# DOCUMENT CONTROL SHEET

| | ORIGINATOR'S REF.<br>NLR-TP-2000-437 | | SECURITY CLASS.<br>Unclassified |
|---|---|---|---|

ORGINATOR
National Aerospace Laboratory NLR, Amsterdam, The Netherlands

TITLE
Real-time self-protection electronic warfare management in fighter aircraft

PRESENTED AT:
the RTO Symposium "Advanced Mission Management and System Integration Technologies for Improved Tactical Operations", Florence, Italy, 27-29 September 1999

| AUTHORS | DATE | pp | ref |
|---|---|---|---|
| F. Tempelman | September 2000 | 14 | 6 |

ABSTRACT
The Self-Protection Electronic Warfare (SPEW) Manager is an automated system that provides a link between the electronic warfare sensors and actors, available in an aircraft. It determines the most effective actions and, if possible, executes those actions. We developed a SPEW Manager, in which the feasibility of the concept has to be proven in a demonstration environment. The SPEW Manager demonstrator consists of a simulated sensor data fusion module, a resource manager and a human-machine interface. It is highly flexible with respect to aircraft type and available actors. Facilities to take both hardware-initiated and crew-initiated actor activation into account are added. Various operational and system modes are supported. The SPEW Manager demonstration will improve the effectiveness and efficiency of using countermeasures against threats.

**Nationaal Lucht- en Ruimtevaartlaboratorium**
National Aerospace Laboratory NLR

NLR-TP-2000-437

# Real-time self-protection electronic warfare management in fighter aircraft

F. Tempelman

This report is based on a presentation held at the RTO Symposium "Advanced Mission Management and System Integration Technologies for Improved Tactical Operations", Florence, Italy, 27-29 September 1999.





| | |
|---|---|
| Division: | Information and Communication Technology |
| Issued: | September 2000 |
| Classification of title: | Unclassified |

## Summary

The Self-Protection Electronic Warfare (SPEW) Manager is an automated system that provides a link between the electronic warfare sensors and actors, available in an aircraft. It determines the most effective actions and, if possible, executes those actions. We developed a SPEW Manager, in which the feasibility of the concept has to be proven in a demonstration environment. The SPEW Manager demonstrator consists of a simulated sensor data fusion module, a resource manager and a human-machine interface. It is highly flexible with respect to aircraft type and available actors. Facilities to take both hardware-initiated and crew-initiated actor activation into account are added. Various operational and system modes are supported. The SPEW Manager demonstration will improve the effectiveness and efficiency of using countermeasures against threats.

## Contents



(14 pages in total)

# Real-Time Self-Protection Electronic Warfare Management in Fighter Aircraft

**Frank Tempelman**
National Aerospace Laboratory NLR
Anthony Fokkerweg 2, P.O. Box 90502,
1006 BM Amsterdam
The Netherlands

**Abstract**
The Self-Protection Electronic Warfare (SPEW) Manager is an automated system that provides a link between the electronic warfare sensors and actors, available in an aircraft. It determines the most effective actions and, if possible, executes those actions. We developed a SPEW Manager, in which the feasibility of the concept has to be proven in a demonstration environment. The SPEW Manager demonstrator consists of a simulated sensor data fusion module, a resource manager and a human-machine interface. It is highly flexible with respect to aircraft type and available actors. Facilities to take both hardware-initiated and crew-initiated actor activation into account are added. Various operational and system modes are supported. The SPEW Manager demonstration will improve the effectiveness and efficiency of using countermeasures against threats.

## 1 Introduction

A Self-Protection Electronic Warfare (SPEW) Manager determines the most effective use of actors to counter detected threats. Such a manager enables co-ordinated countermeasures that can not be performed manually using the separate systems [1]. Most notably, this involves countermeasures combining jamming and chaff. Furthermore, the manager can apply countermeasures to counter more than one threat simultaneously.

Under a contract awarded by the Royal Netherlands Air Force, the National Aerospace Laboratory NLR and its sub-contractor TNO are carrying out applied research and development into a SPEW Manager. This shall result in a demonstration in a realistic simulation environment, proving the feasibility of the manager.

In this paper, we will describe the architecture, components and techniques of the SPEW Manager.

## 2 The SPEW Manager

### 2.1 Architecture

The SPEW Manager is developed using the Shlaer/Mellor (S/M) Object-Oriented Analysis and Design method [2][3]. The S/M Object Communications Model for the SPEW Manager is depicted in figure 1, and is used here to describe the manager.

