DeAIS project: Detection of AIS Spoofing and Resulting Risks

Cyril RAY
Naval Academy Research Institute (IRENav)
Brest, France
cyril.ray@ecole-navale.fr

Clément IPHAR, Aldo NAPOLI
MINES ParisTech, CRC
Sophia Antipolis, France
{clement.iphar, aldo.napoli}@mines-paristech.fr

Romain GALLEN
CEREMA
France
romain.gallen@developpement-durable.gouv.fr

Alain BOUJU
L3i-La Rochelle University
Brest, France
alain.bouju@univ-lr.fr

***Abstract* — Crossroads of international issues, maritime domain is facing growing human activities (fishing, transportation, boating…) involving a large spectrum of ships from small sailing boats to super tankers. This increase of maritime mobilities has favored the appearance and generalization of position report systems for keeping track of ships movements. Amongst these systems, cooperative position reports using devices such as the Automatic Identification System (AIS) have been widely deployed and used. Recent works have shown that falsification of AIS messages is possible, and therefore could mask or favor illegal actions, lead to disturbance of monitoring systems and new maritime risks. This paper presents these new threats and risks and introduces a novel methodological approach for modelling, analyzing and detecting such maritime events.**

Keywords—Automatic Identification System (AIS), maritime risks, data mining

I. INTRODUCTION

The maritime environment has a huge impact on the world economy and our everyday lives. Beyond being a space where numerous marine species live, the sea is also a place where human activities (sailing, cruising, fishing, goods transportation...) evolve and increase drastically [2]. This ever increasing traffic leads to navigation difficulties and risks in coastal and crowded areas where numerous ships exhibit different movement objectives which can be conflicting (e.g. sailing vs. fishing). The disasters and damages caused in the event of sea collisions can pose serious threats to the environment and human lives. The sea surveillance has therefore become a major concern. Many government authorities have set up strategies to prevent these sea tragedies but also to protect the principle of free movement, control of people's rights and territorial integrity. These last objectives imply a need to "provide an answer" to illegal immigration, drug smuggling, and terrorism.

From this dynamic emerges the will to develop sea surveillance systems including ways to improve maritime security and identify illegal or suspicious ships behaviors. The consideration of this control issue by the International Maritime Organization (IMO) has partly evolved in the last decade from education and navigational rules (e.g. International Regulations for Preventing Collisions at Sea: COLREGS) to technical answers for traffic monitoring. The IMO has thereby defined the e-navigation concept, based on the harmonization of marine navigation systems with the collection, integration, exchange, presentation and analysis of maritime information onboard and ashore by electronic means [3].

The understanding of a maritime situation and/or vessels intentions comes through an analysis of ships localizations. Such an analysis can rely on short and/or long-term data records. Short-term is related to the identification of instantaneous comportment (for example an intrusion in a restricted area) and long-term is related to the analysis of trajectories with the identification of specific behaviors (for example having forbidden or dangerous manoeuvres). Nowadays, ships are fitted out with almost real-time position report systems whose objective is to identify and locate vessels at distance (Automatic Identification System (AIS) for example). The AIS completes the radar pictures in order to provide a declarative and a real-time situation to ships. It provides data to land services such as harbour authorities and Vessel Traffic Services (VTS) in charge of traffic surveillance but they also feed on-line providers (e.g. Marine Traffic) with high frequency position reports. Combined with radar surveillance and others, real-time localization of ships in coastal area (around 40 miles) is effective though given the wider range of AIS (as compared with radar), the maritime situation beyond radar range solely depends on AIS messages received. Also, there exist some recent VTS centers that depend totally on AIS technology when they are not equipped with radar.

978-1-4799-8736-8/15/$31.00 ©2015 IEEE

This research belongs to a French National Research Agency (ANR) project which started in November 2014. The following presents new threats and risks raised by falsification and hacking of the AIS and introduces our methodological approach for modelling, analyzing and detecting these new maritime risks. Section II describes possible failures of the AIS at the physical, communication, logical levels and proposes a classification of related risks and threats raised by attacks. Section III sketches risk modeling principles and introduces real-time message-based data mining methodology proposed to identify abnormal messages and navigational behaviors. Section IV gives some conclusions and current perspectives.

II. Risks and Threats

There are several definitions of risk, which usually give a dual meaning to this concept. The risk includes both the potential losses (vulnerability) and the probability of a hazardous event [18].

