COSIMAR: Continuous Operational Signature Monitoring Awareness and Recommendation

J.A.A.J. Janssen, PhD[1], H. Hasenpflug[2], M. Janßen[2,3]

[1] *TNO, The Hague*
[2] *CSSM, Kiel*
[3] *Corresponding Author. Email: michaeljanssen@bundeswehr.org*

Synopsis

Crews of naval vessels lack an up-to-date awareness of those aspects of a ship's susceptibility to threats that are related to the actual ship signatures (acoustic, magnetic, infrared, etc.). The ship's susceptibility depends among others on the current configuration of the ship, the environment, the enemy sensor capabilities and the related ship signature levels. For operational purposes, it is desirable that crews have a tool which informs and advises them on the ship signatures, on ways of managing them and on the consequential detection ranges of adversary sensors in the current tactical situation. A functional demonstrator for such a support tool, called COSIMAR (Continuous Operational Signature Monitoring Awareness and Recommendation), has been developed and tested in a laboratory environment in an international project. The background and approach of this international cooperation between Canada, Germany, Norway, Belgium and The Netherlands had been presented at the INEC conference 2014 in Amsterdam. This year's presentation will show the result of this joint effort. The architecture, human machine interface, signature and susceptibility models will be addressed, including the laboratory environment simulating all required platform and environmental input.

Keywords: Ship signatures; Signature Management, Marine systems; Susceptibility, HMI

1. Introduction

During a naval ship's mission, it is preferable to detect, identify and engage or avoid adversaries before they become aware of the own ship's presence and before the adversaries themselves are able to engage. The sensor suite of the own ship provides the capability to detect and identify the adversaries. As adversary threats also use sensors to 'counter' detect and identify the own ship, it is key to have a low observability of the own ship (e.g. stealth). The observables of the own ship are known as the ship signatures: a ship signature is the manner in which a ship manifests itself to a certain type of sensor and how detectable and recognizable it is when such a sensor is used to observe the ship. As adversary military threats use sensors in different physical domains (acoustic, infrared, magnetic, radio waves, etc.) it is the total of its signatures that makes a platform more or less observable.

During the design phase of a naval ship, measures are incorporated in the ship design to reduce the ship's signatures. Unfortunately, the ship signatures cannot be reduced completely and on top of that these designed-in signatures can deteriorate during the life cycle of the ship. Therefore, naval ships are 'ranged' regularly to measure their signatures and if possible these signatures are adjusted to the designed signature levels. For example, repairing noisy equipment, or deperming and adjusting the degaussing currents. Typically, the signatures of naval ships are measured with relatively long-time frames in between (e.g. frigates 2 years, submarines yearly and mine countermeasures vessel yearly). The signatures though can change on a continuous basis. Even more dynamically signatures depend on the operating mode of the ship (e.g. speed influences noise level) which needs to be taken into account for operational assessment and decisions. In addition to the dynamically changing signatures, also the environment (atmospheric conditions, seawater salinity, etc.) influences the way how the signature exposes itself towards a threat. The environment is even more dynamic and cannot be designed-in in the ship design. Due to this dynamic behaviour the crews of naval vessels lack an up-to-date awareness of those aspects of a ship's susceptibility to threats that are related to the actual ship signatures. A notion of the current signatures of the own ship and ways to influence and manage them contribute to the overall operational effectivity and survivability. This forms the basis of a ship signature management system and is graphically depicted in Figure 1.1.

To demonstrate the feasibility of a ship signature management system, a study towards a stand-alone functional demonstrator of a ship signature management system for surface ships is conducted (see also [1]). This demonstrator called COSIMAR (Continuous Operational Signature Monitoring Awareness and Recommendation) is a cooperation between Canada, Germany, Norway, Belgium and The Netherlands with the

 http://doi.org/10.24868/issn.2515-818X.2018.027

coordination of CSSM (Centre for Ship Signature Management). COSIMAR is demonstrated in a lab-based environment as a standalone application.

In this paper, first the concept of a ship signature management system is given in Section 2. Section 3, describes the architectural approach, the type of signature models used, the simulators and the approach used to interface all software modules. The Human Machine Interfaces are highlighted in Section 4. Finally, Section 5 states the conclusions.