The SPEW Manager consists of three distinctive parts. These are the white boxes in the figure. The first part contains the multi-sensor data fusion (MSDF) functionality. Here, based on data obtained from various sensors on-board the aircraft, combined with intelligence information, a list of threats is constructed. The second part of the SPEW manager is called the Resource Manager (RM). Here, a combination of countermeasures is determined, optimally countering the threats in the threat list. The third part is the Human Machine Interface (HMI), which informs the crew on the situation and which visualises suggestions to counter the threats.

For the demonstration, the SPEW Manager is embedded in a simulation environment. This is the dark box in figure 1: the Interactive Tactical Environment Management System (ITEMS) from CAE Electronics [4].

Dithered boxes outside the Resource Manager box in figure 1 denote interface objects, used to transfer and convert the necessary data between parts.

We will discuss the three parts of the SPEW Manager in more detail in the following sections.

## 2.2 Multi-sensor data fusion

The MSDF part of the SPEW Manager acquires the information about the threats. Furthermore, for each threat, it determines lethality to enable prioritisation of the threats. The constructed list of threats may include inaccurate information (for instance in the aspect angle with regard to the ownship). It may involve incomplete information (for instance the range to the threat can not be determined) and uncertain information (like: we do not know for certain whether a threat is of type *A* or of type *B*). The actual conversion of raw sensor data into a threat list is not the goal of the project, and is therefore simulated. For each detected threat, the following information is provided:

| *Attribute* | *Explanation* |
|---|---|
| Id | Unique name of the threat |
| Threat level | Lethality, ranging from 1 to 10 |
| Position | Position, relative to ownship (range, azimuth, elevation) |
| Velocity | Speed vector |
| Identification | Threat type, which can vary between very detailed (*SAM8*) and a rough classification (*IR missile*) |
| Certainty | Probability of identification being correct |
| TTI | Time Till Intercept (for missiles) |
| Threat mode | If applicable, the mode in which the threat's radar is in: Search, track, ... |

The threat level is determined based on acquired expert knowledge, and can depend on e.g., position of the threat. These values are easily adaptable, to allow fine-tuning of the SPEW Manager.

Note, that when identification of a threat is ambiguous, e.g., when we assume there is 70% probability of the threat being of type *A*, and 30% probability of the threat being of type *B*, the MSDF process results in *two* threats: one of type *A* and one of type *B*. This way of solving the ambiguity problem is necessary for reasons of safety: one cannot neglect perhaps fatal possibilities.

## 2.3 Resource manager

In the Resource Manager box (see figure 1) countering the threats is handled. Various parts can be distinguished. We will discuss them here.

### 2.3.1 System and crew

The System-and-crew box in figure 1 refers to the ownship systems, including the crew. Next to RCMs and CMs from a CMT, countermeasures can be initiated directly by the crew. The SPEW manager takes these into account, and will *never* abort or prohibit the execution of such a countermeasure. When prioritising the various types of countermeasures, we see that crew-initiated countermeasures have the highest priority, followed by RCMs and CMs from a CMT.

The SPEW Manager supports operational modes. Based on characteristics of the environment, the crew is able to select various preferences, with regard to the use of expendables, jamming and manoeuvres. Built-in preferences include *Constrained manoeuvring*, in which manoeuvres are applied as little as possible, *Minimum expendable use*, when for tactical or political reasons the use of expendables should be constrained, and *Run silent*, when jamming is unwanted. Furthermore, the SPEW Manager supports various system modes, controlling the level of automation. These are *Off*, *Stand-By*, *Manual*, *Semi-automatic* and *Fully Automatic*. The HMI supports the selection of these modes during flight.

### 2.3.2 CMT Knowledge Base

To counter a threat, obtained from the MSDF process, a sequence of countermeasures (CMs) can be executed. These sequences are called *countermeasure techniques* (CMTs), and consist of tactics (manoeuvres), techniques (chaff, flare, jamming) or combinations of these. All of these CMTs are aimed at minimising threat lethality, i.e., deny or delay lock-on during search, break lock during track, or cause a launched missile to miss. A threat that, thanks to executed CMTs, goes from *track* mode back to *search* mode is considered to disappear, and another, new threat appears instead: the same physical threat but in *search* mode, probably with a lower threat level.

Extensive knowledge acquisition using expert interviews and trial results has resulted in a representative and large set of *rules*, connecting generic descriptions of CMTs to generic threat descriptions under specified conditions. Furthermore, estimations of the effectiveness of the CMT against the threat are supplied. Again, these estimations are easily adaptable for fine-tuning.