In order to improve the management of these risks at sea, the maritime surveillance system must reach an improved analysis of the behaviors of ships, along with an integrated surveillance system. Much research is still ongoing in the field of Maritime Domain Awareness (MDA), which is defined as the constant perception of maritime environmental elements with respect to time and space, the comprehension of their meaning and the projection of their status after some variable has changed [19]. Thus new axes for reflection should be addressed, in order to improve the process of risk detection.

The International Maritime Organization has defined the MDA as the understanding of all information and activities associated with the marine environment, which may have an impact on security, safety, economy or environment [9]. However, the spoofing of the AIS system (onboard or not) leads to new risks at sea. Those risks are about the vessel itself, the surrounding vessels, the environment, offshore and coastal infrastructures, organizations and finally societies. This underlines the urgent need for the development of large-scale monitoring systems managing the problem beyond MDA principles through the understanding of maritime situation but also through the understanding of technical means providing this maritime situation.

A. *Vulnerabilities of the AIS system at sea, at radiocommunication level and ashore*

1) A lack of control of AIS installations

The installation of AIS transponders on ships, their initial configuration and the permanent information (such as MMSI, name, length, position on the ship, *etc.*) embedded in the transponders are made by certified installers in order to provide a standardized exploitation such as described by IMO (IMO Res.917(22) and IMO Res.956(23, 2004)).

Nonetheless, the data send by transponders, onboard ships or ashore, are not subject to any kind of control. The IMO recalls users and installers that it is their responsibility to make sure that data sent are exact and conform to existing standards, but a shutdown, a bad or a lack of declaration regarding the current status of the ship (specifically voyage related data), a wrong installation (position, power, connection to sensors) or a wrong configuration of the transponder (frequency, type of messages sent) may have an impact on the mutual detection of ships resulting in absence of detection or low detection rate, bad handling of the risk of collision, false alarms and also have an impact on the detection of abnormal behaviour by maritime surveillance systems.

2) Vulnerabilities of embedded AIS transponders

It is clearly stated in IMO Res. 917(22) that only static information was supposed to be saved in the transponder when it is installed and connected onboard. Nonetheless, it is still possible to modify them afterwards through simple means and these pieces of information might be made irrelevant if not correctly updated when some changes in the life of the vessel occur (change of name, change of position of the transponder).

Other data such as voyage related or dynamic information are not controlled by any means though it is strongly recommended that users should check their correctness and check the right configuration and installation of the transponder on a regular basis. It is a common case that ships travelling from one departure point to another have voyage related information that is not updated.

Regarding the use of AIS onboard ships, IMO warns the users and recalls that AIS is a complementary resource of localization of neighbouring ships after the primary resource which is the radar. Nonetheless, given that the radar range is often shorter than AIS range and that the radar is far more sensitive to environmental perturbations (atmospheric conditions, sea state, size and distance from other ships), the AIS is often the only way to identify and localize ships or AtoNs in the far. A ship may currently modify its trajectory (heading, speed, rate of turn) based on AIS data that cannot be confirmed by other sources of information.

3) Vulnerabilities of earthland systems

Numerous services ashore are based on the permanent provision of AIS data received by shore stations. These services may be navigation assistance systems, maritime assistance systems or traffic organization systems that are provided by coastal states or private bodies such as harbours (including traffic surveillance, provision of AtoN and maritime safety information, provision of differential positioning information). Other services such as fleet tracking, logistics also rely on AIS data in order to work properly.

Neither control nor mandatory regulations are imposed on the installers of such shore systems (AIS base stations, receivers, AtoN transponders). The responsibility of the correct installation, connection and configuration of these devices rely solely on the technical units in charge of these operations. There is nowadays no means provided under recommendation of the IMO or of the international organizations in charge of the standardization that enables *a posteriori* checking of the good operational and technical behaviour of these AIS services.

It is therefore possible to envision that AtoN information provided by AIS means or other information provided by the

network of base stations may be erroneous (false positioning of AtoNs, changes in the nominal emission rate of AIS messages, erroneous differential positioning information).

