Mission Driven Sensor Management

Fok Bolderheij
Royal Netherlands Naval College
Nieuwe Diep 8
1780 CA Den Helder
The Netherlands
F.Bolderheij@KIM.NL

Piet van Genderen
Delft University of Technology
Mekelweg 4
2600 GA Delft
The Netherlands
P.VanGenderen@ITS.TUDelft.nl

Abstract – *Sensor Management is becoming increasingly complex due to the shift in naval missions, the introduction of new sensor systems like the Multifunction Radar and sensor data fusion objectives. This paper identifies the relevant, mission related information necessary for Sensor Management, by analyzing the Command and Control (C2) processes. A model is used that distinguishes four main processes that handle information within C2: provide Situational Awareness, perform Threat Assessment, perform Decision Making and execute Direction and Control. The Sensor Management process can be described in terms of those four processes. Analysis shows that the Threat Assessment process is very much operator knowledge intensive. Evidence is brought forward that the knowledge intensive components of the Threat Assessment process are risk estimation processes. A novel method is introduced that enables the automation of these Risk Estimation processes and thus a further automation of the Sensor Management process. This risk estimation is based on vulnerability and survivability, two concepts that are key in military tactics. This novel approach provides a wide comprehension for including other mission related concepts, like the Rules of Engagement and Emission Control Plans in the mission driven management of sensors.*

Keywords: Sensor Management, Maritime Operations, Situational Awareness, Risk Estimation, Threat Assessment

1 Introduction

Since the last decade, armed forces are no longer solely used as an instrument of deterrence in order to prevent a global conflict, but are actively deployed in peacekeeping, peace enforcing and maritime patrol operations. The missions of Royal Netherlands Navy frigates evolved from protection of the Sea Lines of Communication (SLOCs) on the Atlantic Ocean, to Maritime Interdiction Operations (MIOPS) in a littoral environment. Complete and correct assessment of the situation in this type of environment is often very complicated because of the detection limitations imposed by the geographical situation and the presence of other (civilian) traffic. Because of the often short distance to the shore, the threat ranges from small (fast) boats, manned by terrorists to land-based missile sites and long-range fighter or bomber attacks. The threat in this type of environment is more diverse than the threat in the middle of the ocean and reaction times are shorter. In order to provide timely detection, classification and weapon assignment against objects that pose a threat, *more* information needs to be gathered, processed and compiled in *shorter* times.

This need was met by the development of new, high performance sensor systems. An example of a new type of sensor is the Multifunction Radar (MFR). In this type of radar system, search, track and weapon guidance functions are combined. More functionality and high performance comes however at a cost: managing these sensors has become more complex in comparison with the control of conventional sensors.

In addition there is a tendency to fuse the information derived from the separate sensor systems, driven by the need for more accurate and detailed information, therefore the sensor suite must be configured as a whole, instead of setting each sensor separately. A new trend is the use of the available resources spread out over a range of platforms (Network Centric Warfare) for strategic picture compilation and more effective weapon assignment.

Apart from a need for more sensor functionality and performance, mission objectives can impose restrictions on the use of sensors for political or tactical reasons. These restrictions have to be imposed on the sensor settings, thus complicating the sensor management task even further.

Traditionally, sensor management is based on the evaluation of technical parameters. Depending on the type of sensor, parameters like transmitting frequency, transmitting power, polarisation type, pulse length, receiver characteristics etc. can be controlled in order to improve the sensor performance.

The sensor management task is usually assigned to one or more sensor operators, who translate the mission objectives and restrictions into sensor settings. Due to the availability of more sensors and/or more functionality in each sensor, this task is becoming increasingly complex and time-consuming, thus allowing for an easy introduction of errors, probably to result in sub-optimal sensor settings. The extension of sensor functionality and performance without either proving support to the sensor operator or automating the operator task to some extent , will therefore most likely be counterproductive.

