt objekt/mål/hot direkt är bl.a. för att minska antalet falsklarm och samtidigt ge säkrare data om det upptäckta målspåret.

En sensorrapport bör innehålla följande information:

Parameter	**Förklaring**
Rapporterande sensorsystem	
Sensortyp	Klass av sensor
Sensoridentifikation	Unikt nummer på hårdvaran
Målspårs-id	Observation över tiden för denna sensor
Observationstid tidigaste	
Observationstid senaste	
Klassificering	
Position mål	Bäring/avstånd alternativt position
Kurs mål	
Hastighet mål	
Noggranhet	
Position rapporterande sensor	Vid senaste observationstid
Rådata	Extraherade data såsom frekvens, pulsmodulering med mera.

Tabell 6.1 Innehåll i sensorrapport som sänds från sensorsystem till sensordata-korreleringen.

I praktiken finns två varianter av sensorsystem:

- Autonomt sensorsystem (laservarnare, robotskottvarnare, optikspanare, ESM)
- Operatörsstyrt sensorsystem (sikten)

6.1 Autonomt sensorsystem

Med autonomt sensorsystem avses ett sensorsystem som utan hjälp från operatör inhämtar signaler från omgivningen, behandlar dessa och rapporterar vidare. Vidare bör dessa sensorsystem skapa interna målspår för fortsatt följning. För att skapa ett målspår krävs ett antal detektioner (eller detektion under en viss tid). Detta kräver i sin tur att sensorsystemet har tillgång på den egna plattformens position för att kunna göra en så korrekt lägesbestämning som möjligt.

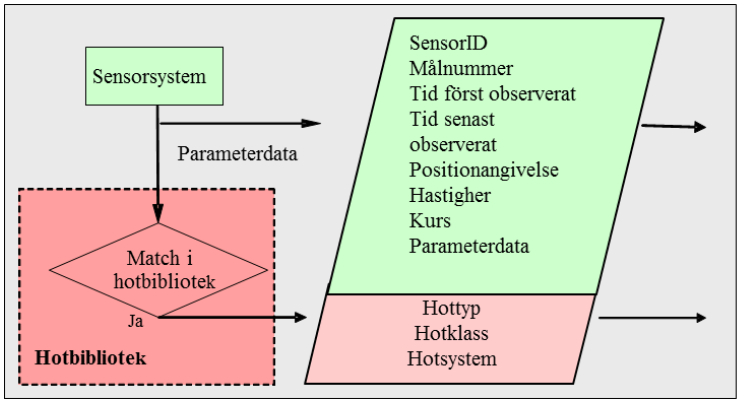
Exempel på denna typ av sensorsystem är radarvarnare, laservarnare och robotskottvarnare.

6.1.1 Hotbibliotek

Extraherade parametrar från signalbehandlingen i sensorsystemen är ingångsparametrar för hotbiblioteken. Hotbibliotekets uppgift är att bestämma vilken typ av hot, vilken klass det tillhör samt vilket system det är.

Under förutsättning att ett hotbibliotek är rätt parametersatt, så är hotbibliotekets möjlighet att bestämma hotet begränsat av dess inparametrar d.v.s. sensorsystemets möjligheter att kunna extrahera parametrar.

Som nämndes i avsnitt 3.1 Hotbibliotek är det viktigt att egna system finns beskrivna.



Figur 6.1 *Sensorsystem med tillhörande hotbibliotek (emitterbibliotek). Sensor ID är identifikationen för rapporterande sensor. Målnummer är det sensorsystemets interna målnummer för det detekterade objektet. Med positionsangivelse menas riktning, avstånd, höjd alternativt position i x, y och z (jordfast koordinatssystem).*

