15th ICCRTS
"The Evolution of C2"

A mixed-initiative advisory system for threat evaluation

Topics:

Topic 9: C2 Architectures and Technologies

Authors:

Hengameh Irandoust, Abder Benaskeur, Froduald Kabanza, Philipe Bellefeuille

Point of Contact:

Hengameh Irandoust

Decision Support Systems for C2 Section, Defence R&D Canada – Valcartier

2459 blvd. Pie XI North, Québec, QC, G3J 1X5, Canada

Telephone +1 (418) 844-4000 x4193

hengameh.irandoust@drdc-rddc.gc.ca

A mixed-initiative advisory system for threat evaluation

H. Irandoust, A. Benaskeur, and F. Kabanza

Abstract

Threat evaluation in naval Anti-Air Warfare (AAW) operations is accompanied by an unprecedented level of stress and cognitive overload for the operators mainly because of the dynamic and time-constrained nature of the context and the important amount of variables involved. A mixed-initiative capability is proposed that provides the operator with the needed information at different steps of his problem-solving task. Recognizing assistance opportunities, the capability provides, opportunistically, feedback that is adapted to the current problem-solving situation. Exploiting threat evaluation algorithms, the capability reasons on several inputs, such as the operator’s actions and preferences; the automation solution and its characteristics; and contextual information, in order to plan the best feedback in terms of content, format, and timing. While relieving the operator’s memory resources by representing the problem space through graphical interfaces, the capability uses several strategies to draw his/her attention on missing data, to highlight relevant (and sometimes overlooked) information, and to signal reasoning flaws. The proposed capability not only supports in this way the operator in his own inferential process, but is also capable of explaining and putting forth arguments in favour of its solutions in order to build the operator’s trust in its recommendations.

Keywords: Threat Evaluation, Naval Tactical Command and Control, Human-Machine Interaction, OMI, Argument, Situation Awareness, Decision Support

1. Introduction

Naval Anti-Air Warfare (AAW) operations expose the naval forces to threats that require recognition, identification, and prioritization and, if required, the application of combat power resources to counter the threat's intent to inflict harm. Currently, these functions are performed by a select number of individuals in the operations room through a series of cognitive processes. While the operators are reasonably adept at performing these functions for simple situations, with a very limited number of threats, their ability to effectively achieve similar results for multi-threat and multi-axes scenarios is severely hampered, given the increased number of variables involved. Furthermore, operations are increasingly conducted in the littoral, an operational environment characterized by high traffic, land-based threats, impeding meteorological conditions, and difficult terrain for naval operations, which is moreover, conducive to attacks from asymmetric threats. All these provide a new set of challenges for the Navy as the time and space for the defending force to detect and react to threats is reduced.

Threat evaluation in naval AAW operations is accompanied by an unprecedented level of stress and cognitive overload for the operators, mainly because of the dynamic and time-constrained nature of the context and the important amount of variables involved in decision making. This paper describes a Threat Evaluation Support System (TESS) that alleviates the cognitive workload of the operator and assists him/her by providing information both in a proactive and reactive manner. Affording a mixed-initiative collaborative problem-solving approach by allowing both parties (the operator and the system) to contribute to the process, TESS also justifies its recommendations by providing contextual explanations, and when necessary, convincing arguments.

The following sections describe the threat evaluation problem in naval operations from an operational perspective, the complexity of threat evaluation, the architecture and components of TESS and its operator-system interaction features and graphical interfaces which support the operators in their threat evaluation task, followed by the conclusion.

2. Threat evaluation from an operational perspective

Threat evaluation is part of Command and Control (C2) operations (Figure 1), of which naval AAW is a special case. Threat evaluation establishes the current intent, capability, and opportunity [1] of non-friendly entities within the Volume of Interest (VOI) based on a priori information (*e.g.*, intelligence, operational constraints and restraints, evaluation criteria, etc.) and dynamically acquired and inferred information (*e.g.*, kinematics and identification of entities as captured by the sensors and compiled in the tactical picture, as well as various indicators), and data received from complementary sources in relation to the mission objectives [2,3]. The output of threat evaluation along with that of engageability assessment, which

determines own options against potential threats, is used by the combat power management process to generate and optimize response to the threat (Figure 1).

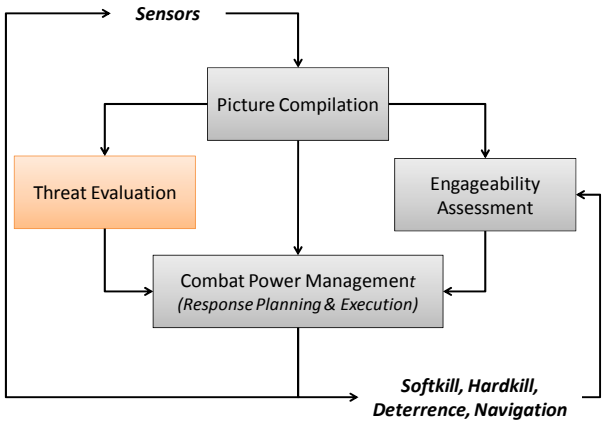

Figure 1: Command and Control Process [2]

Threat evaluation is an ongoing process of determining if an entity intends (*i.e.*, threat intent) and has sufficient resources (*i.e.*, threat capability) to inflict harm on the defending forces and/or their interests, and whether the environment provides the required preconditions for the entity’s plan to succeed (*i.e.*, threat opportunity). It also comprises the classification of threats into categories, such as high, medium, or low, along with the ranking of such entities within each category according to the level of threat they pose to a specific defended asset (*e.g.*, ownship, high value asset or infrastructure).

2.1 Intent indicators

Intent inferences are hard to derive, making intent assessment the most difficult component of threat evaluation. Some indicators such as the track position, speed, identity, or responses (or the absence thereof) to Identification Friend or Foe (IFF) interrogations are readily available from the tactical picture (as a result of the picture compilation process in Figure 1), a priori database or communications from other units in the force. Other indicators such as the Closest Point of Approach (CPA) or conformance to civilian air lanes are easily computable using automation tools. The indicators that are hardest to determine are for example threat manoeuvres, tactics, group composition, deceptive behaviour, etc. As an example, indications of hostile intent for an aircraft may be flying a direct approach/attack profile towards the defended asset or not adhering to warnings.