A novel approach is proposed in this paper to assess the risk associated with the occurrence of threatening objects. This risk assessment is based on *vulnerability* and

survivability, two concepts that are key elements in military tactics. This novel approach provides a wide comprehension for including other mission related concepts, like the *Rules of Engagement* and *Emission Control Plans* in the mission driven management of sensors.

Section 2 of this paper presents the current architecture of Command and Control Processes. The Observe-Orient-Decide-Act (OODA) loop model is used to identify the operator dependencies in these processes. Section 3 discusses various modes of use of Multifunction Radar in the OODA loop. Section 4 proposes a tractable expression for the estimation of the level of risk posed by threat objects and discusses other use of the same concept.

2 Structure of Command and Control Processes

The operational processes responsible for mission control are often referred to as the Command and Control (C2) processes. Because in these processes all the relevant mission information is embedded, the required sensor management information has to be derived from them. Delft and Passenier [1] developed a C2 process model in which four main information handling processes are distinguished. These processes can be mapped on the classical, high-level processes in the Observe – Orient – Decide – Act loop (OODA loop) as described by Boyd [2]. This mapping is given in Table 1.

Table 1 : OODA and C2 processes.

OODA Process	**C2 Process**
Observe	Provide Situational Awareness
Orient	Perform Threat Evaluation
Decide	Perform Decision Making
Act	Execute Direction and Control

The relations between the C2 processes are given in Figure 1.

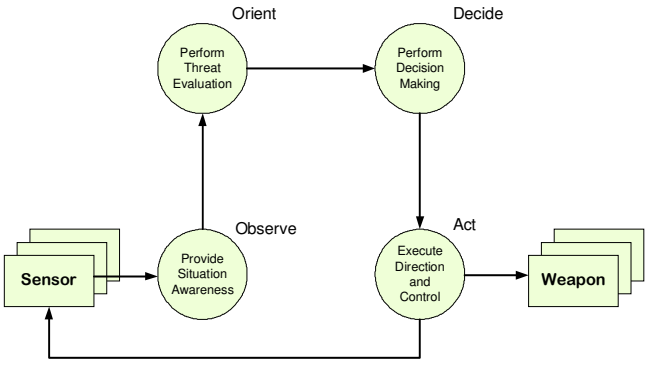

Fig. 1. The C2 processes.

The information necessary to execute these processes is either available in these parts of the C2 processes, as implemented in the Combat Management System (CMS), or present as implicit operator knowledge. These processes are analysed in order to determine their current level of automation in combination with the missing information.

The *Situational Awareness* process uses the sensor systems to detect, track and recognise objects in the operational environment. The delivered type of information is sensor dependent: radar systems provide range, bearing, elevation and velocity information; state of the art radars automatically generate plot and track information; optical sensors can be used for detection and recognition purposes and radar receiver data (Electronic Support Measures (ESM) equipment) can be used to detect the presence of objects by their electromagnetic emissions. Often some kind of Sensor Data Fusion functionality is implemented in the CMS. In modern Combat Systems, the process of obtaining Situational Awareness is largely automated and is sometimes augmented by operator input.

In the *Treat Evaluation* process the sensor data is analysed, interpreted and compiled into the so-called Recognised Picture. Objects are labelled (identified) as Friendly, Neutral or Hostile if the object is classified with enough certainty; it is identified as Assumed Friendly or Suspect if there is some doubt about the classification and as unknown if there is no certainty about the classification of the object. The identity assigned to an object depends on the threat the object poses to the mission objectives and the amount of certainty about the type of object (Classification Process). This of the latter depends on the available sensor information: kinematical data, recognition data or ESM data. Although supported by the Combat Management system, these processes still rely mainly on operator knowledge.