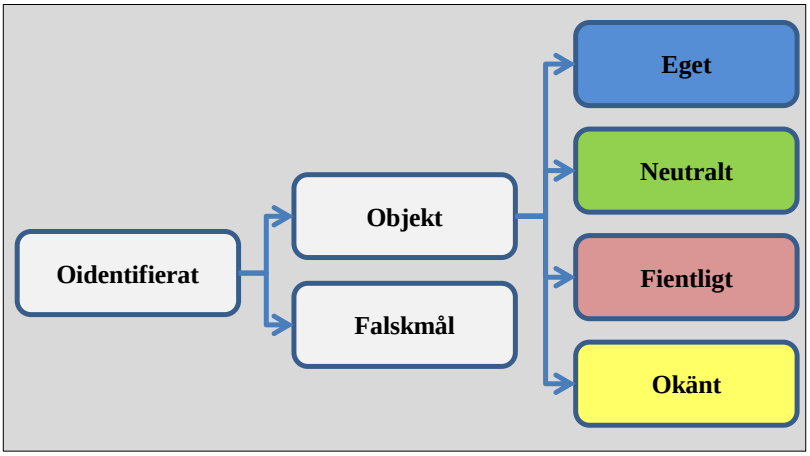
6.2 Operatörsstyrt sensorsystem

Med operatörsstyrt sensorsystem avses system såsom optiska sikten där operatören spanar och klassificerar/identifierar mål/hot. Denna typ av sensorsystem kan sakna egen logik och stöttas av operatör för att kunna klassificera upptäckta mål.

6.2.1 Klassificering

Ett operatörsstyrt sensorsystem har oftast idag inget hotbibliotek kopplat till sig. Där hotbibliotek saknas utgörs detta av operatören. Självklart påverkas operatörens möjligheter att kunna klassificera/identifiera upptäckta objekt av utbildning och träning. Men det kommer även att behövas ett gränssnitt som möjliggör inmatning av operatörens klassning/identifiering.

I vissa fall kommer automatiska sensorsystem att kunna indikera upptäckta hot varvid en invisning av ett operatörsstyrt sensorsystem sker för att låta en operatör bestämma om det är ett hot eller inte. För att kunna märka det interna målspåret i VMS:et med den klassningen som operatören gör behövs möjligheten att mata in klassning av det objekt som observerats. Vid klassningen är det inte bara typ av objekt utan också tillhörighet (eget, neutralt, fientligt eller okänt). Även falskmål (med falskmål i detta fall avses naturliga sådana) ska också kunna hanteras.

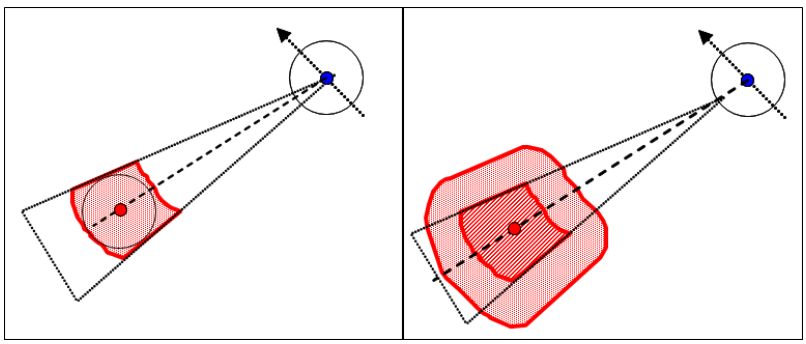


Figur 6.2 Klassificering av upptäckt objekt.

Ett av de största problemen är hur en operatör ska kunna mata in klassning till VMS:et utan att förlora tid. Detta är framför allt viktigt då det upptäckta objektet har klassificerats som fientligt av operatören. En lösning skulle kunna vara att operatören initierar motverkan mot det upptäckta objektet varvid VMS:et fås att förstå att objektet är fientligt. Vilken typ/klass av objekt som motverkas kan då klaras ut efter genomförd motverkan.