4) Vulnerabilities at radiocommunication level

The AIS technology is based on VHF frequency used also in current VHF voice communications. Though the channels used for AIS are not a standard accessible communication channel for VHF voice devices onboard and onshore, shore and embedded VHF radios can have access to the same channels (but their configuration specifically regarding the numbering of the maritime radio channels differ due to the bandwidth of the different channels and their capacity to hold full duplex, half duplex or single channel communications). The use of radios allowing to have access to the AIS channels through manual tuning may cause radio interferences on these frequencies. Such an emitter tuned on AIS frequencies may impair the capacity of neighbouring receivers to receive distant AIS messages and it may also impair the capacity of a close transmitter of broadcasting its messages by masking it to all distant receivers.

A similar problem could also occur on-board or in coastal radio stations because of the proximity of numerous radiocommunication devices dedicated to AIS, VHF voice communications or VHF digital communications such as Digital Selective Call (DSC). Though not tuned on AIS frequencies, the closeness and difference in power of adjacent VHF devices may cause interferences and mask received messages as well as broadcasted messages from the AIS transponder or base station. This interchannel interference could either totally block emitted or received messages or it may be a less sensitive but still active phenomenon by limiting the range of received or emitted messages.

Other means to attack the AIS system in itself consist in targeting the channels used to exchange messages. If this is not done by radio interference, this can be done by overloading these channels with meaningless messages. This could cause all ships to drastically lower the range of received messages (a technical security measure automatically implemented on AIS transponders). This may also have side consequences and block the access to AIS slots for all AIS devices working in CSTDMA mode (carrier sense time division multiple access is a mode only used by class B ships and AtoNs that will cause them to emit in a given slot of time provided no one is already emitting at the same time).

Wrong messages or radio interferences are also susceptible to block the good sending and reception of valid AIS messages. More efficient ways do exist that can be put into action at radiocommunication level in order to disturb AIS communications.

The easiest way to input wrong information in ships and shore systems is to simply emit an AIS message that conforms to all standards and formats but that contains erroneous information (wrong identification, positioning, dynamic and voyage related information, wrong assignments, etc.). The consequences and the main attacks are described in detail below in part B. These attacks are probably among the riskiest ones since they are easy to do, difficult to detect and may be focused on maximum and direct nuisance to the safety and security of targeted ships or to all ships in a given region.

B. Potential threats to security and safety of navigation

Beyond irregular behaviors at sea, malfeasance mechanisms and bad navigation practices have inevitably emerged recently to circumvent, alter or exploit such surveillance systems in the interests of offenders.

By exploiting the vulnerabilities presented earlier, some of which are easier to put in place than others for an identical threat, an attacker may generate numerous issues. The threats may either affect individual ships or put multiple ships simultaneously in hazardous situations. These actions could impact the ships themselves, the people onboard and the cargo by lessening their security level or by exposing them to immediate dangers. Some threats could have an incidence on the surveillance capacity of VTS centres and harbours, but they could also affect the assignment, positioning and use of maritime or terrestrial search and rescue resources or the use of other resources dedicated to the security of the territory, the customs or to military operations.

Not only the consequences of the implementation of such threats might strike the primary stakeholders targeted but the consequences, thus the risks, could be far much worse and affect much wider fields such as the environment at large scale, whole regions and their people, the global trading and economy.

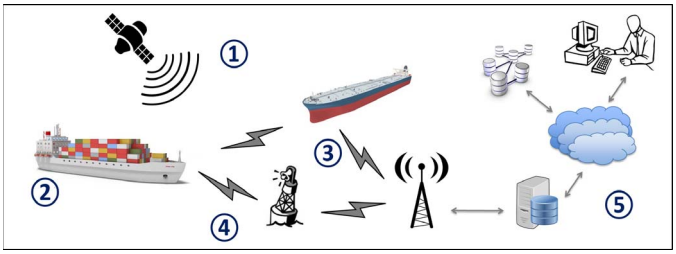

Fig 1. Threats and risks at different levels

Recent experiments have demonstrated some of the vulnerabilities of the AIS [1]. In this work, Balduzzi *et al.* propose an overview of AIS threats and classify them as software and radio attacks. He identifies: ship spoofing, AtoN spoofing, collision spoofing, AIS-SART spoofing, weather forecasting, AIS hijacking and availability disruption threats. Actually the attacks and malfeasance should be considered as possible at each step of the system (Figure 1).

For instance, it is easy to spoof a ship identity by issuing the IMO or MMSI (Maritime Mobile Service Identity) number from another ship. Some fishing boats are practicing this offense in order to fish illegally for example by pretending to be a yacht. It is difficult to detect their illegal fishing at distance. Some captains also switch off their AIS to disappear from monitoring centres screens and electronic chart display and information systems (ECDIS) of neighbouring ships. These acts are committed consciously by people on board (Fig. 1, location 2).