The *Decision Making* process uses the Recognised Picture to plan the deployment of the available resources or the execution of other actions necessary for mission success. Once an object's class has been established with some degree of certainty and the threat it poses to the mission has been determined, actions have to be considered if the threat is evaluated too high. Weapon systems (actuators) are directed to those objects that potentially can harm own assets thus reducing their (operational) value and hence endanger the mission objectives. The type of weapon system, if necessary in combination with a directing sensor is selected by a scheduler. Automation is often based on heuristics and kinematic properties of the threat object usually on a 'first come, first serve' basis. Because of the often short reaction times, the deployment of these systems is safeguarded by 'fire inhibit' switches: once the decision has been made to use force, firing is enabled and the Decision Making process decides about the choice of weapon and the best moment for deployment. The process itself is highly automated, decisions about the actions that are to be taken however are made by an operator.

Once a decision has been made, the *Direction and Control* process executes the plans. Because modern

weapon systems are self-guiding or use the guidance provided by tracking systems this process is usually fully automated only to be supervised by an operator.

3 Sensor Management

Next, the role of sensor management within the C2 processes and the necessary information to run this process have to be determined. Because sensor systems deliver the necessary data for picture compilation in the Situational Awareness process, planning the way in which these resources are deployed can be described as a Decision Making process and controlling them as a Direction and Control process. The OODA loop can now be closed, using the Threat Evaluation processes to deliver the necessary input. An OODA loop based sensor manager can be constructed that uses sensor data as input, evaluates it, plans the deployment of the sensor resources and adjusts the sensors based upon this evaluation.

Blackman and Popoli [3] describe a template for Sensor Management design consisting of two loops:

1. A loop controlled by a 'Macro Sensor Manager' assigning the tasks that need to be accomplished to generate the Recognised Picture;
2. A loop controlled by a 'Micro Sensor Manager' optimising the assigned tasks.

Once the Macro Sensor Manager has allocated a task to the Micro Sensor Manager, the task can be controlled by technical parameters and no operator input is necessary as long as the operational conditions do not change. The described Macro Sensor Manager however needs operator information for Threat Evaluation and Decision Making purposes in order to schedule the individual tasks and allocate the available budget.

In traditional sensor systems different tasks are assigned to different sensors: search tasks are assigned to search radars; target acquisition is accomplished by target acquisition radars and tracking and illumination is done by track radars. Because dedicated radars are available to perform different tasks, there is not much need for budget allocation. The only experience available in task scheduling and budget allocation is related to the deployment of mechanical Single Target Trackers for Weapon Assignment purposes: once the decision has been made to deploy a guided Weapon System, a scheduler selects the missile in combination with a directing sensor. The characteristics of this type of scheduling mechanism fit the needs of a sensor manager for weapon direction; it does however not reserve sensor capacity for not yet detected, potentially more dangerous objects and is therefore not suited for scheduling MFRs or complete sensor suites. In modern MFRs, allocated search budget is not available for tracking purposes, and the illumination of an object will seriously drain the available budget. Priorities have to be assigned to these different tasks.

Various scheduling mechanisms dealing with this problem are proposed in literature. For instance Huizing and Bloemen [4] propose a scheduling algorithm for an MFR, based upon operator assigned task priorities. The question that remains to be answered in this algorithm is on what basis these priorities have to be assigned. Komorniczak et al. [5], describe a prioritising mechanism based upon the kinematical properties of a threat object once this object is detected; this mechanism could be used to assign the priorities required for the tracking functions in [4] but it needs to be expanded for assigning priorities to search functions.

Earlier in this Section, the conclusion was drawn that the Threat Evaluation process generated the input of the Sensor Management process; the priorities connected to the different tasks should be based on the output of this process. With this conclusion we return to the original objective, the (partial) automation of the Sensor Management process, now specifically oriented at the Threat Evaluation process, because this process is operator knowledge intensive.

4 Risk Estimation

As stated before, the threat posed by an object is directly related to the amount of damage the object is able to inflict on our assets, thus reducing their (operational) value and the chances of mission success. Two important aspects come forward here: firstly the aspect of probability of mission success which is related to the failure of the threat objects and secondly the aspect of (operational) costs. These two factors are the most mentioned parameters in the concept of risk. Currently the estimation of the risk posed by threat objects is performed by mental processes executed by an operator. These processes will now be analysed in order to automate them. If it is possible to *estimate* the risk related to a threat object, those objects could be ranked in accordance to the risk, thus providing input for sensor function assignment and budget allocation. Because there are no restrictions with respect to the location of those sensors, a sensor manager that is based on risk estimation could also be used in a Network Centric Warfare role.