The following table shows a generic example of some of the knowledge, from which the rules are distilled.

| ID | Thrt | Mde | TL | Sens | E | GCMT |
|---|---|---|---|---|---|---|
| 1 | SAM1 | S | 3 | R | 5 | OT |
| CONDITION: None | | | | | | |
| # Simple example: SAM1 search radar (low TL) detected by RWR only; Turn to evade the site. | | | | | | |
| 2 | SAM1 | S | 3 | R+J | 8 | N1S |
| CONDITION: None | | | | | | |
| # As above, only now the site is also detected by the ALQ, so jamming can be used (Noise). | | | | | | |
| 12 | SAM1 | T | 4 | R+J | 8 | RGPO1C+ 4C |
| CONDITION: Threat at $(20^\circ<F<60^\circ)\vee(300^\circ<F<340^\circ)$ | | | | | | |
| # Sam is tracking the aircraft. Combination of RGPO and chaff is effective, but only at certain azimuth angles | | | | | | |
| 32 | SAM1 | L | 9 | R+J+ MA | 8 | VGPO1 |
| CONDITION: Time Till Intercept≥5s | | | | | | |
| 34 | SAM1 | L | 10 | R+J+ MA | 5 | 6GturnInto |
| CONDITION: Time Till Intercept<5s | | | | | | |
| # Missile is launched, detected by MAWS. Assuming semi-active missile, VGPO can be attempted. If this fails (TTI<5s), perform last ditch manoeuvre | | | | | | |

From left to right, we see the unique ID of the rule, the type of the threat, the threat level, the sensors that detected it, the expected effectiveness of the proposed countermeasure technique, the type of technique itself, and on the next line the condition under which the technique is effective.

A condition in a rule can have the following form:

- aspect angle between lower bound and upper bound;
- altitude between lower bound and upper bound;
- speed between lower bound and upper bound;
- G-level between lower bound and upper bound;
- time till intercept between lower bound and upper bound.

Each countermeasure in a technique is accompanied by a starting time and a finishing time, allowing exact timing of CMs. These time stamps are determined based on the relative position of the threat.

In figure 2, the S/M object model of the SPEW Manager is supplied. This is an object-oriented model, showing the relations between concepts within the Manager. The representation of the rules can be found in the bottom left corner. There, we can see that a CMTRule object connects a Threat object to a Generic Counter Measure Technique object (GCMT), which of its turn consists of Generic Planned Counter Measure objects (GPCM).

The set of rules forms the core of the SPEW Manager. It is an easy-to-modify text-based file. This enables the application of the SPEW Manager in different aircraft, based on the available actors. Furthermore, new CMTs can be added.

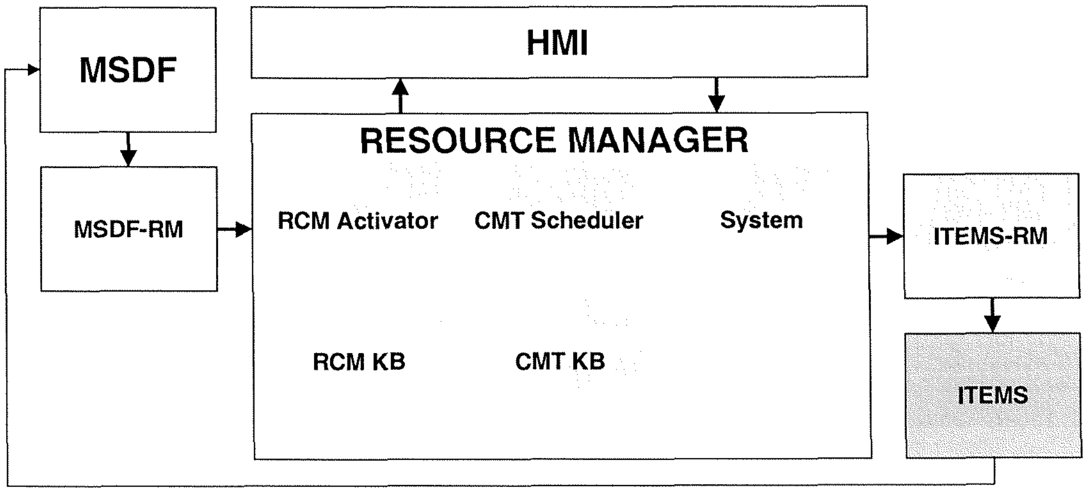



*Figure 1. Object Communication Model of the SPEW manager*

### 2.3.3 RCM Knowledge Base

In various current aircraft configurations, certain sensors are directly wired to actors like chaff and flare. This enables the actor to react immediately on sensor input by executing a so-called *reflex countermeasure* (RCM). These are activated only in case of imminent danger, e.g., the detection of an incoming missile, for which crew actions would come too late, and a flare is ejected automatically. The SPEW manager is able to (a) take these reflex countermeasures into account by simulating them in software, and (b) extend the set of reflex countermeasures in software by the addition of *reflex rules*. These connect certain sensor data characteristics directly to actions to be executed, under certain conditions. These reflex rules are activated based on sensor tracks, and not on threats. The RCMs require that the Resource Manager is not only provided with the fused threat data, but also all *newly discovered* tracks, to be able to see whether an RCM should be activated. Hence, in the simulation of the data fusion process, next to threat information, new tracks have to be supplied.