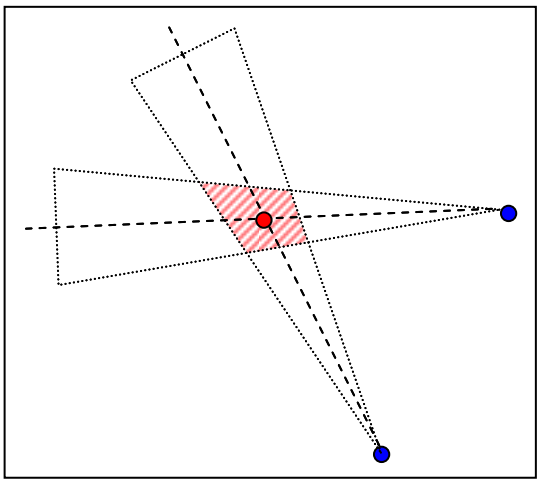
6.3 Lägesbestämning

För att kunna lägesbestämma (positionsbestämma) ett upptäckt hot/mål krävs att det aktuella sensorsystemet känner till den egna plattformens position och orientering. Med ett aktivt sensorsystem kan i många fall både avstånd och bäring erhållas. Men om sensorsystemet är passivt så kan endast en bäring erhållas. I figur 4.1 är riktningen/bäringen från mätande plattform till det upptäckta objektet utmärkt med en linje. Detta är fallet för ett idealt system. I praktiken kommer riktningsbestämningen att ligga inom ett osäkerhetsintervall (olika för olika sensorsystem). På motsvarande sätt kommer det uppmätta avståndet att ligga inom ett osäkerhetsintervall, se figur 6.3.



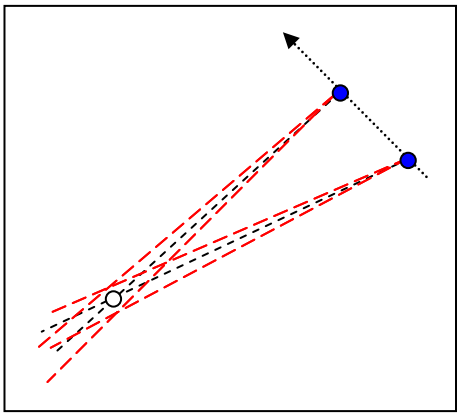
Figur 6.3 Osäkerhet i vinkel och avstånd vid mätning ger upphov till ett osäkerhets-område inom vilket det upptäckta målet kan vara (vänstra figuren). För ett passivt system är osäkerhetsområdet lika med hela vinkelområdet. Osäkerheten i egen position ökar ytterligare området där det upptäckta målet kan befinna sig (högra figuren).

För passiva sensorsystem skulle vid förbandsuppträdande den sammanvägda informationen (målspår från två sensorsystem på olika plattformar) utnyttjas för triangulering och bestämning av det upptäckta objektets position, se nedan.



Figur 6.3 *Osäkerhet vid mätning av vinkel hos de två sensorsystem ger upphov till ett osäkerhetsområde inom vilket det upptäckta målet troligtvis uppträder.*

För ett passivt system är det fortfarande möjligt att efter en tid kunna bestämma positionen för det upptäckta målet genom att utnyttja egentriangulering. Vilket innebär att egen förflyttning utnyttjas för att kunna triangulera fram målets position, dock kräver det att sträckan mellan de punkter där mätning sker är tillräckligt lång och lämplig för att inte osäkerhetsområdet skall bli för stort.

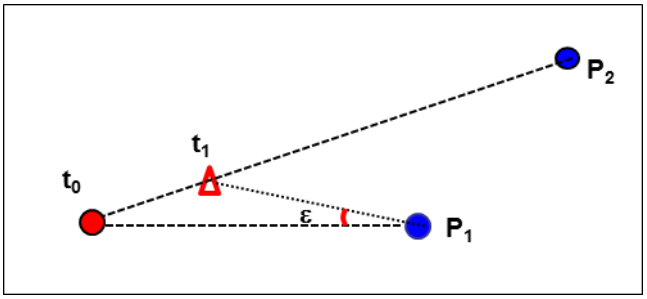


Figur 6.3 *Genom att bestämma bäring till målet vid två olika tidpunkter kan, om den egna positionen är känd vid dessa tillfällen, målets position trianguleras fram.*

6.4 Bestämning av robots anflygningskurs

För sensorsystem med varningsfunktion för inkommande robot gäller det att avgöra om roboten är på väg mot den egna plattformen eller inte. I samband med förbandsuppträdande kan det vara svårt att avgöra vilken av plattformarna i förbandet roboten styr mot.

För att kunna avgöra hotets kurs relativt den egna plattformen studeras ändring i vinkel mellan robotens position sett från den egna plattformen, som funktion av tid. Tiden får inte vara för lång. Se figur 6.4.