Furthermore, ships can be hijacked without the knowledge of their crew or surveillance centres by injecting false differential GPS information. It is possible to affect on-board GPS position in order to divert it from its original way (Fig. 1, location 1). In that case, the captain thinks he follows a wrong cape and manoeuvres the vessel in order to bring it back to the right cape. But the captain actually diverts his own vessel unbeknownst to him. What would be, in that case, the faced risks? The vessel can be guided towards a dangerous navigation area, such as a reef zone. The vessel could then run aground. If we imagine the case of a super tanker, its grounding would be followed by an oil slick, and a disaster for the environment. The vessel could be guided towards an area of dense traffic, such as a TSS, increasing the risk of boarding with another vessel. A cape towards an area where containers are drifting (e.g. in February 2013, a storm caused the loss of 500 containers in the North Sea) would make a collision with a container and damages to the vessel unavoidable.

AIS devices and navigational aids (AtoN) can also be reconfigured at distance (Fig. 1, location 4). The generation of virtual (and false) AtoN or the hacking of their remote maintenance parameters can have dramatic consequences on navigation. One can imagine risks raised for instance by the extinction of a lighthouse at distance during the night.

Other experiments have also demonstrated that it is also possible to generate false alerts at sea, forcing organizations in charge of maritime rescue such as MRCCs to take charge of these alerts and to bring help to the virtual vessel from which the false distress signal comes from (Fig. 2, location 3). This rallying of means uselessly endangers rescuing crews and the mobilized resources cannot be used for a real accident.

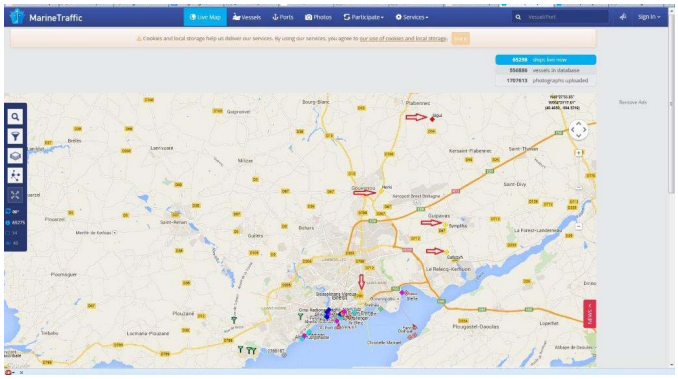

Fig 2. Five false positions (red arrows) in Brest bay injected in MarineTraffic.

At the beginning AIS was mainly used through VHF in order to provide a local situation to ships at sea. With the wide diffusion of AIS technology to all classes of vessels and the ability to access to the Internet in the vicinity of the coast, more and more people, at sea or ashore, use an Internet online AIS provider such as Marine Traffic (marinetraffic.com), AIS Hub (aishub.net), Vessel Finder (vesselfinder.com). These providers could be sensible to many Internet threats like denial-of-service (DoS), virus attack or SQL Injection (Fig. 1, location 5). As these providers (even state ones) are mostly broadcasting positioning information without an accurate analysis of received messages they might broadcast false position reports (Fig. 1, location 3) to their end-users as illustrated by Figure 2.

As a summary, the AIS's system, its implementation and the protocol specification as well as the whole chain of data transmission can be affected by many threats, offering multiple attack possibilities. We propose to use long term analysis of messages and ships' trajectories with the identification of specific behaviors in order to identify abnormalities in AIS messages.

III. METHODOLOGY AND ARTCHITECTURE

This section introduces the proposed methodological approach for modelling, analyzing and detecting maritime threats possibly caused by the AIS.

A. Modelling risks

In order to recognize and detect the risks it is necessary to first model risk scenario. Knowledge on risks is dragged from interviews of maritime domain experts and reviews of the literature.

Risks will be modeled with ontologies. An ontology can be defined as being "a formal and explicit specification of a shared conceptualization." [5, 17]. This definition highlights four particularly important notions in the ontology area:

- Formal: means that the conceptualization and the representation of the domain must be standardized and used by a computer hardware;
- Description: specifies that both concepts and constraints used are defined in a declarative way ;
- Conceptualization: underlines the fact that an ontology is only an abstraction of the real world and that the terms used and the relationships between them shall be described without ambiguity ;
- Community: implies that ontologies promote a consensual knowledge for a community of agents.