2.2 Capability indicators

Capability indicators are generally available from a priori data (*e.g.*, intelligence, database, etc.). Observations made during operations come to confirm the a priori information on the

threat capability (*e.g.*, characteristics of platforms, sensors, and weapons). One of the challenges with capability evidence gathering and exploitation is when dealing with asymmetric threats.

2.3 Opportunity indicators

As with intent indicators, some of the opportunity-related indicators are readily available from the tactical picture or a priori data, others are easily calculated and others are much more difficult to determine. Indeed, as with intent assessment, some instances of opportunity assessment require a predictive analysis of the threat behaviours, *e.g.*, analyzing a trajectory taking into account the engagement geometry, dynamic models (of the entities in the VOI), and potential obstructions.

3. Cognitive demands during threat evaluation

The complexity of a task can be quantified in terms of the potential number of erroneous ways to perform the task for each correct way [4]. Complexity increases proportionally with an increased probability of selecting an erroneous choice as opposed to the correct one. As such, the overwhelming environment, the spectrum of potential threats, and the diversity of the adversary tactics and manoeuvres render the effective execution of naval threat evaluation a complex task. More specifically, threat evaluation is a highly demanding cognitive task for human operators mainly because of the huge amount of data to be analyzed, the level of uncertainty characterizing these data, and the short time available for the task.

3.1 Time and uncertainty

Efforts to establish effective threat evaluation are shaped by two fundamental factors that characterize any (tactical) military operation - uncertainty and time. For threat evaluation, operators have to deal with the unpredictability of (adversary) human behaviour and the imperfection of information sources on which operators rely to observe the environment (including the adversary). These two elements contribute significantly to uncertainty.

Time is another key factor in threat evaluation for three main reasons. Firstly, the information gathered and compiled during the picture compilation process, as well as the knowledge derived by the threat evaluation process remain valid for only a finite period of time. Secondly, time is a resource (both for own force and the adversary) which is consumed as information is gathered and processed. Thirdly, the tempo of the operation, or battle rhythm, puts a constraint on the time resource. The more time a force spends on gathering or processing information to reduce uncertainty, the less time the force will have to decide and act, leaving more time to the adversary for his own information gathering, processing, and action cycle.

3.2. Large amount of data

Operators in charge of threat evaluation must analyze a huge amount of data, of which only a small fraction is relevant to the current situation. The data, which can come in multiple forms and from multiple sources, include threat characteristics but also many other contextual information. Operators have to make difficult spatial and temporal inferences from this large amount of noisy, uncertain and incomplete data. The difficulty of this task is increased by time constraints and several other factors.

In a series of studies conducted by Liebhaber and his colleagues [5-7], it is shown that due to the multi-tasking, tempo, integration demands, and short-term memory requirements, threat evaluation is cognitively challenging under usual conditions, and possibly worse under extreme conditions. It requires mental integration and fusion of data from many sources. That integration/fusion requires a high level of tactical expertise, including knowledge of the types of threats, the own force's mission, own and adversary doctrines, and assessment heuristics built from experience.

Currently, most operation systems only provide support to operators through the display of a picture of the current tactical situation, with information on the identity and kinematics of the entities within a certain VOI. There is, however, no explicit support for the comprehension of the meaning and the relationship of objects, neither for the inferences about their intent, capability and opportunity. Yet, the latter are the areas where much difficulty resides. Threat evaluation functions can be significantly enhanced through the introduction of automation-based solutions and decision support tools.

3.3. Errors and biases

When evaluating threats, human operators proceed by interleaving an "evidence gathering" loop and a "hypothesis generation and evaluation" loop. The evidence gathering loop involves observing objects and analyzing their behaviour to determine evidences as to their intent, capability, and opportunity to harm the defended asset(s). Various errors can be made during this process; some of these may be due to missing knowledge or a failure to consider all relevant information; others may be due to judgment biases. For example, the confirmation bias consists in seeking information consistent with current beliefs and avoiding contradictory evidences.

Liebhaber et al. [5-7] have observed that during the threat evaluation process, operators formulate a hypothesis about the current track (which is assumed to correspond to an object in the environment) by activating a threat profile that corresponds to the type of object (*e.g.*, commercial aircraft or military aircraft). After the activation of a profile, the operator evaluates the presence of indicators of the profile, and generates a plausible assessment based on the

support or contradiction of the indicators. The authors observed that operators participating in this study did not switch profiles in lieu of conflicting data but accommodated these data into their active and persistent profile. Finally, participants appeared to be influenced by specific indicators rather than the overall pattern of data. For example, they were likely to change threat evaluation if only one of the high weighted indicators contained data that conflicted with their expectations.

The cognitive analysis of threat evaluation by Liebhaber and his colleagues is in line with the naturalistic decision making view [8], which suggests that experts simply recognize situations based on experience and spend little time on deciphering the complex interrelationships that appear in the data. They sense the situation, make hypotheses and test and monitor for supporting evidences. In this case, the decision support system must ensure that the operator is not missing some information and that he has not overlooked relevant data.

4. Overview of Threat Evaluation Support System (TESS)

Based on a study [2, 3] eliciting the naval personnel’s cognitive/decision support and information requirements to perform naval Command and Control (C2) in general, and threat evaluation in particular, the Threat Evaluation Support System (TESS) proposed here has adopted several design principles. Of primary importance was the requirement to provide *decision support* rather than *decision automation*. Other factors include support for situational awareness, supporting communication between operators about the threat evaluation tasks, reducing operator workload, building operator trust in decision support recommendations, and allowing operator override. Furthermore, while helping the operators keep track of relevant criteria and constraints and critical information during problem solving, the capability aims to draw the operator’s attention on neglected information.

The architecture of TESS is illustrated in Figure 2. There are three main components, the testbed, the algorithms and the advisory capability, all described in detail in the following subsections.

A threat evaluation scenario is simulated in the testbed, the events and objects of which are compiled into a tactical picture. The algorithms use this picture along with the operational constraints, which are either static (provided by the mission framework) or dynamic, *i.e.* evolve as the scenario unfolds. Domain knowledge is also used to calculate the threat level of objects of interest and rank them.