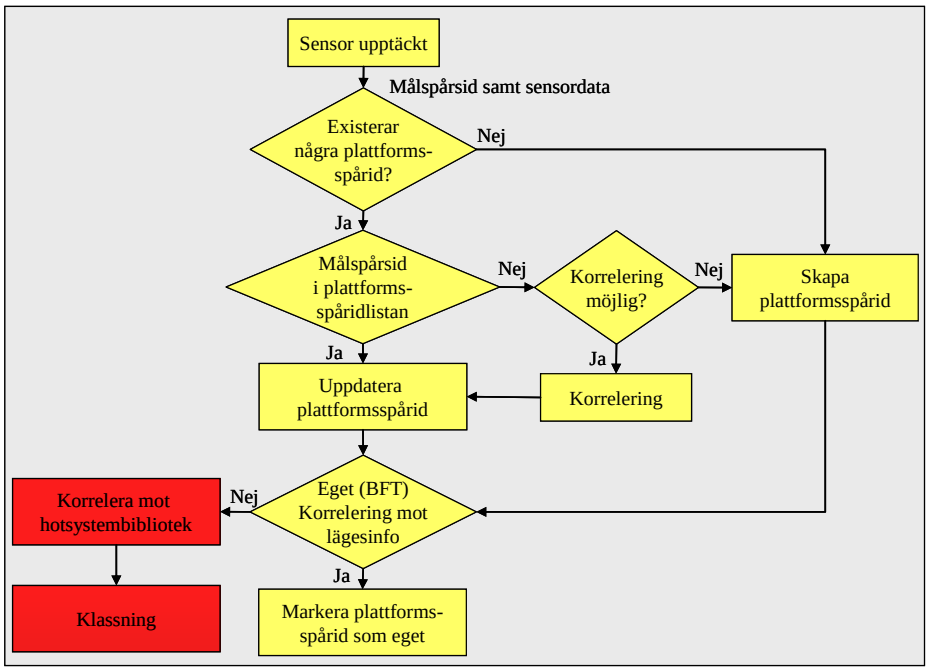


Figur 6.4 *Illustration av problemställning hur två plattformar kan avgöra vilken plattform ett robothot har sikte på. Sensor på plattform 1 (P_1) detekterar roboten vid tiden t_0. Sensorsystemet följer roboten och efter en tid (bestämd av sensorsystemet) vid tiden t_1 kan vinkeländringen ε bestämmas. Storleken på vinkeländringen kan utnyttjas för att bestämma om hotet är på väg mot plattform 1 eller inte.*

Problemställningen är geometriberoende och även om sensorsystemet klarar av att detektera små värden på ε kommer det att vara svårt att avgöra vilken av plattformarna hotet är på väg mot.

7 Sensordatakorrelering

Funktionen för sensordatakorreleringen är i grunden datafusion. Här ska de olika målspåren från respektive sensorsystem korreleras mot varandra för att se om de representerar ett och samma eller olika objekt/mål/hot. För varje objekt bildas ett plattformsspår bestående av minst ett målspår. Nedan ges ett blockschema på hur bildandet av plattformspår kan gå till.



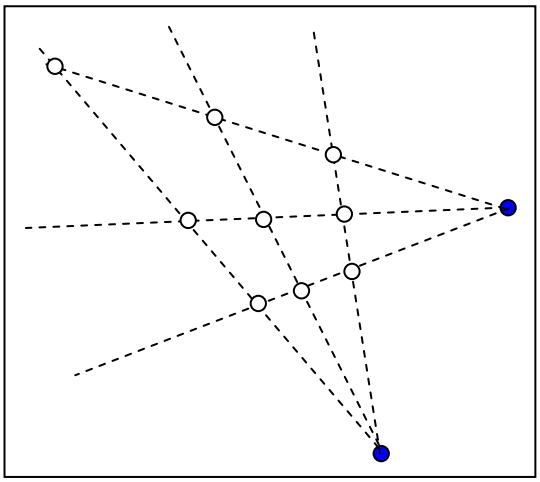
Figur 7.1 Bildandet av plattformsspår i sensordatakorreleringen.

Det är i sensordatakorreleringen som position för egen samt andra egna plattformar (BFT - ”Blue Force Tracking”) måste finnas tillgänglig.

Plattformsspår från andra egna plattformar kan betraktas på samma sätt som egna sensorers genererade plattformsspår. Vilket innebär möjlighet till att ha ett distribuerat sensorssystem.

7.1 Lägesbestämning

Ett problem i samband med samverkande plattformar är risken för att det genereras flera mål än det egentligen finns. Antag att två plattformar har ett och samma typ av passivt sensorsystem. Information rapporteras över så att bägge plattformar har tillgång till samma information. Om sensorsystemen var för sig upptäcker tre mål, så erhålls nio stycken punkter där riktningar från respektive plattform skär varandra (se figur 7.2). Detta är ett associationsproblem som ger upphov av s.k. spökbilder. Jämför med lägesbestämmande SIS. Fenomenet är på inga sätt nytt utan välkänt, men är dock värt att nämnas här.