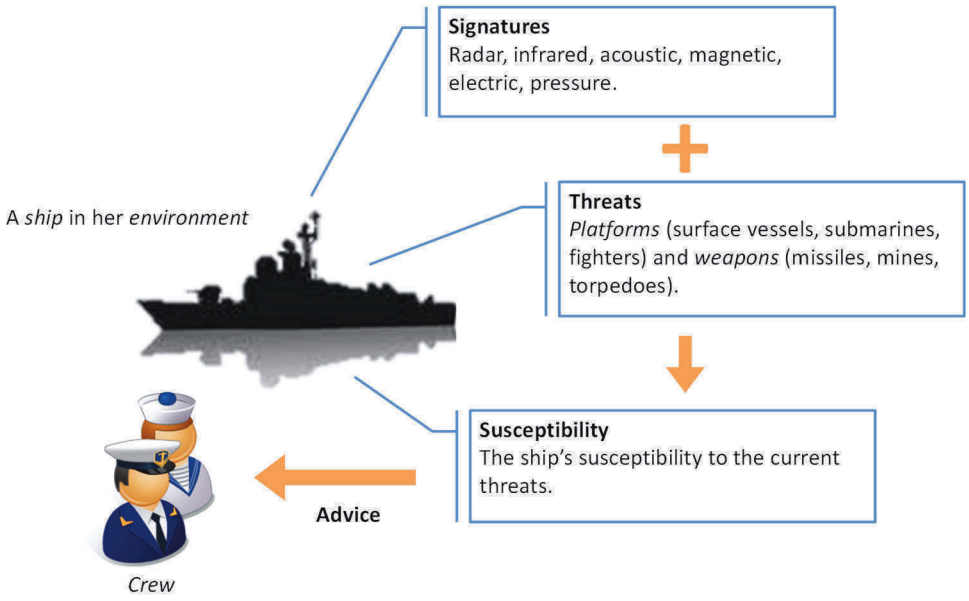


Figure 1: Schematic depiction of an operational tool to inform and advise a ship's crew on both the signatures of the own platform and ways of managing them.

2. Ship Signature Management

The purpose of a signature management system is to contribute to the overall operational effectivity and survivability of a naval ship. Having low signatures provides the ability of a ship to operate undetected against specific threats, supports effective use of own sensors (e.g. sonar self-noise level) and an effective use of decoys. A ship signature management system should provide the following functionality:

- Inform the crew about the own ship's current signature-related susceptibility given the current threat situation;
- Advise the crew which measures to take to improve the own ship's current signature-related susceptibility given the current threat situation;
- Enable the crew to investigate alternative solutions to improve the own ship's susceptibilities at alternative locations and/or under alternative environmental condition and/or alternative threats by adapting the ship configuration and/or course;
- Alert the crew on abnormal deviations of the own ship signatures and/or signature sensors and support the diagnosis of the possible causes.

The COSIMAR demonstrator also must consider the commander's intentions (based on the command aim), the expected threats, and the environmental parameters. An actual estimate of the ship's signatures and especially the impact on the ship's susceptibility must be made available in an operationally useful format.

The anticipated users of a COSIMAR-like ship signature management system are:

- *Warfare officer:* responsible for the tactical operation of the ship. The warfare officer can use information about the own ship signatures to plan the ship's actions;
- *Tactical operator:* responsible for ship signature management among many other tasks. When the ship signature deviates from the normal the operator is alerted. The operator assesses the consequences and advices the warfare officer. In case of malfunctions, the operator also contacts the technical crew;

 http://doi.org/10.24868/issn.2515-818X.2018.027

- *Technical crew:* the technical crew can be anywhere on the ship. It is not expected that a technical crew member will continuously monitor the technical condition of the ship (i.e., sudden deviations from the norm), rather it is likely that the primary action comes from the tactical operator, the result from a warning indicating a signature-related problem, or from the automated system.

3. System Architecture

3.1. Ship Signature Pipeline

The signature-related susceptibility depends on the configuration of the own ship (ship speed, gas turbines power settings, hangar door open/closed, hull cooling on/off, etc.), the own ship's navigation settings and the own ship's environment (e.g., temperature, wind speed andwater salinity). The ship susceptibility is also dependent on the threat situation: the set of adversary platform and weapon types that are of tactical interest to the own ship and instances of which might appear in the next few hours or days.

The COSIMAR ship signature management system uses various models to compute the signature-related susceptibility. A ship has various ship signatures on which it can be detected by adversaries. The COSIMAR demonstrator includes the infrared, radar cross section, acoustic, magnetic, electric and pressure signature. For each of these signatures, ship signature models, propagation models and threat models are developed by the various partners, resulting in 'signature pipelines'. These signature pipelines provide estimated exposure data that is related to specific sensors hosted by specific threats. Calculating the exposure data follows for all signatures a similar pattern (see Figure 2). First the signature at the location of the own ship is calculated. This can be based on sensor data (e.g. acoustic sensors) or models (e.g. pressure signature). Then in a second step, signature specific propagation models are used to calculate the own ship signature at the location of a possible threat. In a final step, the propagated signature is used to compute the detection ranges or depths for the threat sensors.