In the development of the SPEW manager, knowledge acquisition has resulted in an extensive list of reflex rules. Figure 2 shows the representation in the dashed objects in the down right corner. As with the rules discussed in paragraph 2.3.1, this set is easily modifiable. The activation of reflex countermeasures can disturb the execution of "normal" countermeasures. This is taken into account in the Manager.

### 2.3.4 CMT Scheduler

The CMT scheduler determines what actions to schedule to counter the detected threats. In section 3, we will get into this process in more detail.

### 2.3.5 RCM Activator

The RCM scheduler examines the new sensor tracks as supplied by the MSDF process, and determines whether or not an RCM has to be activated. This is done by checking the conditions as supplied in the set of reflex rules. If one of the conditions is fulfilled, the accompanying RCM is activated, but only if crew actions do not prevent this.

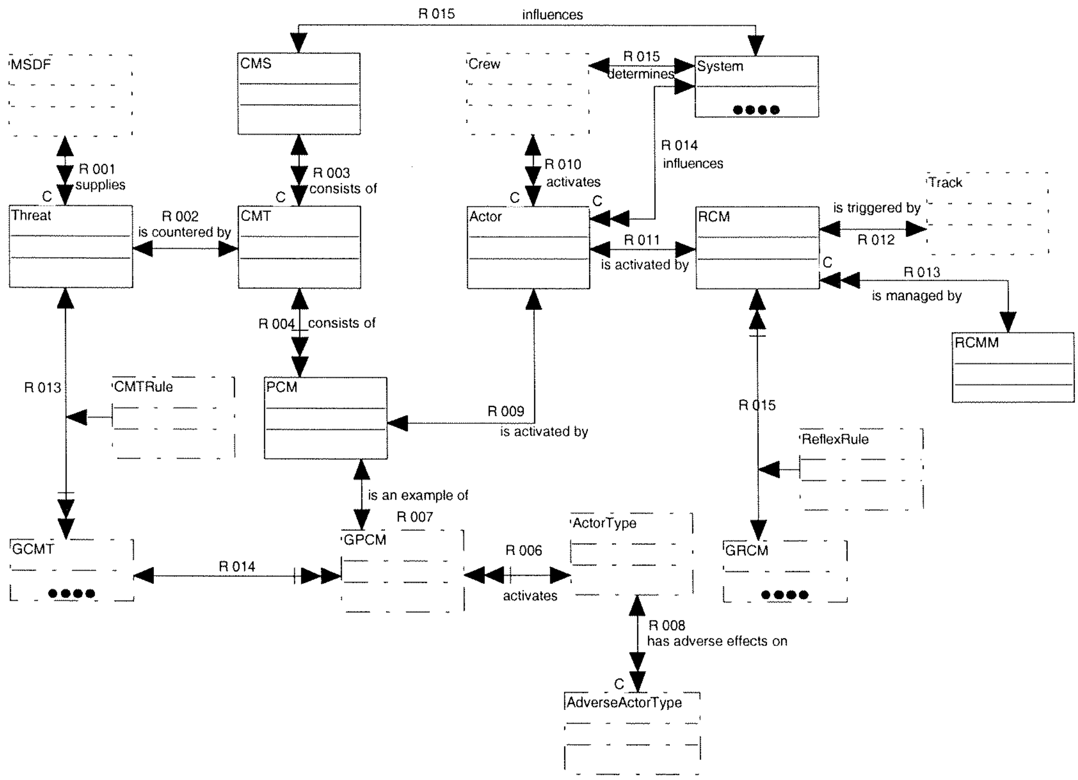



*Figure 2. The SPEW Manager S/M Object model*

## 2.4 Human-Machine Interface

The SPEW Manager adds an advanced colour threat display to the cockpit, from which the crew can select one of three views. The first is a list of detected threats. The second is a chase view of these threats, and the third is a god's eye view of the threat situation. The latter is shown in figure 3 (in reverse video, for clarity of presentation).