Figur 7.2 *Lägesbestämning av tre upptäckta objekt då endast tillgång finns på riktning till objekten.*

7.2 Hotsystembibliotek

Den information som finns tillgänglig är den sammanvägda informationen om tänkbara (läs upptäckta) mål från sensordatakorreleringen. Informationen korreleras mot data i hotsystembiblioteket. Bäst överensstämmelse avgör vilket hot eller klass av hot som det kan röra sig om.

För de hotsystem som finns i hotsystembiblioteket behöver en priorteringsgrad ges. Ju högre prioritet ju farligare för egen plattform. Prioriteringsgraden kan baseras på vilken skadeverkan hotsystemet kan åstadkomma på egen plattform, tillsammans med hur lång tid som åtgår för hotsystemet för att åstadkomma verkan i egen plattform. Detta kräver i sin en grundlig genomgång av de tidsförlopp som olika typer och klasser av hotsystem har för att få en förståelse för hur lång tid som respektive hotsystem tar på sig för att få verkan. Notera att prioriteringsgraden är ett värde per hotsystem.

Innehållet i hotsystembiblioteken bör svara i möjligaste mån mot den hotbild som finns i aktuellt operationsområde. Hänsyn måste även tas till att hotsystembiblioteken bör kunna hantera hot även om dessa inte förväntas i operationsområdet.

8 Hotprioritering

Uppgiften i detta block är att prioritera mellan de upptäckta hotsystemen, i den mening att klara ut vilket hot mot vilket motverkan först ska göras. Då de upptäckta hoten via hotsystembiblioteket har blivit klassificerade och därmed tilldelade prioriteringsgrad underlättas prioriteringen.

Om det finns mer än ett hot med samma prioriteringsgrad kan prioritering ske genom att prioritera det hot som estimeras att först få verkan i egen plattform.

9 Motverkanskanaler

Med motverkanskanaler avse de åtgärder som kan göras för att antingen slå ut hotet eller undvika att bli träffad. De möjliga varianter som finns är:

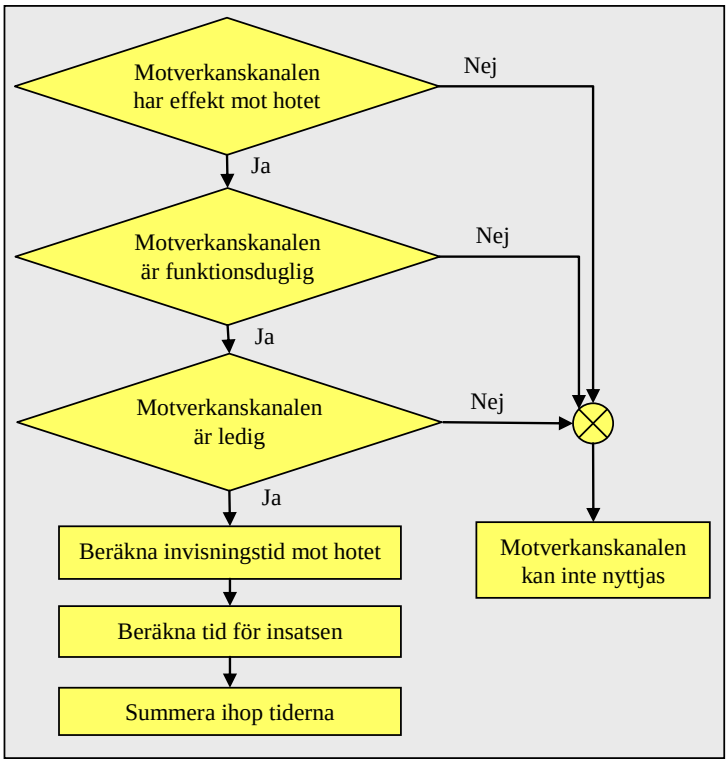
- **Hard kill** - här avses eliminera hotet genom fysisk bekämpning med projektiler eller missiler. Detta är en utvidgning för VMS som normalt inte brukar inkludera vapeninsats.
- **Aktiva skenmål** - är störare inom olika våglängdsband. Somliga av dessa kan vara kopplade direkt till ett sensorsystem via set up-logik.
- **Passiva skenmål** - utgörs av facklor (IR) eller remsor och konstrukturella skenmål (radar). Syftet är att få en målsökare att låsa på och styra mot skenmålet istället för egen eller egna plattformar.
- **Döljande motmedel** - avser främst rök (visuellt och IR). Syftet med insatsen är att dölja egen signatur. Här bör medvetenhet finnas om risken att egna sikten och sensorsystem som arbetar inom det optiska våglängdsbandet kan komma att påverkas beroende på vilken typ rök som används.
- **Manöver** - För att öka effekten av en motverkansinsats kan den kombineras med en plattformsmanöver. Det kan vara för att ändra den mot hotet uppvisade signaturen eller skapa en bättre geometri avseende vind och vinkelseparation (skenmål). Det kan också vara för att säkerställa insats med en hard kill kanal.