The advisory capability uses the solution provided by the algorithms, domain knowledge, the current constraints and user information, to formulate its feedback to the user.

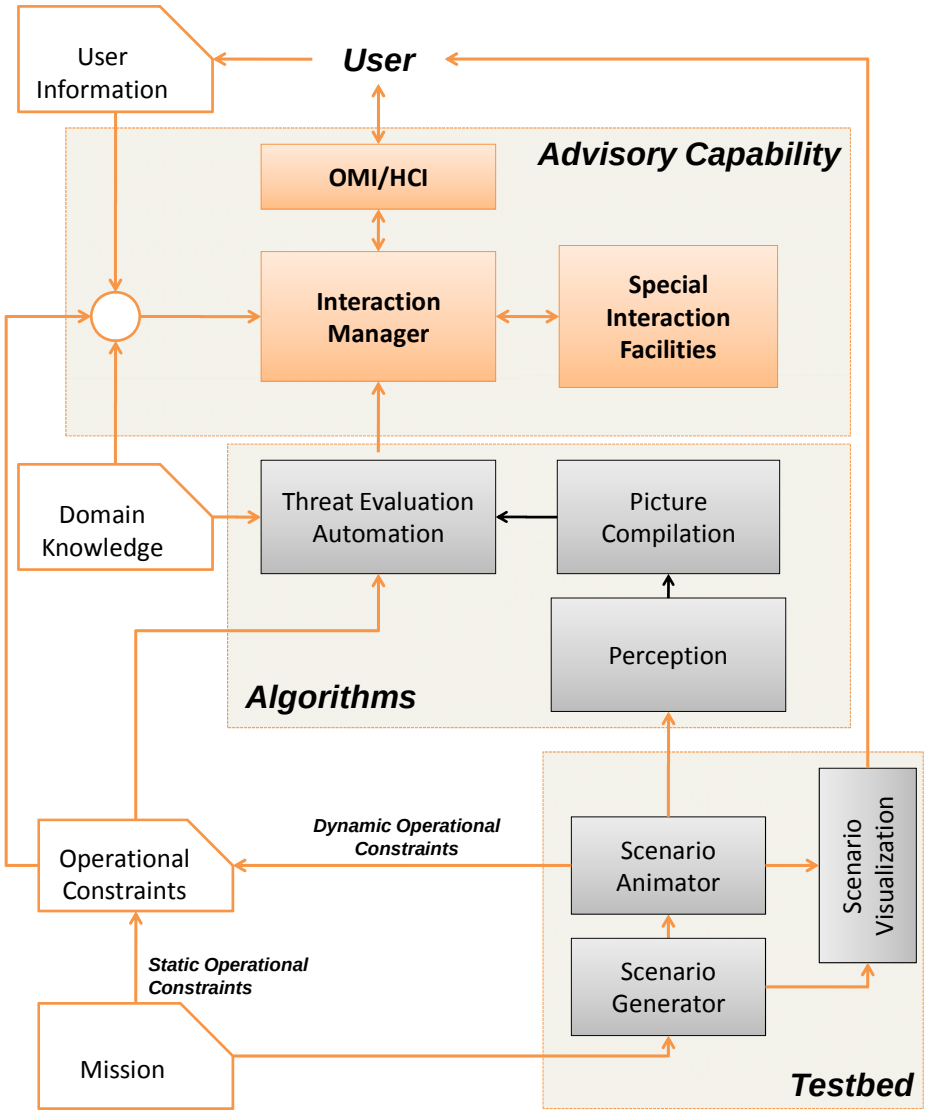

Figure 2: Architecture of TESS

4.1 Testbed

Scenarios related to naval AAW operations are generated, simulated, and visualized in the testbed. The testbed has been developed by integrating several Commercial Off The Shelf (COTS) applications as well as custom applications. It includes, among others, the following main capabilities:

- A flexible scenario generation tool, provided through the integration of the Presagis Stage® Scenario COTS tool.
- A high fidelity ship synthetic environment for scenario simulation, provided through the integration of the BAE Systems’ Ship Air Defence Model (SADM®) COTS tool.

- 3D and 2D visualization capabilities, provided through the integration of the SIMDIS Governmental Off The Shelf (GOTS) tool[1] and its inherent capability to connect to SADM.

The overall architecture of the testbed is based around the OpenSplice Data Distribution System (DDS). This DDS uses a "publish-subscribe" paradigm in which different software components that comprise the system are very loosely coupled.

4.2 Algorithms

This component is comprised of a set of automation algorithms that allow for detection, localization, identification and evaluation of threats. Currently, rule-based and Bayesian-based algorithms are implemented. However, the discussion of the automation algorithms and the underlying architecture is beyond the scope of the current paper.

4.3 Advisory Capability

The Advisory Capability manages the interactions between the operator and the automation and the information provided through the Operator-Machine Interfaces (OMI). The remainder of the paper presents the Advisory Capability, which is comprised of the Interaction Manager, the OMI, and Special Interaction Facilities that provide visual and textual feedback.

4.3.1 Interaction Manager

The core of the advisory capability is the Interaction Manager, which has several roles:

- monitor the user and determine his needs for information
- analyze the user's input and hypotheses
- analyze the operational situation
- evaluate the data on which the automation solution is based
- decide on the feedback to be given to the operator

As shown in Figure 2, the Interaction Manager uses several sources of information to plan its feedback (i.e., the information to be displayed for the operator):

- **The operator's input, profile and preferences:** This information includes data relative to the history of past interactions, the operator's preferences in terms of characteristics of information output, his profile (role, expertise, etc.), and his actions, which are continually monitored. User information is provided to the Interaction Manager through two channels.

[1] SIMDIS was developed by the US Naval Research Laboratory.

Some of the static information concerning the operator's preferences is entered by him at login time. Dynamic information is collected as he/she enters data or manipulates the input devices.

- **Domain knowledge**: This includes all the rules, causal relationships, etc., necessary for the assessment of the intent, capability and opportunity of the objects. This component will also account for criteria, constraints, and restraints that should not be violated during the threat evaluation process. Some of this information can be configured by the operator. The operator can add, modify, and delete categorization criteria and data to be used to assess or prioritize threats. Ultimately the operator may accept or reject the automation's recommendations regarding the intent, capability or opportunity of a given threat.

