An expert-based method for the risk assessment of anomalous maritime transportation data

Clément Iphar, Aldo Napoli, Cyril Ray

Version of Record: https://www.sciencedirect.com/science/article/pii/S0141118720304314
Manuscript_02bbfff3e38f605ea88e38518c3e4b9e

An expert-based method for the risk assessment of anomalous maritime transportation data

Clément Iphar

MINES ParisTech - PSL Research University - Centre for research on Risks and Crises (CRC), F-06904 Sophia Antipolis, France

Aldo Napoli

MINES ParisTech - PSL Research University - Centre for research on Risks and Crises (CRC), F-06904 Sophia Antipolis, France

Cyril Ray

Arts et Metiers Institute of Technology, Ecole Navale, IRENav, F-29240 Brest, France

Abstract

Risks in maritime navigation linked to cyberthreats emerge, and they must be assessed together with the more traditional risks such as grounding or colliding another vessel, as now the latter might be the consequence of a cyberattack. The fields of mobility and transportation data see vulnerabilities of navigation systems jeopardising their normal use, and putting both users and their environment at risk. In this article, we propose a method based on expert knowledge for the risk assessment of cyberthreats in maritime transportation data. A specific focus is proposed on the AIS (Automatic Identification System), a world-wide message-based vessel localisation system that has demonstrated weaknesses allowing errors, falsification and spoofing of its transmitted data. The discovery of abnormal reporting cases is assessed by an expert-designed rule-based analysis frame resulting in the triggering of alerts and the assignment of risk levels, tailored to increase the awareness of the people in charge of monitoring the maritime traffic.

Keywords: Maritime risk assessment, AIS data falsification, traffic safety

*Corresponding author: Clément Iphar. Phone: +39 0187 527 391. Viale San Bartolomeo, 400; 19124 La Spezia, Italy

Email addresses: clement.iphar@mines-paristech.fr (Clément Iphar), aldo.napoli@mines-paristech.fr (Aldo Napoli), cyril.ray@ecole-navale.fr (Cyril Ray)

1. Introduction

The recent years have seen the rise of cybersystems, which are involved in an increasing part of our lifes. Since every system has vulnerabilities of its own, their development creates the need for the conception of means aiming at protecting those systems and being able to respond to an attack, as well as assessing the potential issues resulting from a variety of attacks. A cyberattack usually consists in the access, the change, the diffusion or the destruction of potentially sensitive information [1]. Money extortion, intelligence or the interruption of usual business processes are usually the main reasons for cyberattacks, although in some cases the attribution of the attacks is not clear [2], despite its importance in implementing further security layers. Such malicious acts can be motivated ideologically [3], and it is difficult to measure the extent to which cyberattacks occur as firms tend to under-report such attacks, and only make it public when stakeholders such as investors or the general public already suspect with a high likelihood its existence [4]. The attacks can target critical infrastructures of countries [5] or the daily life of citizens with cyberthreats existing in areas as various as domotics [6] or street furniture [7].

Intelligent transportation systems (ITS), related data and information, as well as the means of transport themselves are affected by this emerging trend. Issues about cyberattacks have been identified and studied for cars [8], airplanes [9] and vessels [10]. These issues typically concern the degrading or crashing of systems and services, spoofing, stealing data but also more malicious and sophisticated attacks with fake-sensed data.

With the multiplication of low-cost sensors, surveillance systems are on a rise, particularly collaborative systems that require little equipment. Cooperative data related to mobility witnessed a recent rise in several fields such as pedestrians, goods transportation, cars, vessels or airplanes. These data are subject to anomalies, misuses and falsification, and anomaly detection methods can in this respect be used in order to assess these data. Data streams from sensors have various qualities, and the assessment of this data quality with respect to the nature of the sensor is necessary in order to construct analysis frames that take into consideration all available information so that falsification issues and attack issues can be clearly discriminated. Since falsifications and attacks address different issues originating from different sources, it is particularly important to be able to differentiate them as soon as possible so that the relevant methods can be applied for data analysis.

In the maritime ecosystem needs but also perspectives to enhance cybersecurtity have been stated, including for instance for shipping [11]. One emerging concern concerns all information systems relying on these aforementioned collaborative sensors. The Automatic Identification System (AIS) is a legally-enforced system put in place by the International Maritime Organisation. As a large source of data on maritime navigation, this system is widely used for the understanding of the maritime situation. Its high rate of transmission and vast network of receiving antennas allow a large harvest of AIS messages that enable a

precise tracking of vessels both on short and large geographic and temporal scales. However, this system is very weakly secured and therefore is prone to issues and attacks such as erroneous information, data falsification and data spoofing. In spite of those issues, its data is largely used as a basis for maritime-based studies, without seeing its data quality questioned somewhat. In this respect, a data integrity analysis would allow to put into perspective the blind use of AIS information and highlight the main issues that the system face, so that action can be taken to mitigate the risks linked to an improper use of such maritime information and on a larger scale being in grade of assessing the type of issue faced by the system so that an user could take targeted action. Research have demonstrated that AIS is vulnerable, prone to spoofing [12], with missing [13], collided [14], erroneous [15] and falsified [16] messages. Although few cases are reported (for example [17] in East China sea, [18] off Russian coast and [19] in the strait of Hormuz), it has a concrete impact on maritime navigation.