In literature a number of definitions of Risk are given: Bedford and Cooke [6] describe Risk Analysis as an attempt to answer the following three questions:

1. What can happen?
2. How likely is it to happen?
3. Given it occurs, what are the consequences?

Yellman [7] states that there are three facets of risk:

1. Expected Loss;
2. Variability of the losses;
3. Uncertainty of the mental model.

All those definitions and descriptions have in common the combination of the consequences of an unwanted phenomenon (costs or losses) and the probability of occurrence of this phenomenon (uncertainty).

Romberg [8] describes how search can be used during a mission to reduce the risk posed by threat objects. Risk is calculated according to:

$$r(n) = \sum_{i=1}^{I} v(i,n)\left(1 - \prod_{k=1}^{K} (1 - L(k) P_f(i,k,n))\right) \quad (1)$$

$$RISK = \sum_{n=0}^{N} r(n) \qquad (2)$$

where:

- N = total mission time;
- I = number of own assets;
- K = number of threat objects
- V = value of asset i at time n;
- L = lethality of threat object k (probability);
- P_f = probability of threat object k reaching asset i undetected;
- $RISK$ = the total risk during the mission.

Here the assumption is made, that the detection of a threat object automatically results in its neutralisation. Eq. (1) contains all the necessary elements to estimate the risk posed by each object in the recognised picture, but also supports the estimation of the risk posed by not yet detected objects (intelligence). The recognised picture consisting of K_1 detected objects therefore has to be supplemented with K_2 imaginary threat objects, where the total number of threat objects K is the sum of K_1 and K_2. For each of the threat objects (both real and imaginary) a risk estimation is executed. The estimated risk now directly translates into a sensor priority: a high risk yields a high priority. The type of the threat object relates to the necessary sensor function: a real (detected) threat object has to be tracked by the sensor; an imaginary object relates to a search function. If absolute certainty about the number of threat objects belonging to a certain class is available, the imaginary object can be removed from the Recognised Picture once all the threat objects from this class are detected and the search activities for this type of object can be ceased.

In our approach eq. (1) is adapted to fit the needs of the sensor scheduler:

$$r(i,k) = \sum_{i=1}^{I} v(i)(1 - \prod_{k=1}^{K}(1 - L(i,k)P_{occ}(i,k))) \qquad (3)$$

Because the mission duration is not known and it is the instantaneous risk we are interested in, the time aspect is eliminated. Furthermore $L(k)$ is expanded into $L(i,k)$ because the lethality of a threat object depends on the interaction of a specific threat object and a specific asset: a certain type of missile will have a different impact on a non armoured frigate than on a heavily armoured cruiser. The final adaptation of the algorithm lies in the change of P_f into P_{occ}. This is more than only nomenclature: P_{occ} is defined as the probability of the occurrence of an unwanted event inflicted by a threat object. The contribution of all the underlying events leading to this final, lethal event, like the failure to destroy the missile using hard kill systems or distract it by means of soft kill systems will be taken into account.

Other important information can be derived from (3): $L(i,k)P_{occ}(i,k)$ gives the *vulnerability* of asset i in relation with threat object k and (1- $L(i,k)P_{occ}(i,k)$) yields the related *survivability*.

To estimate the probability of occurrence, the *Failure Mode Effects Analysis* (FMEA) as described by Bedford and Cooke [5] was used. This method has proven its merits in risk analyses in the aircraft industry and the construction of nuclear power plants. To demonstrate the suitability of this method, the probability of occurrence of a hit by an active homing missile (threat object) will be estimated, based on the probabilities of underlying events. At first, a *state diagram* is constructed (Fig. 2.), showing the different missile states and the state transitions.