- **Operational constraints and restraints:** These are relative to the current tactical situation. These constraints (must do) and restraints (must not do) can be static, such as mission plans, Rules of Engagement[2] (ROE), and dynamic operational parameters that evolve as the situation unfolds. Time available for information exchange with the operator is also part of the operational context and is taken into consideration by the Interaction Manager when providing feedback.

- **Threat evaluation automation algorithms output:** The output is not only the result reached by the algorithms, but also the intermediate results and the level of certainty associated to them. The latter will enable the Interaction Manager to express its level of confidence in the automation results. The intermediate results enable it to decide in which format the solution must be presented to the operator. The question to be answered by the Interaction Manager is: *How this information must be provided to the operator given its quantity, degree of complexity, criticality, novelty, uncertainty, etc.?* And *what must be its granularity (level of details to be included)?*

For example, the Interaction Manager will present the occurrence of critical new evidence as a textual/audio warning, but it will provide a visual representation when it comes to flight profiles, from which the operator may infer intent (if the object's flight path is 'on course' then the intent inference could be that it is 'friendly', while if the object veers 'off course' the intent inferred may be biased towards 'hostile'). Depending on the nature and characteristics of the information, the Interaction Manager would display or communicate it differently. However, the operator may define his or her preferences regarding how the information is to be displayed on the computer screen.

[2] In threat evaluation, this refers to what own-force knows (or assumes) about the adversary ROE.

Thus, exploiting threat evaluation algorithms, the Interaction Manager accepts several inputs, such as the operator’s actions and preferences; the automation solution and its characteristics; and contextual information, in order to plan the best information presentation for the operator in terms of content, format and timing.

4.3.2 Special Interaction Facilities

Special interaction facilities are triggered for cases which cannot be handled by the OMI. This includes the visual representation of information or putting it into textual form. One of the cases where this becomes necessary happens when the Interaction Manager has to justify the automation’s assessment for the operator. This justification is necessary to provide insight to the system’s reasoning and convince the operator of the soundness of the system’s recommendations.

Several cases are possible. Sometimes, the operator does not disagree with the system’s recommendation - he simply does not understand how a given conclusion is reached. This means that an explanation of the system-generated solution must be provided. In TESS, most explanations are contextual and embedded in the different functionalities of the system. Through the Detailed Information Area and drill-downs, described in Section 4.3.3, the operator can access all the low-level information from which a given categorization or ranking is proposed by the system. But some domain related explanations can be provided upon operator’s request.

Another case, where the system would attempt to justify its view, is when the operator overrides its recommendation. The purpose of the justification is not to resist the operator’s decision, but to make sure that the operator has considered the information on which the system’s assessment is based. Since the ultimate responsibility for the decision related to threat evaluation lies with the operator, the Interaction Manager accommodates and reacts coherently to any reasonably anticipated input to the threat evaluation problem solving process. More specifically, the Interaction Manager allows the operator to make contributions to the problem-solving activities and to override all assessments and decisions generated by the automation. However, in order to avoid errors and biases, it verifies whether the operator has understood the system’s rationale and has not neglected important information.

For example, the operator can change the categorization of a threat, in which case the system will ask for evidence, assuming that the operator has access to some information missing from the system’s database. The operator can ignore that request and proceed with his own solution, input the data he has privileged access to, or indicate that no new evidence is available. If no new evidence is provided, the system will conclude that the operator is overlooking some piece of information. It then verifies whether the data from which the system’s recommendation has been derived satisfy the conditions of sufficiency. For instance, if a certain indicator is

sufficient by itself to establish a 'hostile intent', then it suffices to draw the operator's attention on that indicator through visual means. Sufficient criteria are already listed in the Detailed Information Area and will be highlighted accordingly. However, if the system's conclusion is based not on specific significant indicators, but on a combination of different pieces of information, in that case, the Interaction Manager will build an 'argument' which captures that set of data and will present it to the operator textually. Thus arguments are used when the indicators they are based on are not informative enough by themselves.

In TESS, arguments are built from a set of evidences that verify the conditions for a certain conclusion, following Toulmin's deductive structure of arguments [9] where the inference from a set of *data* to a *conclusion* or *claim* is legitimated by a *warrant* and possibly a *backing*. The warrant is in fact that piece of domain knowledge that justifies that a conclusion can be derived from some data, while the backing provides the deeper rationale.

Given the nature of the underlying automation algorithms, it is not only the evidence (indicator of intent, capability or opportunity) that is taken into account, but also the certainty associated with that piece of evidence and the weight associated to that type of evidence. Thus, the problem solving process used by the algorithms can be summarized by the following expression:

$$(E_1,CF_1,We_1,..,E_n,CF_n,We_n) \rightarrow (D,CF)$$

Where E is evidence, CF_i certainty factor, We weight, D decision, and CF the global certainty factor. The decision can be reached from one or a set of evidences. The weight of evidences influences how easily the decision can be made. The certainty factor (CF) is derived from that of the individual evidences (CF_n). The argumentation facility uses this reasoning and its results to construct the arguments. Thus, the decision reached by the algorithms becomes the system's claim or conclusion and the evidences become as many arguments justifying that conclusion. There is not, however, always a one-to-one relationship between a decision and a conclusion. The argument structure is as follows:

$$(A_1,CF_1,..,A_n,CF_n) \rightarrow (C,CF,W_a)$$

where A stands for argument, C for conclusion, and CF for certainty factor, and W_a for warrant. The latter is reflected in the system's argumentation, conveying the level of confidence of the system in its decision. The weight is not expressed in the arguments, as the operator knows the relative importance of the evidences. It can however be used in the warrant, W_a , which is the component that explains, if asked for, that a given conclusion can be reached from a set of evidences, thus justifying the validity of the inference.

The explanations and arguments, provided by the system, ensure that the rationale behind the automation results is understood and that the data used to reach those results have not been overlooked by the operator. They are by no means used to counter the operator’s decisions. The latter has, in all cases, the last word.