In addition, the expected development of autonomous shipping makes of increasing importance the development of reliable systems that can provide effective countermeasures to navigational issues, physical threats or cyber threats. Indeed, an unmanned vessel fully relies on its sensors and means of communication, either in fully autonomous mode or in remote control. Although it is believed that autonomous shipping is technologically possible [20], the challenges raised are numerous, including the widening of the concept of risk in the maritime navigation [21]. Indeed, besides inevitable regulatory and operational changes in the long run [22], the risk assessment of maritime navigation, and the working policy of companies and of civil authorities in charge of monitoring the maritime domain will change.

As evoked, the AIS is vulnerable, and several studies demonstrated its shortcomings. The misuses of the AIS evolved along the years, in line with its new uses. Those new uses, which were possibly not forecast by the International Maritime Organisation at the time of its initial deployment, create today large amounts of anomalies in transmitted data, over acts of carelessness from the crew, or actual falsifications as the consequence of the ill-will of crew members or pirates. Those anomalies create in return an increase of illegal actions and of possible still emerging risks that are still concealed or little known by authorities in charge of maritime traffic monitoring. Those anomalies also have a direct influence on emerging technologies. For instance, the pirate generation and spoofing of ghost vessel tracks around an autonomous vessel could slow down or stop its course, and force it to compute rerouting options at all time, possibly endangering its safety.

In the scope of rising cybersecurity threats and increasing available data for monitoring the behaviours, anomaly detection and risk analysis methods can help pointing out the cases where data present inaccuracies and assess their possible impact. The detection and the classification of abnormal vessel behaviour is therefore a key task of the maritime situational awareness, in order to assign issues to general case, properly assess their risk level and thus

deploy the adapted countermeasures.

In the domain of anomaly detection of maritime traffic, the use of maritime information coming directly from the vessel offer the larger range of methods, including Bayesian networks in which vessel behaviours are categorised following the statistical-based theory of Bayes [23], hidden Markov Models in which this probabilistic model is used in order to discriminate various vessel routes [24], unsupervised route extraction in which routes are extracted from raw data based on vessel trajectories [25], genetic algorithms [26] or low-likelihood behaviour which is based on the measure of the behaviour expectancy from a vessel [27]. Port state control benefits from the understanding of local incoming traffic and identification of possibly risky vessels [28] and the authorities monitoring maritime traffic benefit from traffic analysis and the understanding of spatial-temporal dynamics [29].

In the domain of risk analysis, a variety of approaches for risk assessment are possible in the maritime domain [30], such as the quantification of uncertainty in maritime transportation [31], the determination of accident probabilities and their consequences [32], the analysis of wintertime condition accidents, the determination of the grounding [33] and maritime accident [34] frequencies, the assessment of the risks linked to wildlife [35], or the proposition of meta-models for the oil spill risk following maritime transportation accidents [36]. Various methods to deal with those issues are found in the literature, including fuzzy approaches for the definition of individual risk factors of vessels [37], Bayesian methods for the assessment of piracy risk on offshore platforms [38], or the various methods for ship collision avoidance [39], using probabilities [40], vessel domain modelling [41], traffic cluster flows [42] and spatial distribution of vessels [43] to assess collision risks, both in open seas, in fairways [44], in ports or anchorage areas [45] and within inland waters [46]. Risk mitigation methods can include the use of TSSs (Traffic Separation Schemes) in maritime navigation [35], as well as tools to quantify the effects of risk reduction measures [47]. From the environmental point of view, emissions in ports taking into consideration the local environment [48] and the impact on populations [49].

In general, machine learning techniques are widely used for data analysis [50]. Those techniques include regression, classification, clustering, deep learning, image processing or natural language processing. Since the topic of cybersecurity has few available and usable data for the construction of a model of the training of an algorithm, this field of study is prone to the use of alternative methods that do not require such training datasets. In this work, a base of rules in description logics is used in order to assess data. The approach suits cases where the understanding of the situation must be contextualised in an inference-based system. Description logics, by their nature and their large use in ontology building [51], enable a formal and unambiguous description of expert rules. This base of rules enables a better interpretability and a better understanding of the results with respect to other techniques of machine learning, as it is possible to directly link one rule to an actual natural

language situation. In this paper, bases of rules have been built from message processing to risk level assessment, with the help of several field experts, from industry, academia, and the military.