On the top left, the system mode of the SPEW Manager is displayed. In this case, this is automatic (AUTO). On top, the current jammer mode (XMT1), and the number of expendables available (40 chaff cartridges: C40 and 50 flares: F50) is displayed. On the top right, we see the operational mode (Run Silent: SLNT) in which the manager is running.

The ownship is displayed, accompanied by its flight plan. Detected threats are displayed within coloured circles denoting their range: each threat has its own colour. Friendly entities are shown in green. On the bottom, a time line displays the planned CMTs, in the colour of the threat they counter. These planned CMTs move from right to left (*t=0*): when a countermeasure is at the left, its execution will start.

We see that the first CM planned is J1: a jamming action. After that, ejecting chaff C and three more jamming actions J2, J3 and J4 are scheduled.

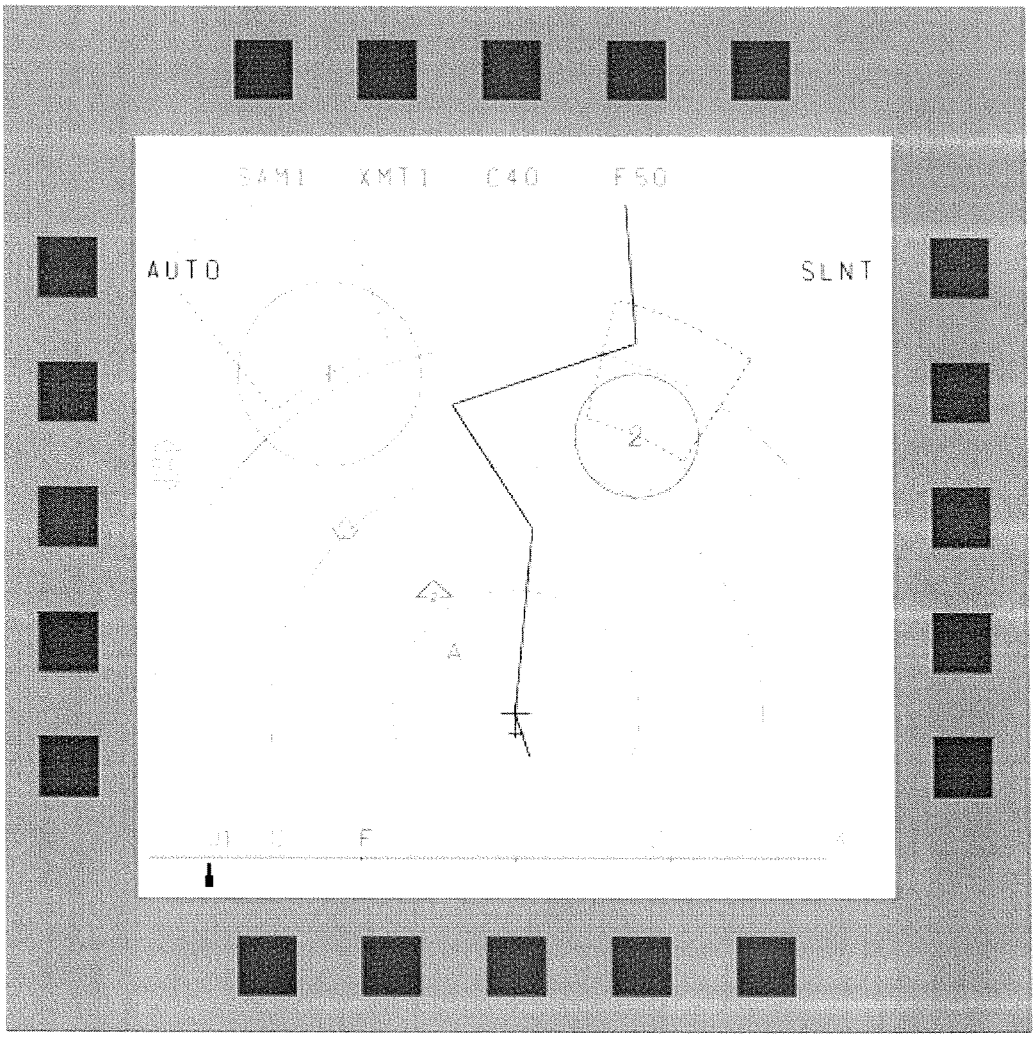



*Figure 3. God's eye view of the threat situation*

# 3 Countering the threats

## 3.1 Scheduling

Threat levels accompany threats. It is obvious, that threats with a high threat level (i.e., lethal threats) have higher priority than lower-level threats.