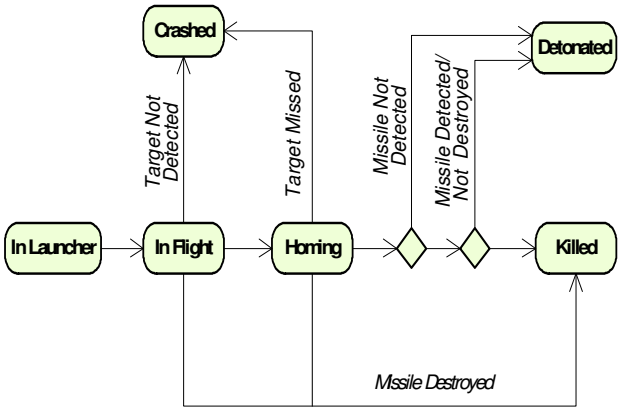

Fig. 2. Missile State Diagram.

The missile states that were distinguished are:

- In Launcher;
- In Flight (midcourse);
- Crashed (own assets not detected) ;
- Homing (terminal illumination);
- Detonated (own asset hit);
- Killed (destroyed by own assets).

Analogous to the construction of a fault tree in the FME Analysis, an event tree was built (Fig. 3.) based on the events that cause a *state transition*.

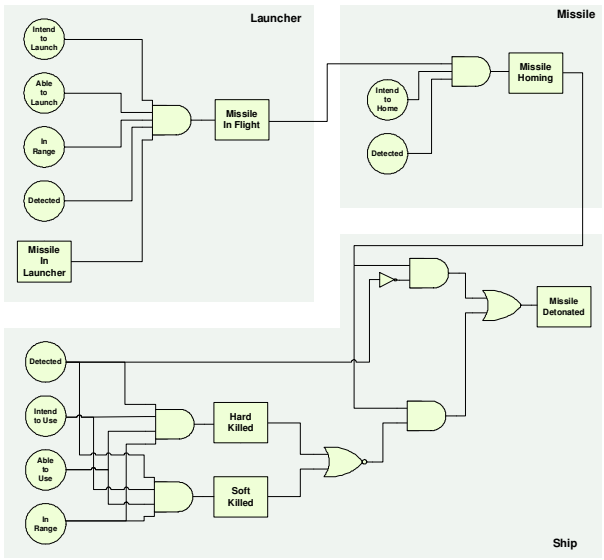

Fig. 3. Event Tree resulting in Missile Detonation

These events can be divided into three main categories:

1. Events related to the launcher;
2. Events related to the missile;
3. Events related to the own assets;

The underlying events should be broken down to a level where the probabilities of occurrence of those events can either be estimated by experts or derived from historical, statistical or technical data. For instance, the conditions that lead to the launch of the missile are:

- The opponent intends to launch (intention to launch);
- Both the launcher and the missile are in a sufficient technical condition (able to launch);
- Our asset is in range;
- Our asset is detected by the opponent.

If these conditions are met, the missile will be launched. The probabilities of occurrence of underlying events now have to be determined. The opponent's intentions depend on the current conflict level; the estimation of this probability has to be based on expert knowledge. The probability of a successful launch by the opponent can be derived from observations of trials and the estimation of the technical condition of the launcher and the missile. The missile's performance determines whether our asset is in range. An estimation of environmental factors, the opponent's sensor capacity and observed reconnaissance yields the probability of detection.

The combination these probabilities as the input of a logical *And Gate* construction, using *Bayesian Calculus* results in the probability of the event Missile Launch. This event in its turn is an necessary precondition for the Missile Homing event. In a similar way the other underlying events are combined into the Missile Detonated event and its related probability of occurrence.

After the construction of the event tree was finished, it became apparent that the tree could be used as a *knowledge base*; the detection of a missile leads to the conclusion that the underlying events have taken place; the opponent apparently had the intention to launch, the launcher and the missile were in good condition, our asset was in range and was detected. This provides some knowledge about to the future deployment of other threat objects, thus offering assistance in the Decision Making process.