Risk analysis is used in decision making, as some consider risk analysis as a tool to compute probability and compare them to acceptability criteria, and others use utility functions to codify the value judgement over the scope of possible outcomes and select the action to do by the application of some mathematical optimisation method [52]. Furthermore, such assessments, when prepared and codified, enable the correct communication of the safety status of a vessel in a situation of maritime distress [53], and thus an efficient response. In general, risk assessment in maritime environment relies on risk criteria for workers, passengers and public ashore, the maximum tolerable risk being variable for each group [54]. The question that arises and that this paper addresses is how is it possible to assign a risk level to a vessel, given its nature, its behaviour, its location and the various risks at stake in order to provide the pieces of information to lead the user to an educated choice. This research have been applied to an AIS dataset constituted of messages received by our antenna and parsed by an in-house parser.

The methodological approach presented in this paper allows to assess the integrity of AIS data. This assessment lies on the detection of new forms of anomalies in vessel data. This approach allows (1) the precise detection of data-borne errors and falsifications and (2) to propose corresponding risk scenarios. This data integrity assessment will lead to (1) optimise the analysis of hazardous situations, (2) anticipate new types of threats, (3) select data and methods to be integrated in incoming autonomous systems and (4) reduce the cognitive load of the operators in charge of monitoring the maritime navigation.

In total, we benefited from the input of 6 experts, involved at 4 different steps of the methodology: the item and threshold determination, the risk analysis, the risk indicators and the user requirements. Those experts, 5 from the French Navy and 1 from the Merchant Navy, have either been involved during in-person ad-hoc stays or as part of their involvement within a research laboratory, that included mainly expert knowledge dissemination, and occasionally implementation when the expert had received a specific formation. In addition to those 6 individuals, we received support for the risk analysis from the Cerema (Center for studies and expertise on risks, environment, mobility, and planning), an academia-related governmental body.

In the following of this paper, Section 2 presents the Automatic Identification System (AIS), which represents the most important source of information of sea-going vessels. As our study is based on data from this system, its characteristics and shortcomings are presented. Section 3 presents the proposed methodology for anomaly detection of data in AIS messages from the definition of anomalies in the maritime domain to the seek for those anomalies in the messages, and the definition of falsification scenarios that are in linked with the issues

that AIS messages processing can highlight. Based on this method, Section 4 presents the risk assessment of the AIS system that individuates each message and assesses risk values with respect to various characteristics. Section 5 illustrates, before some concluding remarks, the implementation of this system and the way the risk is displayed to the user in various scenario cases.

2. The Automatic Identification System

The Automatic Identification System is a maritime safety system that enables a large understanding of vessel activities at sea, due to its high message emission frequency, which implies large amounts of data to process. It is therefore largely used and of great value for maritime monitoring applications. This section presents the system from which the data we process for risk assessment comes from, and more particularly its characteristics, its shortcomings and a risk analysis of it that has been performed.

2.1. Broadcast data for the safety of navigation

The Automatic Identification System is a maritime information system for vessels transmitting information about their position, kinematics, physical characteristics, identity and some information related to the safety of navigation. Albeit originally dedicated to maritime collision avoidance, it began to be used for monitoring and surveillance purposes. Currently, mariners use it to be aware of their environment, coastal authorities for knowing the traffic off their coast, countries for being aware of the location of their pavilion vessels, companies for monitoring their fleet and researchers for its existence as a useful tool for the comprehension of maritime traffic and its various consequences.

The Automatic Identification System was put in place by the Safety Of Life At Sea (SOLAS) convention, and some ships from the signatory countries are concerned by the deployment of this system. The SOLAS convention states that all ships of 300 gross tonnage and upwards engaged on international voyages and cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size shall be fitted with an Automatic Identification System [55]. Following this definition, all seagoing vessels are not obliged to carry the AIS, therefore relying only on this system provides a partial view of the maritime traffic. However, it is possible for vessels to carry the system although it is not compulsory for them to do so, on a voluntary basis.

The transmission of AIS is done in the Very High Frequency (VHF) bandwidth, on two worldwide dedicated wavelengths: 161.975 MHz and 162.025 MHz. In order to transmit and receive AIS signals, some dedicated devices have been put in place since the introduction of the system. Four kinds of devices are in use: class A transceivers (on the vessels for which AIS is compulsory), class B transceivers (on the vessels for which AIS is not compulsory), multi-channel receivers and radio scanner receivers.