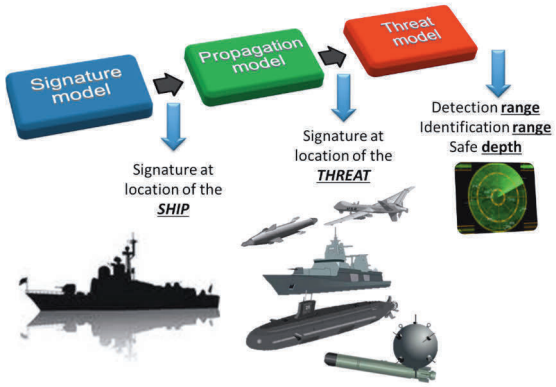


Figure 2: Schematic overview of the signature pipelines.

3.2. System-of-systems

For COSIMAR a 'system of systems approach' was selected as the architecture pattern, this enables a modular approach, while still providing the freedom of choice during the implementation phase. When defining building blocks within such architecture, the functionality of each block together with interface definitions are key elements. When well defined they enable using the building blocks as 'black boxes' of which the functionality is unambiguously defined while the content may be 'closed'. COSIMAR provides a framework in which signature, propagation and threat models are loosely coupled integrated. This open architecture assures that the international partners can integrate their own nationally developed models. These models can either be shared or can be kept national. In Figure 3 the included models from the various partners are shown.

 http://doi.org/10.24868/issn.2515-818X.2018.027

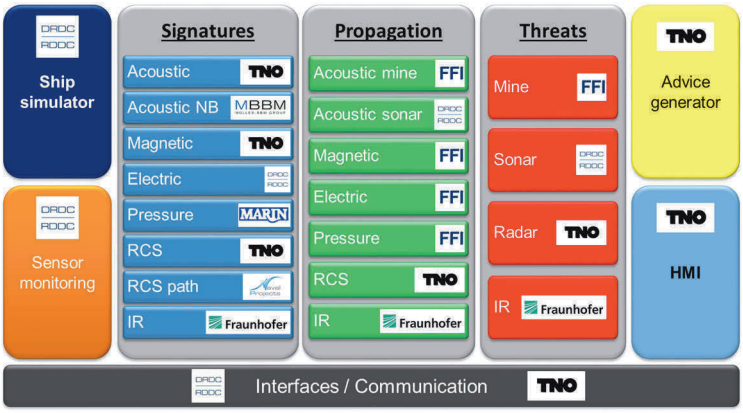


Figure 3: Architecture building blocks.

3.1. System Interfaces

As was shown in Figure 3, the COSIMAR demonstrator uses various software modules of various participants. Since the data collection system and the signature, propagation and threat models are foreseen to be separate processes running largely independently from each other, the architecture should support multiple, independent and concurrently executing processes that may be written in different languages (e.g. C++, Java, Matlab and other) and run on different operating systems (MS Windows, Linux and other). Each process is expected to run on its own computer platform, with all platforms connected to a standard high-speed wired network (Ethernet) that allows for a swift exchange of large data volumes and for simple but efficient process-process synchronization.

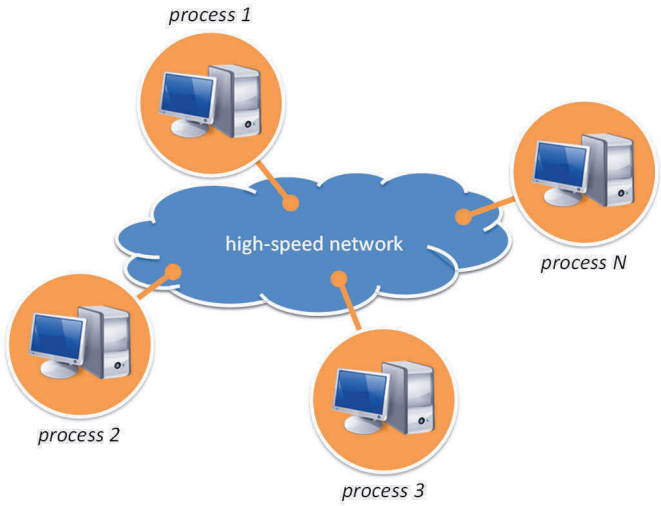


Figure 4: Overview of the system physical architecture. Individual processes each run on their own computer platform, connected via a high-speed (ether)network.