En kombination av ovanstående utgöra en motverkansinsats beroende på vad som krävs gentemot aktuellt hot. Motverkansinsats kan då göras med olika typer av insatser över tiden eller flera samtidiga insatser. Ett exempel på motmedelsinsatser över tiden är att blända ett upptäckt sikte med störlaser för att därefter genomföra bekämpning. Ett exempel på fler samtidiga motmedelsinsatser är då aktiv radarstörning utnyttjas samtidigt som radarremsor skjuts ut.

Om en viss motverkanskanal förväntas ha verkan mot aktuellt hot och motverkanskanalen är tillgänglig, beräknas hur lång tid det tar för motverkanskanalen att få verkan i hotet. Den tiden kan delas in två deltider, tiden för inriktning av motverkanskanalen samt tiden från inriktning till dess verkan kan erhållas i målet.

10 Insatsoptimering

Insatsoptimering ska utgående från den framtagna hotprioritetslistan, ge förslag på vilken motåtgärd som ska utföras mot vilket hot. För att insatsoptimeringen ska kunna föreslå insats med en motverkanskanal krävs att tre villkor är uppfyllda. För det första måste motverkanskanalen kunna vara effektiv mot hotet. För det andra måste motverkanskanalen var funktionsduglig och har möjlighet att verka mot hotet (kan i vissa fall innebära en viss manöver av plattformen eller del av plattform, som att vrida tornet på ett stridsfordon). För det tredje gäller att motverkanskanalen är tillgänglig och inte upptagen med någon annan insats.



Figur 10.1 *Flödesschema för att se om en motmedelskanal kan användas mot ett upptäckt hot samt vilken tid motverkansinsatsen tar innan hotet är oskadliggjort.*

Under förutsättning att dessa tre villkor ovan är uppfylld bör motverkanskanalen kunna ange utfallsannolikheten för utgången av motverkansinsats mot det aktuella hotet med geometriska och temporala förutsättningar. Bedöms olika motverkansinsatser vara lika framgångsrika kan optimeringen göras baserad på tid. En variant baseras på initial verkan i/på hotet. Den andra baseras på när hotet är utslaget/utstört. För att kunna bottna i vilken bedömningsvariant som är den optimala (beroende på plattform, motverkanskanal och hotsystem) krävs diskussion med personer med taktiskt kunnande för respektive plattform.

Det kan hända att insatsoptimeringen kommer att få avgöra hur två (eller fler) hotsystem ska motverkas parallellt. På motsvarande sätt som för ett hotsystem kan optimeringen göras efter tid, avseende initial verkan på hotsystemen alternativt när hotsystemen är åtgärdade.

För vissa motverkanskanaler (som t.ex. laserstörare) behöver frågeställningar besvaras som rör hur mycket motverkan som krävs för att motverkanskanalen ska bedömmas ha inhiberat hotsystemet.

10.1 Rules Of Engagement - ROE

Alla militära insatser styrs av ROE (Rules of Engagement) vilket även måste beaktas i ett VMS-perspektiv. Beroende av underrättelser om hotnivå, spänningar mellan inblandade kommer olika regler att gälla för olika tillfällen t.o.m. inom en och samma insats.

Det innebär att VMS behöver klara av att hantera det regelsystem som för tillfället gäller. För att klara detta behöver systemet vara flexibelt, och lätt att ändra på mellan olika typer av uppdrag. Detta ställer höga krav på att enkelt kunna ändra insatsoptimeringen.