When we have selected a CMT for countering a threat, it may be possible that the CMT can not be executed immediately because either the actors it needs are occupied, or currently present threats prohibit the use of certain CMs that have negative effects on them (the so-called *adverse effects*). These negative effects are known to the scheduling process: they are supplied in a text file. When the CMT cannot be executed immediately, we have two choices:

- Schedule it and execute it at a later time;
- Do not counter the threat now, but wait until the actors that cause the conflict are released. Thus, this approach does not use any scheduling, only selection.

If we choose the first approach, we assume that we know what the threat and actor situation looks like in the near future, and thus which CMT is the best at that time, or whether a CMT can be executed at all. We can optimise the use of assets in the near future. The second approach has the disadvantage that no optimal use of assets can be guaranteed, but it has an important advantage: there is no need to predict the future. Whereas, in the first approach, CMTs, scheduled in the future, may become sub-optimal, obsolete or impossible due to (1) changes in the threat situation, (2) changes in actor availability or (3) changes in relative positions, the second approach only considers the present situation.

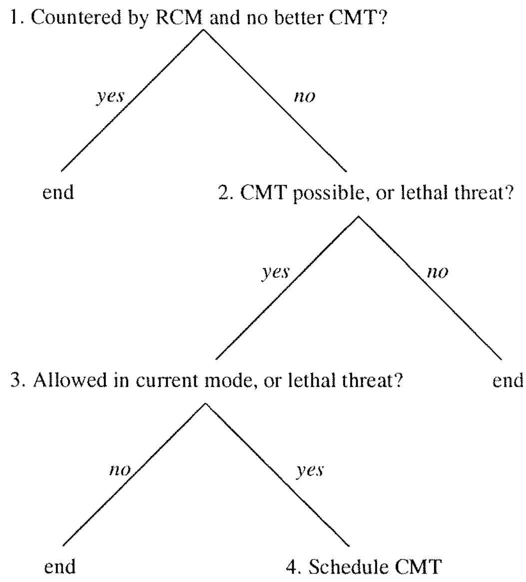
We did develop algorithms for both approaches. The one, using the first approach, was based on branch-and-bound [5] and showed promising experimental results. However, based on the considerations as mentioned above, for the (first) demonstration we chose the second, more down-to-earth approach.

### 3.2 Selection of rules

For each possible threat object, we made sure that at least one rule describing which generic CMT can be chosen to counter the threat with this vector. We assume that for threats that cannot be identified in detail, more generic identifications can be found, for which rules exist.

A rule contains a condition specifying whether the rule is applicable or not, based on the type of threat, and the relative position of it. Operational mode constraints can be present in these conditions as well. However, when lethal threats are present, we *do* want to be able to select these CMTs if no other CMTs are available. That is why CMTs that are not allowed to occur, considering the current operational mode, may still be chosen when a lethal threat is detected.

Since all elements influenced by the operational mode constraints: manoeuvres, chaff, flares and jammer actions, are all CM types, we simply check the operational mode when selecting a CMT and we try not to choose CMTs containing these CMs. However, if there is no alternative for countering the threat (there are no other CMTs available) and the threat level of the threat is high, we 'override' the operational mode. The notion "high" is configurable within the SPEW Manager, allowing fine-




tuning.

Note that when we select a CMT, we always prefer choosing a CMT that does not use manoeuvres, since manoeuvres often have negative influences on other CMTs (and perhaps on the flight plan). Only if there is no alternative, we choose the CMT containing a manoeuvre. If the operational mode *constraint manoeuvring* is active, we only choose the CMT containing the manoeuvre if the threat is lethal, even if there is no alternative.

### 3.3 The scheduling process

During the scheduling process, any event that may change the threat situation is handled to update the schedule of planned CMTs. There are several events that might change the schedule of planned CMTs: a new threat is detected, actors start to conflict, a CMT is finished, a threat has disappeared, an RCM is activated, or an actor has become available. We will describe the actions to undertake after each event below.

***New Threat Event***

When a new threat is detected, it depends on the availability of CMTs and actors what actions have to be undertaken. Essentially, the algorithm that is executed consists of four steps, and is depicted on the left. We will describe it below.

*Step 1*
Check if the new threat is countered by a RCM. If not, proceed to step 2. If it is, check whether there is a CMT that is expected to perform better. Is there no such CMT, then stop, else proceed to step 2. Note that when a conflict is present between the running RCM for countering threat *A* and a possible, better, CMT for countering *A*, we do not cancel the running RCM in favour of the CMT. Also note that the crew may have already countered the threat itself. In that case, selecting and scheduling a CMT may not be necessary. We do, however, not take this into account since we cannot know which threat the crew counters.