For the data exchange between the models the publish/subscribe messaging pattern is selected to allow a dynamic network topology while maintaining network scalability. All models can both act as publishers as well as subscribers to exchange data over the network. To discriminate between messages, topic-based publish-subscribe messaging is used. In this approach, messages are published to named logical channels called topics. Subscribers will only receive messages published to the topics they are subscribed to. All processes subscribing to the same topic will receive identical copies of the messages published on that topic. An example is shown in Figure 5: Model X publishes a data element in Topic A. Model W and Model U are subscribed to Topic A and immediately receive the data that is published on Topic A by Model X. Model X also publishes on Topic B, both Model U and Model Y receive the published data. Model Y also published data on Topic C which the is received by Model Z.

 http://doi.org/10.24868/issn.2515-818X.2018.027

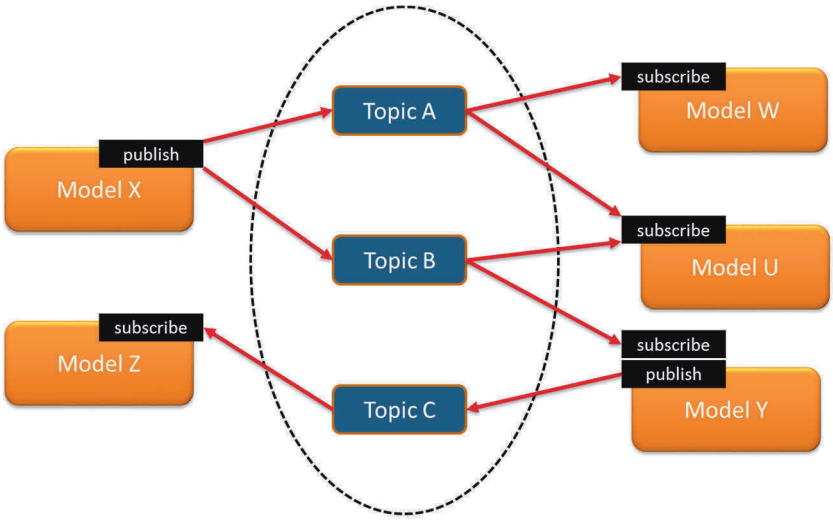


Figure 5: COSIMAR communication approach.

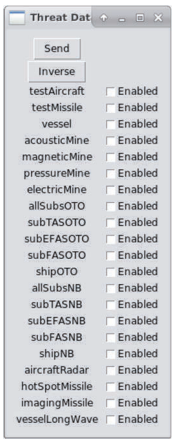
3.2. Simulators

The various models in the signature pipelines use own ship information (e.g. own ship noise), environmental data (e.g. meteorological data), the status of relevant ship assets, the expected threats and tactical settings. In an on-board implementation this data would be provided by signature sensors, weather stations and the ship platform management system,combat management system and the bridge system. The COSIMAR demonstrator is a demonstrator in a laboratory environment. Therefore, the virtual ship simulator SCORSIM (Signature COntrol Room SIMulator) is developed that provides all required data for the models in realistic scenarios. It provides:

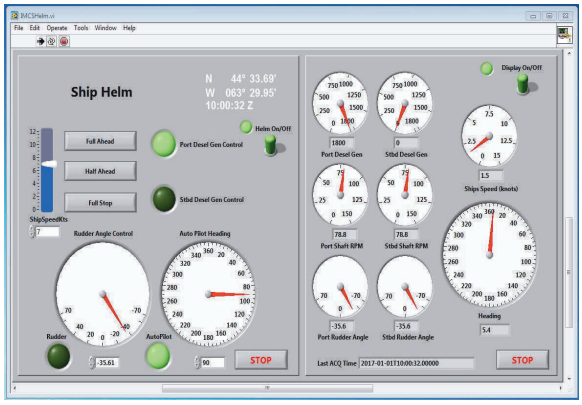
- The expected threats;
- The priority of the warfare domains;
- Helm control;
- Own ship data such as course, speed, etc.;
- Machinery states;
- Environmental data including atmosphere and bathymetry;
- Signature sensor data such as hull vibrations; shaft currents; hull potential; magnetic data; door sensors; hull temperatures;
- Signature errors (the ability to introduce defects in sensor readings).

An overview of the simulator suite is shown in Figure 6.

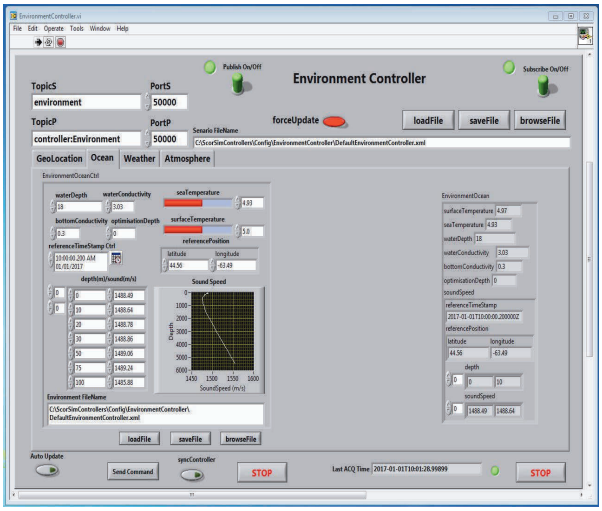
 http://doi.org/10.24868/issn.2515-818X.2018.027