4.3.3 Operator-Machine Interfaces

Given the time-constrained environment in which the users operate, rather than dialoguing with the operator, it is preferred to transition most of the information through effective interfaces. Other than being communicative, appropriate interface design can remove much of the burden on working memory resources [10]. Thus, many of the variables, constraints and their dependencies, which are normally handled by the operators, are offloaded to the graphical interface. To that end, a functional view is used in TESS.

Functional view

Decision making is facilitated when a higher-level of data abstraction is presented from a functional (task-related) versus physical (geo-spatial) perspective. To improve the decision-making capability of the operators with respect to threat evaluation, a functional view (Figure 3) has been designed which accompanies the classical physical display.

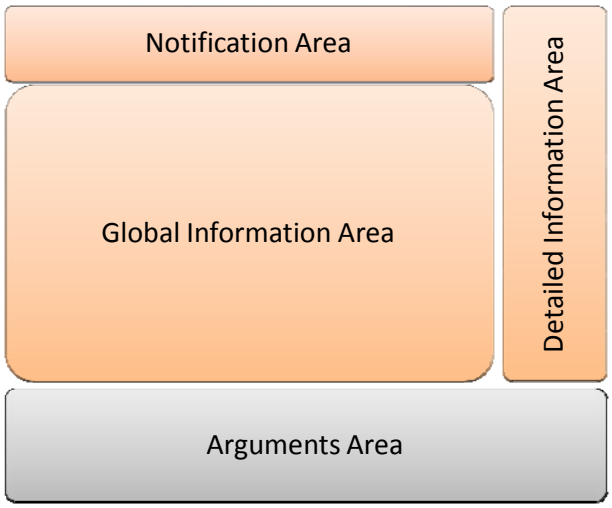

Figure 3: Functional display layout

The threat evaluation functional display will address deficiencies that exist in geo-spatial (physical) displays. Currently, the operators must hook (click on) each individual object/track in order to gather the necessary kinematical information to perform the threat evaluation task. The physical display can also lend itself to ‘tunnelling’ whereby the highest priority threats may not be visible should an operator range in. The threat evaluation functional display aggregates all of the threat-specific data into a comprehensive picture of the situation.

The purpose of the threat evaluation functional display is to augment the operator's ability to make decisions with respect to the recognition, categorization, and prioritization of threats in the VOI. The operator may of course choose to perform the threat assessment and its sub-processes himself from low-level sensory data. The role of the functional view is to synthesize the overwhelming information and to provide threat assessment as a function of intent, capability, and opportunity, with supporting rationale. To that end, the operator decisions are simplified to deciding upon the validity of the recommendation.

The Notifications Area is used to display events (or changes) that warrant the operator's immediate attention. As an example, the appearance in the VOI of an object which has passed some predefined quick reactive test[3] will be notified as a warning to the operator in the Notifications Area.

The Global Information Area contains a 2D threat list that provides an amalgamated view of the categorization and relative rankings of all threats in the VOI relative to the reference point (ownship or defended asset), as calculated (initially) by the threat evaluation algorithms.

The Detailed Information Area contains the detailed information and rationale for the threat evaluation presented in the Global Information Area, thus providing insight into the assessment rationale. The Arguments Area is only visible when required to provide further insight in support of the automation assessment. As discussed above, arguments are only required and presented, as supplemental information, in the absence of the conditions of sufficiency.

A subset of the pertinent design constraints and heuristics which form the basis of the overall OMI design philosophy is:

- **Requirements for situational awareness:** Having good Situation Awareness is a key determinant of task performance and relates to the ability of the operator to maintain awareness of task-relevant objects in the defending force's immediate environment. It is vital, therefore, that operators are given accurate and timely information relating to relevant entities in the environment.
- **Group related information together:** Operators must integrate information about several variables in order to evaluate the degree of threat and decide on actions. Tasks that require mental integration of information will benefit from close display proximity. Therefore, on the threat evaluation display, information is grouped into four functional areas in order to illustrate the relationships between the data elements. The visualization of the threat environment is enhanced by providing a comprehensive and prioritized list of all threats. This threat list provides an integrated view of a series of threat properties (*e.g.*,

[3] Which can mean that the object satisfies the criteria of high-level threat requiring immediate action.

categorization, ranking, opportunity). As such, the operator is no more required to hunt for the individual rankings comprising this list and is able to view the relationships between the properties of individual threats. At the same time the operator can have access to 'ungrouped' data upon request.

- **Provide rationale for system recommendations:** One solution for maintaining system transparency of the advice or solutions offered by a decision support system is to provide the operator with the capability to drill-down and view any data used to derive the assessment as well as the assessment itself. That is, the interface provides a means by which they can explore the original sources from which the assessment was constructed. Understanding the system's rationale for its assessments helps to instil operator trust with the system-generated recommendations.
- **Keep the operator engaged in the decision loop:** The collaborative mixed-initiative feature of the advisory capability ensures that the operator is not removed from the decision loop. By establishing a dialogue and requiring the operator's input to the problem solving process, the system keeps the operator engaged as much as possible.

It is anticipated that the 'big picture' offered by the threat evaluation functional display, as presented, will also help to address the phenomenon of 'saturation and recovery'. In situations, such as operations in the littoral environment whereby the density of tracks is high, the operators' ability to accurately perform the threat evaluation task may be saturated. The threat evaluation functional display will assist the operators by providing a consolidated list of prioritized threats as opposed to relying on the operators to generate and maintain this list dynamically. Given the operational tempo during an engagement, discussions with the operational community have indicated that all attention and energy will be focused on an engagement until its completion. This may result in the global appreciation of the threat situation to be lost. Upon completion of an engagement, the threat evaluation functional display will support recovery from the attack by providing the operators the ability to quickly re-focus on the larger picture of the existing threats in the VOI.

5. Illustration of interaction features and OMI

This section illustrates some of the interaction features and OMI of TESS. It must be noted that most of the functionalities and mechanisms presented have been validated by naval operators.

As shown in Figure 4, the x-axis represents the time or range (to be chosen by the operator) to the defended asset and the y-axis represents the threat ranking. In this context, a threat is any object identified as non-friendly (*i.e.*, hostile, suspect, neutral, unknown, and assumed friend). Each threat (or swimlane) is assigned a relative threat ranking number with the highest threat ranked '1' at the top of the list. By clustering threats into four categories: high-level (red) threat; medium (yellow), low (white), and don't care (grey), the rationale is to help the operator maintain global situation awareness while focusing on those objects that are more threatening.