11 Insatsbeslut och initiering av motverkan

Beslut om insats samt initiering av motverkansinsats kan ske på tre olika sätt:

- Automatiskt
- Semiautomatiskt
- Manuellt

I automatisk mod tar VMS fram den bästa lösningen och initierar denna. Fördelen med denna mod är att insatsen sker snabbt, vilket för vissa typer av scenarion kan vara den enda lösning då de andra modena blir för långsamma. Den kan å andra sidan i andra scenarion leda till att aktiviteter initierade av operatör avbryts vilket i sin tur kan få förödande konsekvenser.

I semiautomatisk mod ger systemet förslag till den bästa lösningen alternativt de bästa lösningarna varefter en operatör bekräftar insatsen och insatsen initieras.

I manuell mod är det operatören som beslutar hur insatsen ska genomföras.

Det är också möjligt att tillåta flexibilitet, så att om en typ av varnare (sensorsystem) larmar initieras motverkan automatiskt medan för andra typer av varnare (sensorsystem) så initieras motverkan semiautomatiskt. Exempel på detta är när larm från en robotskottvarnare initierar en motmedelsinsats automatiskt medan larm från övriga sensorer hanteras semiautomatiskt.

När en motverkanskanal väljs för insats mot ett hot sätts motverkanskanalen i läge upptagen till dess motverkan är genomförd. Internt i VMS behöver det aktuella hotet markeras som ”under åtgärd”, samt med vilken eller vilka motverkanskanal som är kopplade till motverkan mot hotet.

12 Insatsuppföljning

En av de viktigare funktionerna är insatsuppföljning, tragiskt nog är det också den svåraste. Beroende på vilken motverkanskanal som utnyttjas så kommer uppföljningen av motverkan att variera i svårighetsgrad.

En del av insatsuppföljningen inkluderar felfunktionalitet hos motverkanskanalerna. Exempel på detta kan vara en eller två skenmålsgranater som inte avfyras, på grund av felfunktion. Detta kan tekniskt sätt lösas så att informationen erhålls från motverkanskanalen. Om det är felfunktion på skenmålsgranaterna så att någon av dessa inte briserar kan vara betydligt svårare att få bekräftat.

Brist på ammunition för motverkan, leder till begränsad motverkan mot aktuellt hot. Exempel på detta kan vara när ett helt kastmönster inte kan skjutas med alla skenmålsgranater på grund av att omladdning sedan tidigare inte hunnits med.

Insatsuppföljningen är lättare att genomföra när en operatör med hjälp av ett eller flera sensorsystem kan konstatera om målet är utslaget eller utstört. Det måste då finnas möjlighet till inmatning med denna innebörd till VMS.

En annan möjlighet är att utnyttja den temporala aspekten, exempel på detta är att tidpunkten då hotsystemet skulle ha fått verkan i egen plattform har passerat. VMS kan då dra slutsatsen att motverkansinsatsen lyckats. En variant kan vara att en motverkansinsats exempelvis störning genomförs under en given tidsrymd och att detta är tillräckligt för att uppnå avsedd verkan. Dessa exempel är dock inte bekräftande utan snarare bedömningar som kan utnyttjas i brist på bättre insatsuppföljning.

13 VMS vid förbandsuppträdande

Hittills har egentligen endast uppbyggnaden av VMS för en enskild plattform beskrivits. I avsnitt 7 nämns dock kort om att plattformsspår från andra plattformar/enheter överförs via ledningssystemet. Vidare belyses i samma avsnitt problematiken med s.k. spökbilder samt problematiken med att bestämma vilken plattform en robot är på väg mot när plattformar uppträder i förband.

För att utnyttja enskilda plattformars VMS för att erhålla ett fungerande förbands-VMS kommer ett antal krav att behöva ställas på uppbyggandet av VMS.

Kommunikation mellan plattformarna måste finnas med tillräcklig bandbredd och tillgänglighet. Medvetenhet måste finnas om att information som överförs mellan plattformar kommer att drabbas av fördröjningar.