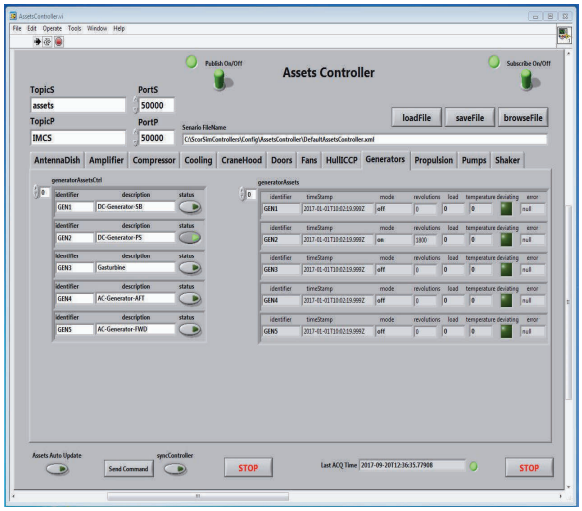
Threat database and warfare domain settings



Helm control



Environmental settings



Asset configuration

Figure 6: Simulators for the COSIMAR demonstrator.

4. Human Machine Interfaces

As mentioned in Section 2, a ship signature management system supports as well the tactical operator as the technical crew. These users have a different view on the status of the ship signatures. In this section, both the operational view (Section 4.1) and the technical view (Section 4.2) are described.

4.1. Operational HMI

The results of the susceptibility analyses are shown to the tactical operator on a dedicated graphical user interface, the COSIMAR HMI (Human Machine Interface). Besides an indication of the detection ranges or safe depths, the HMI also shows which signatures contribute to these detection ranges / depths and how it relates to the warfare domains (AIR, SURFACE, SUBSURFACE and MINE). The priority of the warfare domain is set by the warfare officer. Based on the computed detection [u1]ranges or depths in combination with the priorities of the warfare domains the COSIMAR demonstrator generates advices to the tactical operator to optimize the current ship signatures. To be able to generate these advices, the models are interrogated by the COSIMAR advice module in order to determine what will change when a specific action is applied (e.g. reduce ship speed). These advices are also presented in the HMI.

The COSIMAR HMI is shown in Figure 7. This HMI shows the detection ranges and safe depth areas on the map of the tactical display (left side panel). The right side panel shows detailed signature information. This right side panel contains two tabs: CURRENT and WHAT-IF. The CURRENT tab contains all information and controls for the current situation; the information under the WHAT-IF tab can be used to plan a mission. In both tabs generic information such as the time, speed, position and course are shown. Below the header ‘THREATS and SUSCEPTIBILITY’ an information block is created for each of the four warfare domains (AIR, SURFACE,

 http://doi.org/10.24868/issn.2515-818X.2018.027

MINE and SUBSURFACE). The border colour of these blocks shows the priority of each of these warfare domains as set by the warfare officer: RED means high priority (e.g. threats expected); YELLOW means medium priority (e.g. threats may appear) and WHITE no priority (e.g. no threats expected for this warfare domain).