As a threat’s time (or range) to the defended asset changes, it will move horizontally from left to right along the x-axis (within its swimlane, if relative threat ranking is stable). As a threat’s relative ranking increases or decreases with respect to other threats, it will change swimlanes up or down accordingly.

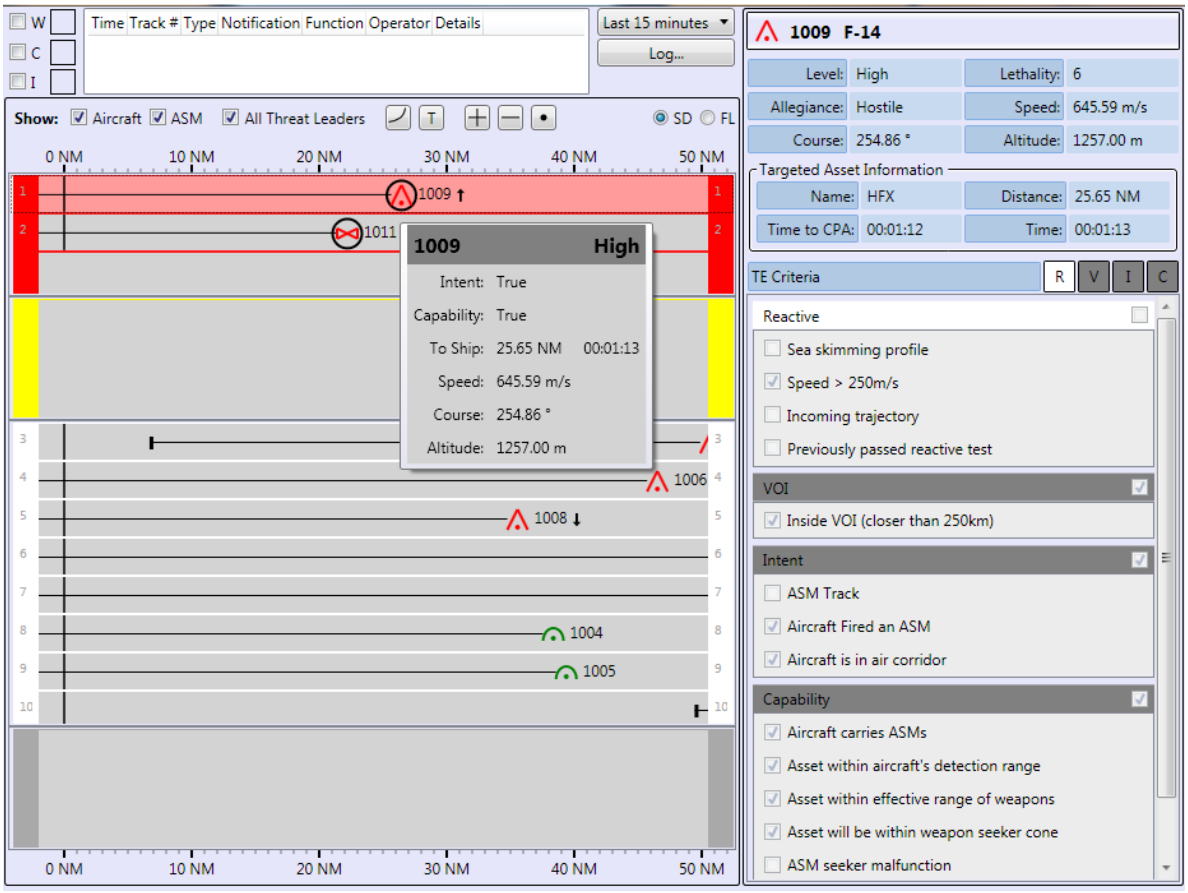

Figure 4: Threat evaluation display

By nature, the inclusion of decision aids to support the categorization and prioritization of threats is intended to assist the operators with being more proactive versus reactive. The presentation of ranked threats with a temporal or spatial relationship to the defended asset(s) provides the operators with the ability to view threats getting closer and the resulting impact on the threat’s categorization and ranking. Moreover, the functional view increases the operator’s ability to anticipate potential engagements since the capabilities of each individual threat are clearly visible. Specifically, the operator can witness the point at which the threat can sense and engage the defended asset(s).

The Detailed Information Area, on the right, shows the primary threat attributes at the top, information on targeted asset (if not ownship), and compliance with assessment rules. Displaying both the rules and the system’s assessment of the outcome allows the operator not

only to understand the rationale regarding the assessment but also assists with predicting category jumps. In certain situations, the operator may be able to provide additional information to refine the assessment.

Within the Detailed Information Area, the threat assessment rules are grouped and presented based on the **R**eactive Test, the **V**OI (Volume of Interest) Test, **I**ntent, and **C**apability. The operator can select these criteria and obtain low-level information on processed data. This enables him to agree or disagree with the system's assessment. This information can be manually entered by the operator thereby forcing the system to re-calculate the threat ranking based on the new data.

In Figure 4, there are a few neutral tracks (green semi-circles) represented in the white zone, which have been identified as civilian aircrafts. In addition, a few hostile[4] aircrafts (triangular red) are represented in the white and red zones. One of the hostile aircrafts is assessed as a high level threat (track # 1009). In fact, the track #1009 has just moved to this rank, as indicated by the arrow to the right of the track number. To make sure the operator has noticed the change, the swimlane is blinking red. For a quick appreciation, the operator can select the threat to see its attributes in the rollover (intent: true; capability: true).

In Figure 5, the operator overrides the system's solution. He has decided to move the track #1009 to the medium threat level category, even though the algorithm had classified it as a high threat. To show that this threat was moved by the operator, a "!" icon appears next to the track and the swimlane is highlighted. The system displays a message (not shown here) asking for the operator's rationale for this change. As mentioned before, when the system's recommendation is overridden, if the Interaction Manager assesses that the operator has neglected or overlooked important information (*e.g.*, threat indicators, criteria) that is sufficient for justifying a given assessment, then the operator's attention is drawn on that information by visual cues. Thus, the threat level information that justifies the system's categorization is highlighted in the Detailed Information Area. These are sufficient arguments for the system's categorization of the threat as high. If the operator is convinced and clicks on the icon, the track goes back to the category in which the algorithm had classified it.