Det kan finnas hotsituationer som kräver motåtgärder måste vidtas av flera plattformar samtidigt. Frågan är då om det ska hanteras av de egna plattformarnas VMS eller om det ska lösas ut med utformade standardrutiner för plattformarnas besättningar. VMS ska kunna stödja operatörerna/besättningen inte ersätta dem. Självklart måste det finnas en taktik för hur agerandet ska vara för att på bästa sätt möta hotsituationen för förbandet.

Vid förbandsuppträdande kan det vara aktuellt att olika observationsområden delas ut till plattformarna i förbandet. Önskas att VMS ska känna till dessa observationsområden måste de enkelt kunna matas in till VMS.

Som framgår av texten ovan finns det fler frågeställningar än svar när det gäller VMS på förbandsnivå. För att kunna erhålla ett VMS på förbandsnivå måste regler tas fram för hur olika hot och hotsituationer ska hanteras/motverkas. Dessa regler behöver tas fram av en grupp där såväl teknisk som taktisk kompetens ingår. Den tekniska kompetensen bör omfatta hotkunskap, sensorsystem, motverkanssystem plattformsegenskaper. Den taktiska kompetensen bör omfatta plattformens stridsteknik och taktiskt uppträdande.

14 Diskussion

Arbetet med ett generiskt VMS har identifierat ett antal områden där fördjupat arbete behövs för att utveckla generiskt VMS.

Integration med ledningssystem

I detta ligger hantering av målspår och association till plattformsspår samt hantering av egna enheter s.k. ”blue force tracking”. Troligtvis finns till stora delar denna typ av information och/eller informationshantering i plattformens ledningssystem men den måste göras tillgängligt för VMS.

Vid förbandsuppträdande behöver data och information överföras mellan plattformar, en funktionalitet som förhoppningsvis redan finns integrerat med ledningssystemet. Här måste VMS kunna få plats och tid för dataöverföring.

Via ledningssystemet kan VMS ges möjlighet att samverka med ”hard kill” –funktionen, t.ex. eldledningssystem.

Operatörsstyrda sensorsystem

Sensorsystem såsom sikten som kräver att en operatör gör klassificering medför problematik avseende hur operatören ska kunna ”mata” in uppgifter om hotklass/hottyp till VMS:et utan att förlora värdefull tid för att hinna med att göra en motverkansinsats.

Biblioteksfunktioner

Har en mycket större betydelse än vad många tror. Här skulle större ansträngningar behöva göras för att få fram en metodik för generell uppbyggnad av biblioteksfunktioner.

Omhändertaget hot

En frågeställning som behöver klargöras är när ett hot ska anses vara omhändertaget. Är det när det har varit stört en viss tidsrymd eller när vapeninsats har gjorts och slagit ut hotet. Detta beror naturligtvis på vilket hotet är samt vilken eller vilka stör och övriga motverkansåtgärder som finns tillgängliga. Om ett optiskt sikte har upptäckts med en optikspanare och störts med störlaser, och inte längre kan ses med någon sensor är hotet då borta eller bara riktat temporärt åt ett annat håll?

Insatsuppföljning

Insatsuppföljning är en av de svårare uppgifterna att lösa ut. I vissa fall kan tappat målspår (från en sensor) indikera att hotet är borta. Problemet är i många fall att det inte går att avgöra om hotet har blivit tillräckligt stört för att missa sitt tilltänkta mål. Vilket kan göra att resurser slösas på ett hot som i praktiken redan är avvägt.

Arbetet med generiska VMS har gett insikt i hur VMS ska kunna vara uppbyggt. Vissa VMS verkar vara uppbyggda enligt delar av de tankar som beskrivits i denna rapport. En förhoppning är att den framkomna beskrivningen ska kunna tjäna som en roadmap för kommande VMS.

15 Referenser

[1] Lars Berglund, Calle Rosenquist, Linus Hilding, Generiskt VMS – Lägesrapport, FOI MEMO 3378, 2010

[2] Gustaf Olsson, Genomförd demo Generiskt VMS, FOI MEMO 3215, 2010

[3] Gustaf Olsson, VMS, långsiktig teknikutveckling och forskning - Några tankar och idéer, FOI-R--3073--SE, Dec 2010

[4] Gustaf Olsson, Demo Generiskt VMS, FOI MEMO 3760, 2011-12-12

[5] Carl-Lennart Westerlund, Mikael Tulldahl, Peter Johansson, Lägesrapport - Utformning av dynamiska VMS-bibliotek, FOI MEMO 2163, 2007