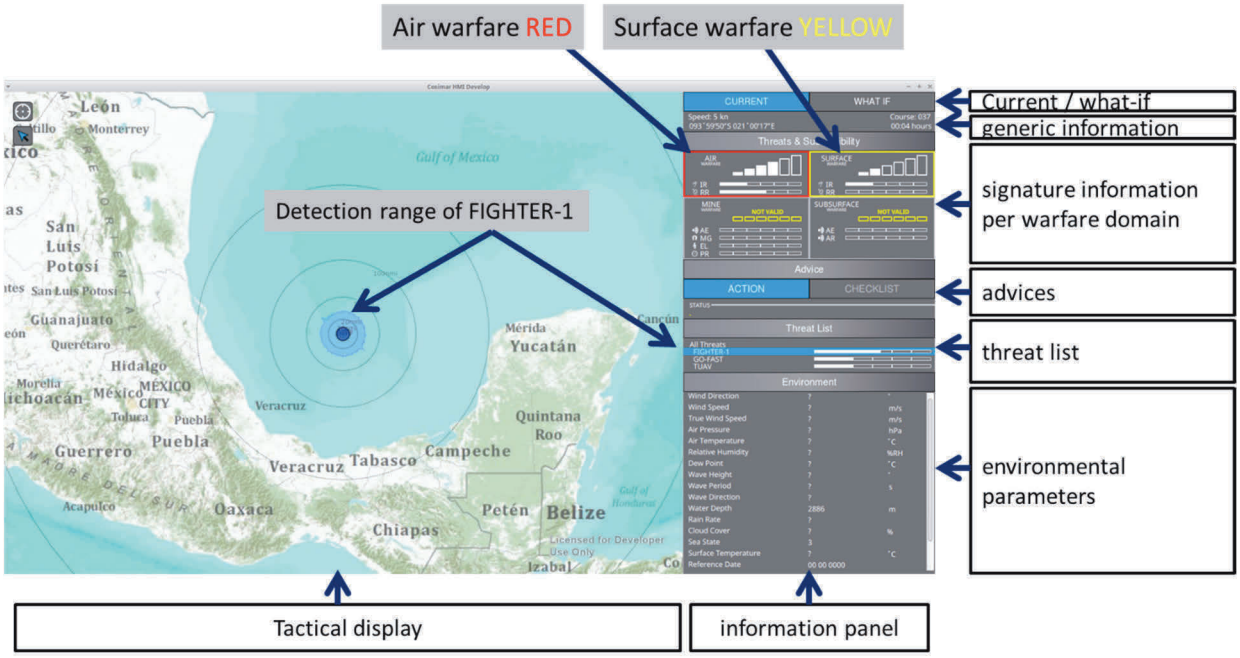


Figure 7: COSIMAR Human Machine Interface

Inside each warfare domain block, a strength indicator shows the susceptibility of the ship to threats in this warfare domain. The more bars the higher the ship's susceptibility. With increasing susceptibility, the bars grow and turn orange, red and finally the complete block turns red (see Figure 8). This block also shows which signature(s) contribute to the shown susceptibility.

Figure 8: The indicator shows the ship's susceptibility to a threat. Above figure show the susceptibility to a mine threat at high ship speed. Four signatures (acoustic, magnetic, electric and pressure) can contribute to the mine threat susceptibility as shown below the strength indicator. In this case the main contributor is the emitted acoustic noise (shown by the horizontal bar), a secondary is the pressure signature.

When the susceptibility reaches the 'orange' bar, COSIMAR will generate an advice to reduce the ship's signature. Only for warfare domains with a priority indication of RED or YELLOW advices are generated because only in these warfare domains threats are expected. An example of an advice is shown in Figure 9. In this case it is advised to reduce speed in order to reduce the acoustic signature (indicated by AE (Acoustic Emission)). The advice also shows in a horizontal bar the predicted resulting signature reduction when the advice is followed.

Figure 9: Advice to optimize the own ship's signature.

 http://doi.org/10.24868/issn.2515-818X.2018.027

Below the header ‘Threat List’, all threats that are expected are shown (see Figure 10). It also shows with color-coding the own ship’s susceptibility towards the individual threats. Selecting a threat (line turns blue) will show on the tactical display the detection ranges (or safe depth areas in case of mines, see Figure 11) of this threat. When selecting multiple threats, the worst case situation is shown. Below the header ‘Environment’, the environmental parameters are listed on which the models base their outcome.

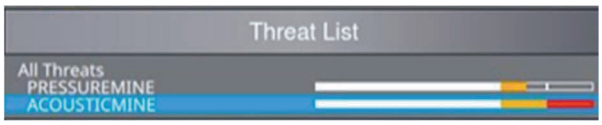


Figure 10: Threat list.