It is also possible to use the event tree to visualise the implications of mission imposed restrictions (e.g. Rules Of Engagement, Emission Control plans) or malfunctioning equipment: these restrictions or malfunctions will have an impact on the deployment of own sensors and actuators; thus increasing the chances of success of the threat objects i.e. the probability of occurrence of the unwanted phenomenon.

Once the probability of occurrence of the unwanted phenomenon caused by an asset /threat object interaction is estimated, the resulting risk can be determined using equation (3); assuming that an asset's operational value and a threat object's lethality are already determined.

Analysis of the event tree provides a set of countermeasures: to prevent the launch of a missile, one of the following conditions has to be satisfied :

- the conflict level is reduced by holding peace negotiations;
- the launcher is taken out by a pre-emptive strike;
- assets are kept out of weapon range;
- detection is avoided.

The effect of each of these countermeasures could be calculated by estimating the related risks. With respect to the Sensor Management, risk could be reduced by enhancing the Probability of Detection and Track Accuracy for hard and soft kill countermeasures. It is clear that failure of detection directly results in a missile hit if the missile system is not malfunctioning. Once the missile is detected it has to be neutralised by the either the hard kill or soft kill systems.

5 Conclusion

The description of Sensor Management process in terms of the OODA loop processes provides a way to construct a Sensor Management System that is controlled by operational information. This information is to a great extent available within the C2 processes except for the risk estimation information.

The implementation of the described risk estimation process in the Threat Evaluation processes provides a tool to accomplish automatic Threat Ranking and offers support for the Decision Making processes. The combination of information provided by the Classification, Identification and the Risk Estimation processes enable the automation of sensor function assignment and budget allocation to a large degree, thus supporting the effective use of complex sensors like the Multi Function Radar and also enables the management of sensors located at different platforms.

Acknowledgements

This work is part of the STATOR research program on sensor management supported by Thales Naval Nederland, the Royal Netherlands Naval College, and the International Research Center for Telecommunications-transmission and Radar of the Delft University of Technology.

In order to support this research many interviews were made with staff of the Royal Netherlands Navy. Their willingness to share their views on the Command and Control process functions and operator roles is greatly appreciated.

References

[1] J.H. van Delft and P.O. Passenier. Functions and tasks in current CIC, In J.H. van Delft and H. Schuffel, editors, *Human Factors research for future RNLN Combat Information Centers*. TNO-TM 1995

A-19, TNO-TM, Soesterberg, The Netherlands, 1995 (in Dutch).

[2] Boyd, John R. A Discourse on Winning and Losing. Unpublished briefing notes. Various editions, 1987-1992.

[3] Samuel Blackman and Robert Popoli. *Design and Analyis of Modern Tracking Systems,* pages 1004-1018, Artech House, Norwood , MA, 1999.

[4] Albert G. Huizing and Axel A.F. Bloemen. An Efficient Scheduling Algorithm for a Multi Function Radar*, IEEE int. symp. on Phased Array Systems and Technology*. 0-7803-3232-6/96, IEEE, 1996.

[5] Wojciech Komorniczak, Tomasz Kuezerski and Jerzy F. Pietrasinski. The priority assignment for detected targets in Multi-Function Radar, *Proc. 13th Int. Conf. On Microwaves, Radar and Wireless Communications*, pages 244-247, Mikon, 2000

[6] Tim Bedford and Roger Cooke, *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press, pages 10, 99-120, Cambridge, UK, 2001.

[7] Ted W. Yellman. The Three Facets of Risk *Proc. 2000 World Aviation Conference*. October 10-12, 2000, San Diego, CA, American Institute of Aeronautics and Astronautics, Washington, DC, 2000.

[8] Harland Romberg. A game theoretic approach to search *AIAA Guidance, Navigation, and Control Conference and Exhibit*, Denver, CO, 14-17 August 2000. AIAA-2000-4052, 2000