*Step 2*
Check whether at least one CMT is possible by looking at (1) the status of the actors, (2) possible conflicts with more important CMTs, (3) conflicts with crew-initiated CMs and (4) adverse effects. If after removing the impossible CMTs from the available CMTs to counter the threat, no CMT is left, *and* the threat is not lethal, then stop: no CMT is scheduled to counter the threat. Otherwise, proceed to step 3.

*Step 3*
If according to the operational mode, no CMT is allowed to execute, *and* the threat is not lethal, then stop: no CMT is scheduled. Otherwise, proceed to step 4.

*Step 4*
Here, we *always* schedule a CMT from the remaining list of possible CMTs. We prefer choosing a CMT in the following order:
1. No manoeuvres;
2. No negative influences on sensors;
3. Highest effectiveness.

In all four steps, CMTs containing manoeuvres are chosen only in the situation of a lethal threat. This is because manoeuvres usually have adverse effects on other CMTs and we do not want to interfere too much with the flying direction (e.g. mission planning, position with respect to other threats).

When a manoeuvre is suggested, it is not checked whether the manoeuvre is actually performed. This is due to the following reasons: manoeuvres are only suggested when the TL is high and there are no other good options. Therefore, the manoeuvre is required: there is no alternative for the crew not following the advice. Furthermore, it is hard to check whether the crew is performing exactly the required the manoeuvre.

***Actor Conflict***
An actor conflict occurs when an actor does not work properly anymore, e.g., it is broken, empty (no more chaffs or flares) or when the crew is using the actor while being occupied by a CMT.

All scheduled CMTs that require the actor in question are removed from the schedule. For the accompanying threats, new CMTs are selected.

***CMT Finished***
A CMT has finished regularly when all CMs of which it consists have finished regularly. The finished CMT is removed from the schedule.

***Threat Disappeared***
A threat can disappear. Either because of executed countermeasures (for instance: by the crew), or because an ambiguity has disappeared thanks to newly obtained sensor data, or for other, unknown, reasons. All CMTs, scheduled to counter the threat in question, are removed from the schedule.

***RCM Activated***
This event occurs when a software-implemented RCM is executed, based on the data in a raw sensor track. All CMTs, conflicting with the RCM, are removed. The accompanying threats are countered by other CMTs, if possible.

***Actor Available***
This occurs when the actor is released: the crew does not use it, no RCM uses it, and no CMT uses it (anymore). Taking action on this event is useful since we may have chosen a less effective CMT or no CMT at to counter threats. This is due to the fact that the actor needed to be used but was occupied at the selection time, or the CMT had an adverse effect on the actor. All threats, not being countered, are checked to see whether or not they can be countered now. All CMTs that have not started yet are considered to check whether a better CMT can be selected to counter the corresponding threat.

## 4 The demonstration

At the time of writing, a demonstration of the SPEW Manager is in preparation. The SPEW Manager implementation is embedded in the aforementioned ITEMS environment. ITEMS is a flexible software package that allows the user to generate a target-rich scenario without being limited to hard-coded sets of data. For our demonstration, ITEMS has been adapted to detail threat behaviour on countermeasures, and to obtain necessary* variables from the environment.

The demonstration runs on Silicon Graphics workstations for the ITEMS part and on a SUN Ultra workstation for the SPEW Manager itself. Ethernet is used to communicate between them.

Various scenarios will be run, both with an automated crew (in which a predefined flight path is flown and manoeuvre advice is automatically followed) and with human flight control. A very simple example of such a scenario is depicted in figure 5. There, ranges of threats do not overlap: no more than one threat has to be taken into account at the same time.