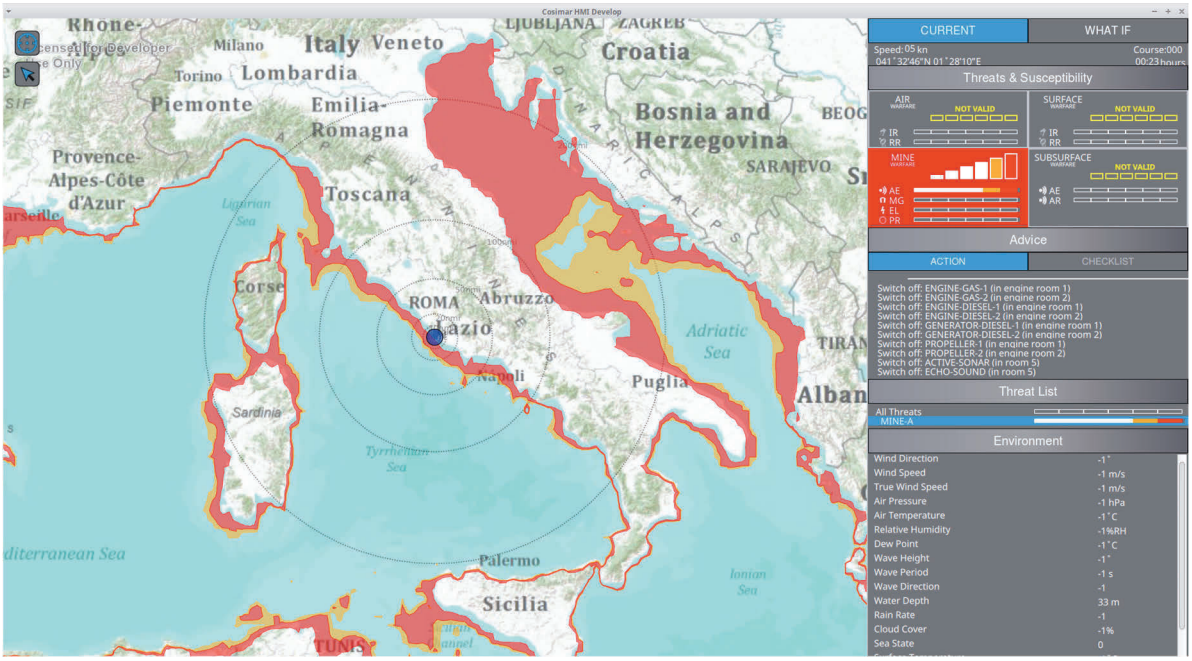


Figure 11: When a threat is selected (in this case an acoustic mine), the unsafe areas are shown.

In case of planning, the operator is interested in a future situation. This can either be different weather conditions later that day, the impact of increasing speed or the signatures along some route the ship sails. These questions can be answered using the what-if mode. In this mode all these parameters can be changed for a number of waypoints along a planned route. This is shown in Figure 12.

The colours of the waypoints correspond to the susceptibility colours similar to the ones in Figure 8. A grey waypoint indicates that the susceptibility is not computed yet, while a closed waypoint is the waypoint as selected by the operator.

 http://doi.org/10.24868/issn.2515-818X.2018.027

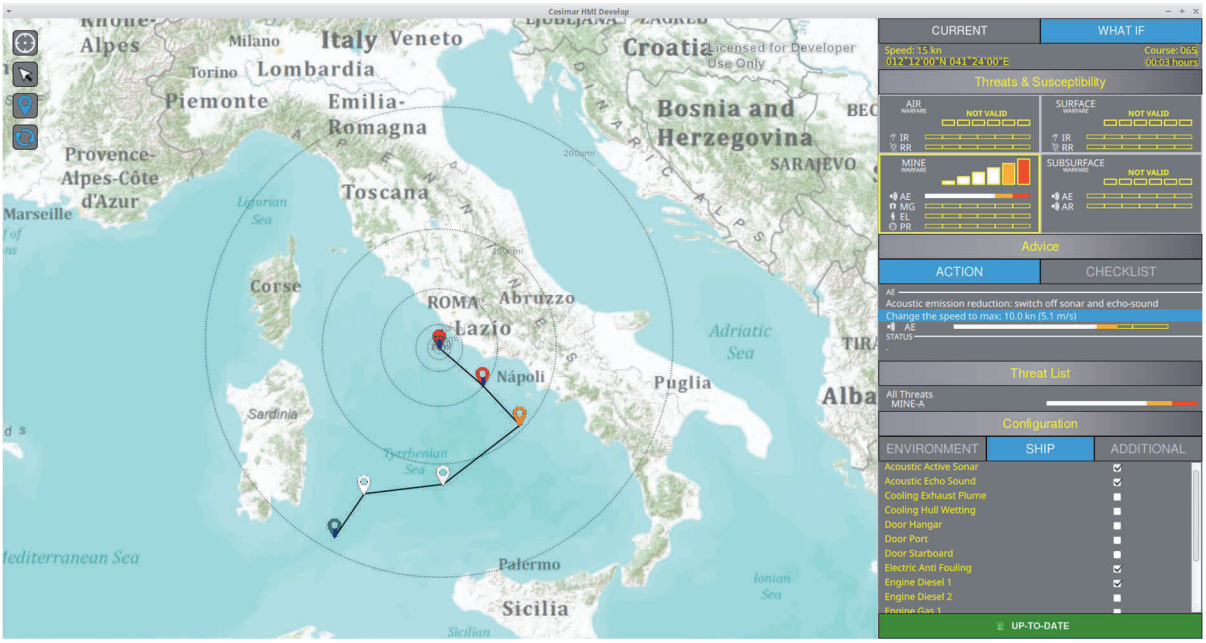


Figure 12: The What-If Mode of the COSIMAR HMI. A sailing route can be planned and the related predicted signatures can be computed.

4.2. Technical HMI

Asset-health-monitoring consists of monitoring the proper functioning of the own ship's assets by comparing the readouts of the signature sensors with 'normal' operating values. When the measured values deviate too much from the normal values this is an indication of a malfunctioning asset or another hardware-related problem that must be brought to the attention of both the operational and the technical personnel. For this the sensor monitoring module SENSE (Sensor Error Notification System) is developed (see Figure 13). SENSE is intended to be used by the technical crew and provides means to dig deep into the technical system to find the cause of the deviation to the normal operating values.