In order to understand the behavior of a vessel and to check that information it delivers is reliable, its sole location is not sufficient. Indeed, this behavior can be analyzed through a great amount of pieces of information (meteorological conditions, surrounding vessels, *etc*….) which must be taken into account. It is here that lies the concept of semantic behavior. At each location is attached a number of pieces of information that are judged relevant enough, and which will then be used during the risky behavior detection process. The creation of a semantic representation of trajectories, and consequently a representation of behaviors, requires the enhancement of the locations of vessels by several contextual pieces of information [6]. In order to do that, three main ontologies were created, basing on the model previously developed by Yan [7, 8]:

- A trajectory ontology including various spatiotemporal concepts, necessary for a geometric definition of trajectories.
- A geographic ontology including the concepts specific to territory description (roads, harbors, bays, *etc*….).

- A domain ontology which is, as its name stands for, relative to the studied domain.

Our analysis of risks will be based on a four-step method, shared by several possible risks [4]:

- 1st step: **technical and functional analysis of the system.** Its goal is to understand the studied system through its components and the search of the understanding of its purposes. It is a model of the studied system ;
- 2nd step: **the qualitative analysis.** Beyond the simple identification of threats (search and identification of threat sources), its purpose is the study of threats processes, i.e. the research of feared events or of breakdowns, as well as the reasons for the threat sources to trigger themselves and the potential consequences of feared events ;
- 3rd step: **the quantitative analysis.** It enables us to measure, to weight, in terms of occurrence probability and seriousness of consequences, the feared events or the system breakdowns previously analyzed. The eventual purpose of this step is the organization into a hierarchy of feared events or of system breakdowns ;
- 4th step: **the synthesis.** It enables the highlighting of breakdowns and their combination use. The objective is to ascertain the most critical components and thus to propose the technical improvements likely to master them.

B. Towards real-time detection

Monitoring of coastal maritime areas for various purposes like safety and security, traffic management or protection of strategic areas, has been largely based on the identification of positions and trajectories and abnormal behavior detection [10]. This kind of detection is based on (1) the long-term and large-scale integration of positions from maritime traffic continuously and, (2) spatio-temporal analysis able to determine and classify a given maritime situation. This analysis requires the identification and classification of navigational behaviors, techniques of falsification of position reporting systems and knowledge extraction methods to detect abnormal maritime situations.

This detection can rely on a rule-based engine approach allowing to formalise rules and to ensure the link between the conceptual specification of a situation and its implementation [6, 12, 13]. Several studies addressed spatial ontologies to describe maritime traffic and identify dangerous and/or suspicious behaviors [14, 6]. Related to these behaviors, researchers have proposed solutions for anomaly detection from supervised approaches. They used sets of recorded trajectories and situations to define a panel of typical abnormal behaviors from statistical analysis [10, 15, 16].

Nevertheless, situation awareness in these works is mainly concerned with navigation mobilities. An information system designed for detection of AIS spoofing should provide a wider spectrum of analysis. The proposed approach relies on a simple postulate: an attack or a falsification of the AIS has consequences on received messages.

An AIS device can broadcast up to 27 different messages in a range of approximately 35 nautical miles. Data exchanged include in particular static information (vessel name, dimensions, etc.) and dynamic information (heading, speed, GPS position, etc.). Positioning information is transmitted at high frequency (2-12 seconds for a moving ship, 3 min for an anchored vessel). The system transmits on less regular basis meta-information related to the ship (international identifier, name, size) and its route (destination, date and time of arrival). Additionally the system broadcasts some control messages (e.g. management of channels and transceiver modes by a base station is done by a message 22) and aids to navigation messages.

In order to detect when an AIS device is falsified or is undergoing an attack through a message-based analysis, real-time AIS information should be analysed online and compared to historical, expected or predicted information [11]. This approach entails a challenging combination of the cartographic and risk context, position reports from ships and behavioral analysis and context-based analysis of AIS messages. The processing architecture currently designed relies on a hybrid spatio-temporal database system combining online and offline processing (on-going work). Messages are processed on the fly, specific message patterns or spatio-temporal behaviors are mined according to the maritime context. At the same time, messages are stored in the historical database where data are aggregated and summarized in order to feed on-line processing and analysis with a historical maritime context.