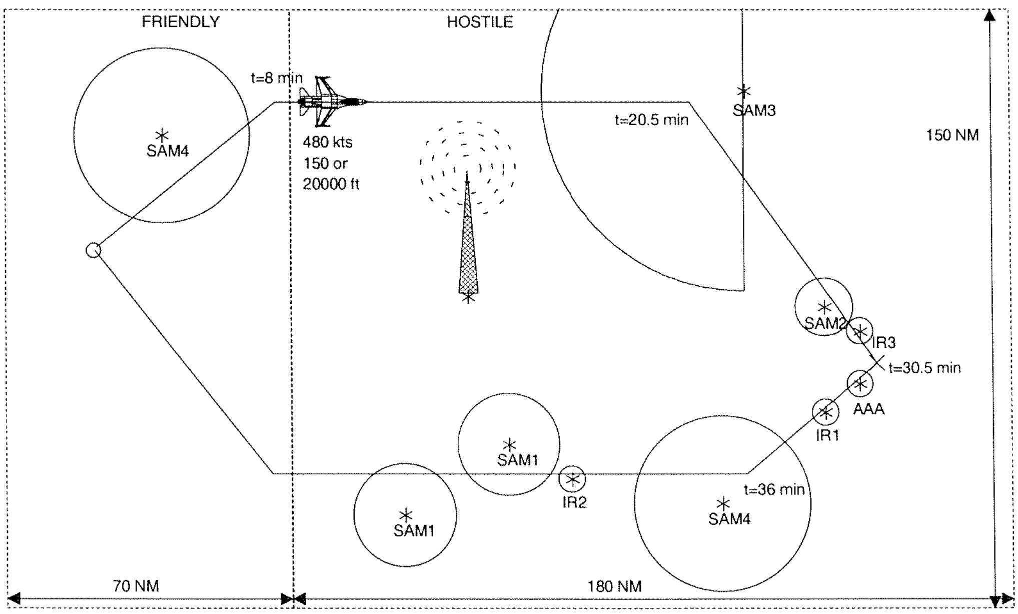



*Figure 4. A simple scenario*

The scenario consists of a threat theatre of 150 × 180 miles in which a number of ground-based threats are displayed. Circles around the threats denote the range of the search radar, belonging to the threat. Hence, these also denote when the ownship can detect the threat. For this paper, the depicted ranges do not correspond to real threat types.

The ownship in the depicted and a number of other scenarios is of the F-16 type. Next to F-16 (fighter) simulations, the feasibility of the SPEW Manager will also be tested using P3 Orion (surveillance) configurations. This involves a new set of actors to be loaded: the P3 Orion does not have as much countermeasures on-board, nor does it have the same manoeuvring capabilities as the F-16. P3 Orion simulations will prove the flexibility of our approach.

## 5 Conclusions and future work

Obviously, not too many conclusions can be drawn yet before the simulation results have been evaluated. However, we can see that the flexible design of the SPEW Manager, especially its configurability with respect to available actors and countermeasure techniques, results in a versatile and multi-platform electronic warfare improvement.

It is expected that a SPEW Manager such as ours is the only way to facilitate countermeasure techniques to be applied that require exact timing of its individual countermeasures. The demonstration will show this. Additionally, a SPEW Manager like ours will allow us to develop new countermeasure techniques, requiring exact conditions on timing and positions.

The way reflex countermeasures are fitted in show that our approach can take fighter hardware constraints, limitations and possibilities into account. The rules for selecting CMTs, kind of actors, and so on are easily configurable. This way, if an aircraft has other actors (or it concerns another aircraft), or if the rules are different, the SPEW Manager can still handle these new situations, without having to change the code. The modules that are configurable are the:

- CMT-rules;
- RCM-rules;
- Available actors including adverse effects on each other;

A jammer is effective when the aspect angle is within a certain range, which can be specified in the (configurable) actor description.

If in the future, other kinds of CMs are available (other than jammers, chaffs, flares and manoeuvres), new operational mode descriptions can be added easily as well.

Future work includes developing and applying more advanced real-time scheduling algorithms that, combined with better short-time predictions of the situation, will improve the performance of our SPEW Manager even more. Next to the mentioned techniques, constraint satisfaction approaches [6] look very promising.

Second, we will look at the possibility to include airborne threats, other than missiles. Essentially, these should fit in our approach without many problems.

Third, we will experiment with the Human Machine Interface. What information has to be supplied to the crew, and how should it be displayed? One can for instance imagine various ways to display uncertainty and ambiguous information.

**References**

1. Roost, J.J.M, and Ruys, D.P. *Combined and Interactive Self-protection ECM. Experience with Monopulse Systems.* Technical Paper TP 93-543, National Aerospace Laboratory NLR, Amsterdam, The Netherlands, 1993. Presented at the AGARD Avionics Panel Symposium on the Challenge of Future EW System Design, 18-21 October 1993, Ankara, Turkey.
2. Shlaer, Sally, and Mellor, Stephen J. *Object-Oriented Analysis: Modeling the World in Data.* Yourdon Press, Englewood Cliffs, New Jersey, 1988.
3. Shlaer, Sally, and Mellor, Stephen J. *Object Lifecycles, Modeling the World in States.* Yourdon Press, Englewood Cliffs, New Jersey, 1992.
4. CAE Electronics Inc., http://www.cae.com
5. Papadimitriou, C.H., and Steiglitz, K. *Combinatorial Optimization: Algorithms and Complexity.* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1982.
6. Tsang, E.P.K., *Foundations of Constraint Satisfaction.* Academic Press, London/San Diego, 1993.