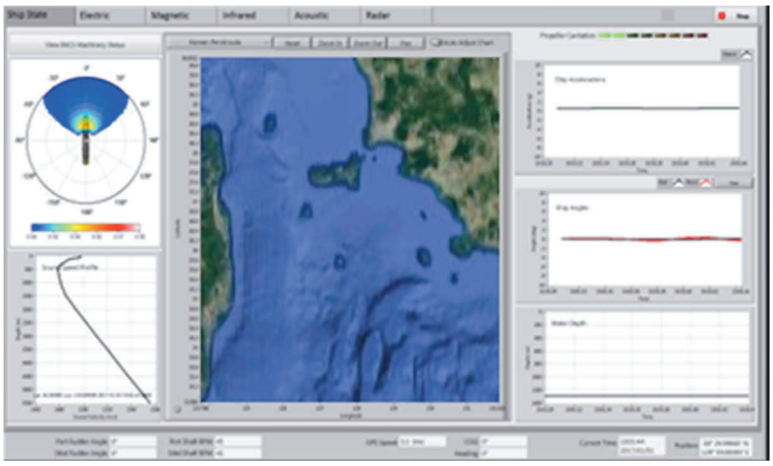


Figure 13: The signature sensor monitoring module SENSE.

5. Conclusions

In this paper, the COSIMAR ship signature management demonstrator is described. The COSIMAR demonstrator is developed in an international cooperation between Canada, Germany, Norway, Belgium and The Netherlands under the umbrella of CSSM. The COSIMAR demonstrator is built using a system-of-systems approach with signature models written in different programming languages, running on different operating systems and having a variety of technology readiness levels. The human machine interface was developed in several interactive sessions with end-users and was evaluated with end-users. The final demonstration with

 http://doi.org/10.24868/issn.2515-818X.2018.027

participation of all international partners took place in Ottawa, Canada. COSIMAR demonstrated the functionality of a ship signature management system that: 1) informs the crew about the own ship's current signature-related susceptibility given the current threat situation; 2) Advises the crew which measures to take to improve the own ship's current signature-related susceptibility given the current threat situation; 3) Enables the crew to investigate alternative solutions to improve the own ship's susceptibilities at alternative locations and/or under alternative environmental condition and/or alternative threats by adapting the ship configuration and/or course; 4) Alerts the crew on abnormal deviations of the own ship signatures and/or signature sensors.

In order to be able to introduce operational Ship Signature Management Systems on-board of navy ships, the following steps need to be taken: The physical models used for signature and propagation calculation need to be validated, an overall accuracy assessment needs to be done. The integration of a Ship Signature Management System with other systems and procedures on-board needs to be investigated. In this context the peculiarities of different ship types such as frigates, submarines or mine countermeasure vessels need to be taken into account. From an organisational point of view, the supply with up-to-date threat sensor data and models needs to be ensured. The CSSM partner nations are presently preparing further cooperative projects in order to support the technical way ahead to provide operational Ship Signature Management Systems to our navies.

6. Acknowledgements

The authors would like to thank DMO, DRDC, FFI, MARIN, FRAUNHOFER IOSB, MULLER BBM, NAVAL PROJECTS, TNO and CSSM and all who contributed to the COSIMAR demonstrator.

7. References

[1] Fehr M., Hasenpflug H., Rhebergen J.B.: 'An operational ship signature management system, OSSMS', Proceedings of the International Naval Engineering Conference 2014, Amsterdam, The Netherlands, May 20-22 2014.

8. Sources of figures

Figure 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12: TNO
Figure 6, 13: DRDC

9. Authors' Biographies

Johan Janssen earned an MSc in Electrical Engineering in 1993, and a PhD in Computer Engineering in 2001, from the Delft University of Technology. In 1998, he joined TNO in The Hague. Currently he coordinates TNO's research programmes and projects related to manning and automation for naval ships including ship signature management.

Hans Hasenpflug has a background in aircraft technology. In 1984 he started to work for the Dutch Ministry of Defense at the department of naval architecture on the topic of underwater ship acoustics. For the last 10 years he has been working as Dutch National Coordinator in the German-Netherlands Centre for Ship Signature Management. During this period, he was involved in several national and international research and technology projects in the field of signature management.

Michael Janßen received a degree in electrical engineering at the University of German Armed Forces in Munich in 1983. Since 1998 he is working at the Bundeswehr Technical Centre for Ships and Naval Weapons, Maritime Research and Technology, today as head of its department Signaturemanagement. He is the German National Coordinator in the Centre for Ship Signature Management.

 http://doi.org/10.24868/issn.2515-818X.2018.027