IV. CONCLUSION

This paper introduces issues emerging from falsification of AIS messages. Risks and threats have been exposed and a methodological approach for modelling, analyzing and detecting these new maritime risks is presented. The objective of this research is to detect when a ship's AIS system or a maritime surveillance system is undergoing an attack through real-time message-based analysis and data mining.

ACKNOWLEDGMENTS

Research presented in this paper is supported by *The French National Research Agency* (ANR) under reference ANR-14-CE28-0028. The project is also labelled by French clusters Pôle Mer Bretagne Atlantique and Pôle Mer Méditerranée and co-funded by DGA.

REFERENCES

[1] M. Balduzzi, A. Pasta, K. Wilhoit, "A Security Evaluation of AIS, Automated Identification System", The 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, Louisiana, USA, December 8-12, 2014

[2] UNCTAB.: Review of maritime transport.Report, United Nations Conference on Trade and Development (UNCTAD), UNCTAD/RMT/2011,UN publication, 2011

[3] IMO.: Strategy for the development and implementation of e-navigation. In: Report of the maritime safety committee on its eighty-fifth session, annexe 20. International maritime organisation documentation, 2008

[4] Dassens, Launay. Etude systémique de l'analyse de risques – présentation d'une approche globale, *Techniques de l'ingénieur*, 2008

[5] Studer, Benjamins, Fensel. Knowledge engineering: Principles and methods. *Data & Knowledge Engineering*, Vol 25, pp. 161-197, 1998

[6] A. Vandecasteele, A. Napoli. Using Spatial Ontologies for Detecting Abnormal Maritime Behaviour. *In Proc Of OCEANS 2012*, 2012

[7] Z. Yan. Towards Semantic Trajectory Data Analysis: A Conceptual and Computational Approach, *in PhD Workshop, VLDB*, Lyon, France, p. 3, 2009

[8] Z. Yan. Semantic Trajectories: Computing and Understanding Mobility Data, Doctoral thesis, 2011

[9] IMO. Amendments to the International Aeronautical and Maritime Search and Resacue (IAMSAR) Manual, 2013

[10] T. Devogele, L. Etienne, C. Ray, *Mobility Data: Modelling, Management, and Understanding*, Part 3, Chapter 11 : Maritime monitoring, pages 224-243, Chiara Renso, Stefano Spaccapietra, Esteban Zimanyi (eds), Cambridge University Press, 2013

[11] L. Salmon, C. Ray, C. Claramunt, Une approche holistique combinant flux temps-réel et données archivées pour la gestion et le traitement d'objets mobiles, *30ième Journées Bases de Données Avancées (BDA 2014)*, 2 pages, 2014

[12] B. Idiri, A. Napoli. The automatic identification system of maritime accident risk using rule-based reasoning. *In Proc.of the 7th International Conference on System Of Systems Engineering - IEEE SOSE*, pp. 125-130, 2012

[13] M. Morel, S. Claisse. Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behaviour detection & Collaborative identification of threat (I2C). *In Proc. of the Ocean and Coastal Observation: sensors and observing systems, numerical models and information systems*, Brest, France, 2010

[14] J. Roy. Anomaly detection in the maritime domain. In: Theodore T. Saito, T.T., Craig, S.H., Daniel, L. (eds.) SPIE 6945, *Optics and Photonics in Global Homeland Security IV*, 69450W, Conference Vo. 6945, 2008

[15] C. Brax. Anomaly detection in the surveillance domain. Doctoral thesis, Örebro University, School of Science and Technology, 2011

[16] M. Riveiro, G. Falkman, T. Ziemke. Improving, maritime anomaly detection and situation awareness through interactive visualization. *In: 11th International Conference on information Fusion*, pp. 1-8, IEEE Press, New York, 2008

[17] A. Vandecasteele, A. Napoli. An Enhanced Spatial Reasoning Ontology for Maritime Anomaly Detection. *7th International Conference on System Of Systems Engineering – IEEE SOSE*, pp. 247-252, Genoa, Italy, 2012

[18] B. Dufour, R. Pouillot. Approche qualitative du risque. *Épidémiologie et Santé Animale*, 41: 35-43, 2002

[19] M. Glandrup, Improving Situation Awareness in the Maritime Domain, *in Situation Awareness with Systems of Systems*, P. van de Laar, J. Tretmans, and M. Borth (Eds), Springer, 2013