As shown in Figure 6, the operator justifies his ranking by unmarking the indicator 'Aircraft carries ASMs' in the Detailed Information Area. This helps the system to understand the operator's position. The fact is that the track which had momentarily disappeared from the display was near to a base and had enough time to reload ammunition. The system has assessed that it is highly likely that the aircraft carries ASMs. Given the non-straightforward nature of this information, the advisory capability decides to present it as textual arguments, displayed in

[4] From the NATO identification (country of origin) perspective and not from intent perspective.

the Arguments Area in the bottom of the screen (Figure 6). Once again, the operator is free to accept or ignore this information.

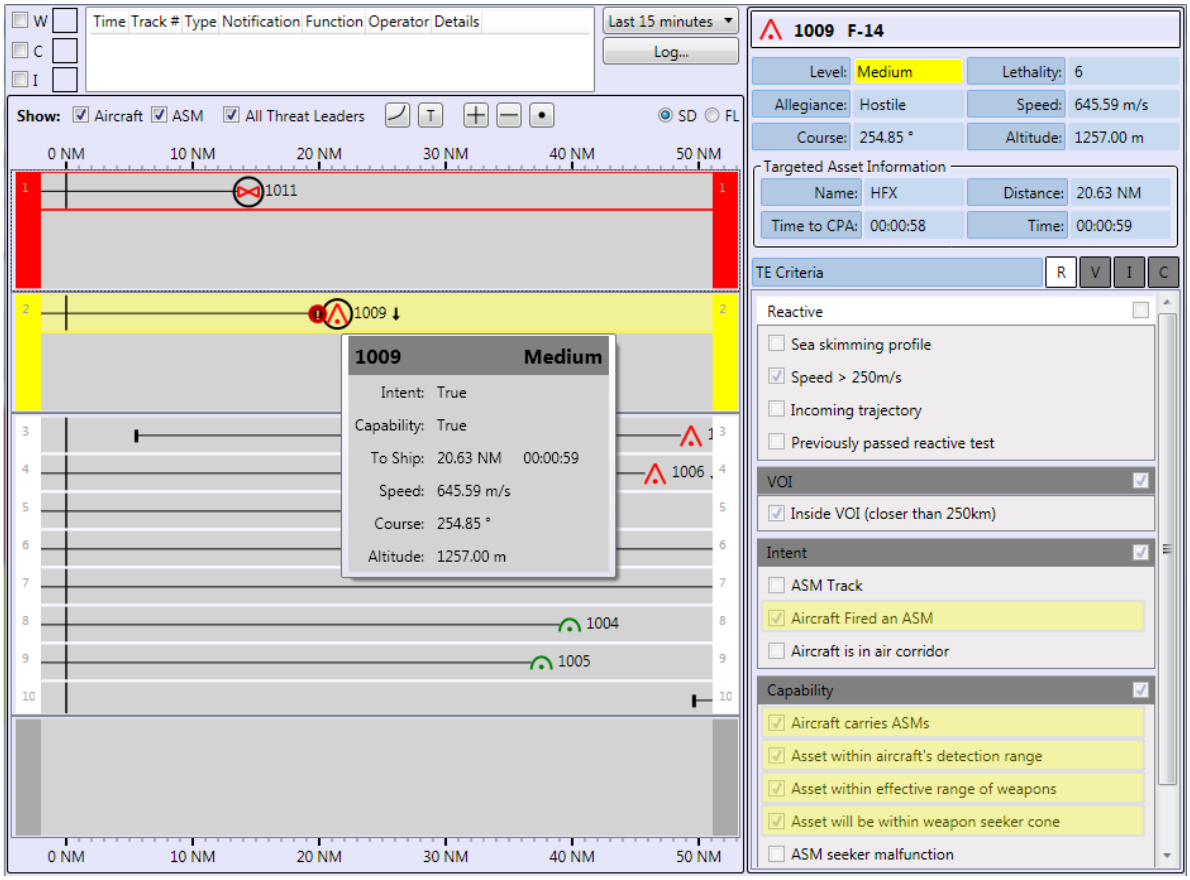

Figure 5: User overrides system evaluation

As shown in these illustrations, with the mixed-initiative paradigm, the advisory capability and the operator attempt to solve the problem collaboratively. The advisory capability uses different strategies of assistance. It monitors and analyzes the operator’s assessment as he performs the threat evaluation and intervenes when necessary. It helps the operator by reminding him of current criteria, constraints, restraints, and all other relevant factors during the problem solving process. It makes recommendations, provides explanations, and draws the user’s attention on critical data but also on information that may have been overlooked.

6. Conclusion

The system described here is aimed at actively supporting threat evaluation which is currently being performed primarily through a series of cognitive processes by the operators. The proposed capability supports the operator in different ways. First, it relieves the operator’s memory resources by representing the problem space through graphical interfaces. The OMI design concept for the threat evaluation functional display enhances visualization of the threat

environment; increases the operator’s ability to anticipate potential engagement actions, and improves the ability of the operator to quickly view details for each threat. Canadian Forces naval operators involved in a Human Factors experimentation to assess the threat evaluation capability of a previous version of the system concluded that the capability is well designed, increases overall situation awareness, improves decision making abilities and is easy to use [11].

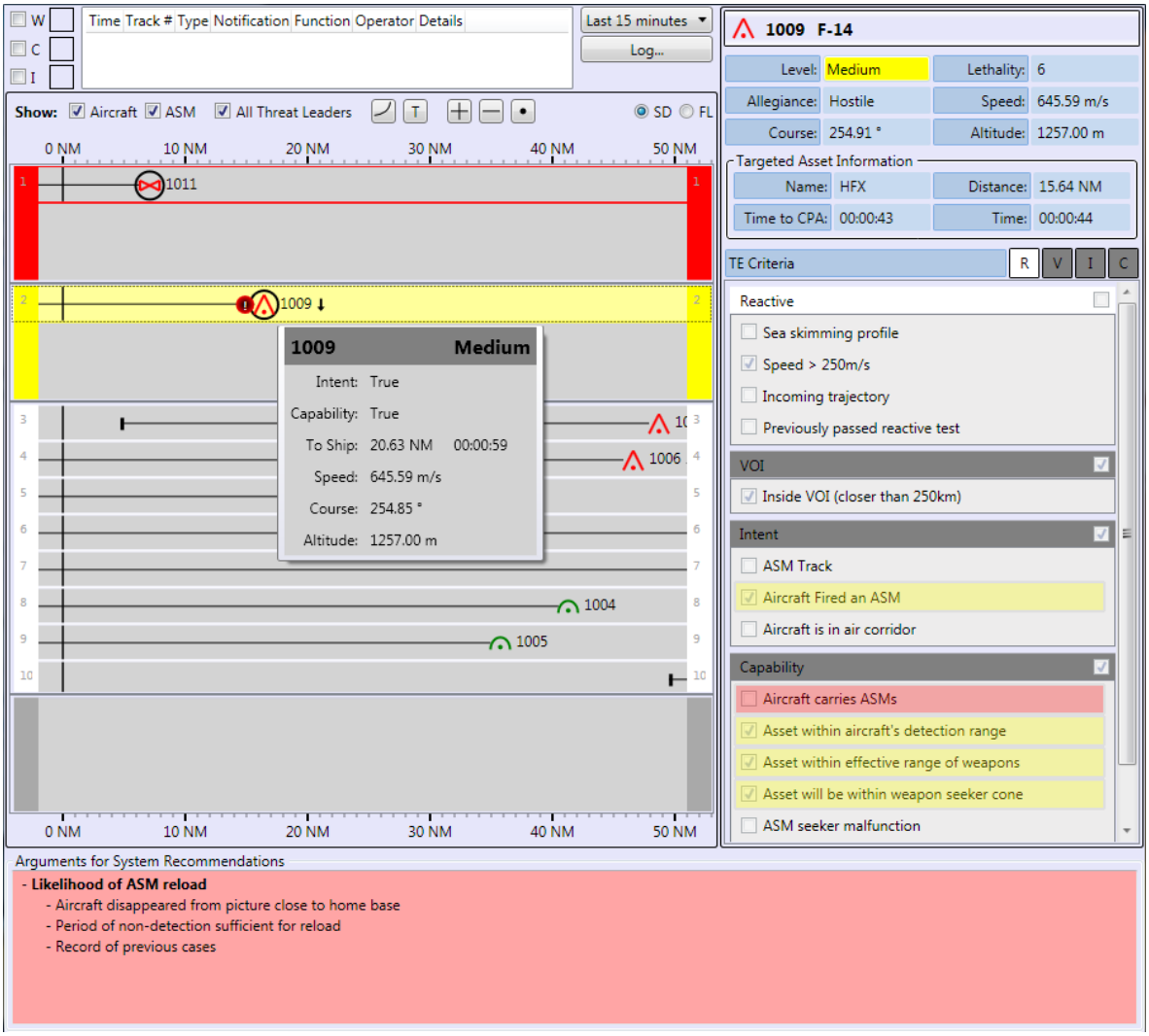

Figure 6: Arguments against operator’s threat ranking

As presented, the advisory capability also uses several strategies (visualization, arguments, etc.) to present complex information. While it proactively draws the operator’s attention on relevant information, it also reacts to what may be errors, biases and reasoning flaws on the part of the operator.

The system is based on a mixed-initiative paradigm, which means that both parties, the system and the operator, contribute opportunistically to the problem solving process. The aim of the advisory capability is primarily to support the operator in his own inferential process by providing all the necessary information. Also, to be transparent and trustworthy, it provides explanations and justifications for almost all of its recommendations, while allowing the operator to override them and ultimately stay in control of the decision making process.

References

1. Steinberg, A. (2007) Predictive Modeling of Interacting Agents, *Proceedings of the International Conference on Information Fusion* (Fusion), pp. 1–6.
2. Irandoust, H., A. Benaskeur, K. Baker, S. Banbury (2009) *Naval Force-level Tactical Command and Control – Mission Analysis and Problem Characterization*, Technical Report, DRDC Canada – Valcartier, TR 2009-199.
3. Benaskeur, A., H. Irandoust, K. Baker, S. Banbury (2009) *Naval Force-level Tactical Command and Control – Goal Hierarchy and Analysis*, Technical Report, DRDC Canada – Valcartier, TR-2009-197.
4. Bar-Yam, Y. (2003). *Complexity of Military Conflict: Multi-scale Complex Systems Analysis of Littoral Warfare*. Report to Chief of Naval Operations Strategic Studies Group, 2003.
5. Liebhaber, M. and Feher, B. (2000), Naval air defense threat assessment: Cognitive factors and model, In *Command and Control Research and Technology Symposium*.
6. Liebhaber, M. and Feher, B. (2002) Air threat assessment: Research, model, and display guidelines, In *Command and Control Research and Technology Symposium*.
7. Liebhaber, M., Korbus, D., and Feher, B. (2002) Studies of U.S. Navy Air Defense Threat Assessment: Cues, Information Order and Impact of Conflicting Data, (Technical Report 1888) SPAWAR System Center, San Diego, USA.
8. Zsambok, C.E. and Klein, G.A. (1997) *Naturalistic Decision Making*, Lawrence Erlbaum.
9. Toulmin, S.E. (1964), The Uses of Argument, Cambridge University Press.
10. Smith-Spark, J.H., Glasspool, D.W., Oettinger, A., Yule, P. and Fox, J. (2005) Planning, working memory, and interface support in a medical domain. In B. Hommel, G. Band, W. La Heij and G. Wolters (eds.) *Proceedings of the 14th Conference of the European Society for Cognitive Psychology*. Leiden, Netherlands: European Society for Cognitive Psychology, pp. 22-23.
11. *INCOMMANDS Sea Trials Command Decision Support Lab Prototype: Human Factors Evaluation for Sea Trials Command Decision Support Capability Prototype*, DRDC Toronto CR 2009-041. Scientific Authorities: S. McFadden, W. Wang, & A. Benaskeur.