Initially the system was only terrestrial, with transmissions done from one vessel to another, or between a vessel and a shore station, in a range of distance which is limited by the curvature of the Earth (circa 20 nautical miles in normal conditions and circa 40 nautical miles in optimal conditions for class A vessels [56]), or the transmission power (5 to 10 nautical miles for class B vessels). Recently, the development of low orbit satellites enabled to receive messages even farther from the coast line, as the received messages are uploaded, stored and then downloaded as soon a coast line and a shore station is reached. The development of the Internet allowed an even more important step forward in the maritime situational knowledge as websites display AIS information from all over the world. Consequently, where ships previously disappeared beyond the skyline from a terrestrial point of view, they can now be tracked in the whole world by every person who can access the Internet network.

The rate of transmission, or the reporting interval of AIS message largely varies according to the type of vessel, its speed and the type of message sent and ranges, for a class A vessel, from 2 seconds to 3 minutes for positioning report messages. In one day, the European Maritime Safety Agency (EMSA) receives about 9 million terrestrial AIS and 7 million satellite AIS messages, from over 96,000 vessels detected by more than one source [57] and [58] estimates that in a month, and 130,000 vessels of all categories are sending those messages.

AIS messages have been designed to carry information of various nature, each one carrying a given type of information. In this respect, 27 types of messages have been designed, each one consisting of its own layout of data fields, their nature being in accordance to the type of information it is supposed to carry. In [59] is proposed a separation in six categories of messages which are presented as standard, aid to navigation, timing, safety, binary and other.

The various pieces of information inside AIS messages can be divided into three main categories: static, dynamic and voyage-related [60]. Static data consist of the data fields which are not intended to change, or at least to barely change, such as the call sign, the name of the vessel, its length and beam, or the type of the ship.

Dynamic data consist of the pieces of information contained in the data fields for which a change over time is expected, *i.e.* that display a physical motion such as the course over ground, latitude, longitude, speed over ground. Voyage-related data consist of pieces of information for which a change over time is often expected, *e.g.* at each new voyage, such as the draught, the estimated time of arrival, the destination or the hazardous nature of the cargo.

#	Message name	Emitter	Type	Family
1	Position report (scheduled)	Mobile	Standard	Positioning
2	Position report (assigned scheduled)	Mobile	Standard	Positioning
3	Position report (response to interrogation)	Mobile	Standard	Positioning
4	Base station report	Base	Timing	Positioning
5	Static and voyage related data	Mobile	Standard	Static data
6	Binary addressed message	Mobile/Base	Binary	Communication
7	Binary acknowledgement	Mobile/Base	Binary	Communication
8	Binary broadcast message	Mobile/Base	Binary	Communication
9	Stardard SAR aircraft position report	Mobile	Standard	Other
10	UTC/date inquiry	Mobile/Base	Timing	Communication
11	UTC/date response	Mobile	Timing	Positioning
12	Addressed safety related message	Mobile/Base	Safety	Communication
13	Safety related acknowledgement	Mobile/Base	Safety	Communication
14	Safety related broadcast message	Mobile/Base	Safety	Communication
15	Interrogation	Mobile/Base	Other	Communication
16	Assignment mode command	Base	Other	Communication
17	DGNSS broadcast binary message	Base	Binary	Positioning
18	Standard Class B equipment position report	Mobile	Standard	Positioning
19	Extended Class B equipment position report	Mobile	Standard	Positioning
20	Data link management message	Base	Other	Other
21	Aids-to-navigation report	Mobile/Base	AtoN	Positioning
22	Channel management	Base	Other	Communication
23	Group assignment command	Base	Other	Communication
24	Static data report	Mobile/Base	Standard	Static data
25	Single slot binary message	Mobile/Base	Binary	Communication
26	Multiple slot binary message with Communications state	Mobile/Base	Binary	Communication
27	Position report for long range applications	Mobile	Standard	Positioning

Table 1: All 27 AIS messages with their purpose, the type of station that sends them (a mobile station is a vessel except for message 9, a base station is a shore-based station), the type of communication ("Other" corresponds to channel management or interrogation messages) and the family of messages (dynamic or static data messages, "Communication" corresponds to addressed or broadcast information messages)

2.2. The weaknesses of AIS

The AIS is an open system, and this open system has been conceived and motivated by international authorities so that it could be used by the greatest possible amount of users. However this openness led to the lack of control of the system, and there are several ways in which the AIS fails to transmit genuine data: issues due to the intrinsic weaknesses of the system, errors in the messages, falsified data in the messages [61] and AIS signal spoofing [62]. Those four ways are presented hereafter.

2.2.1. The AIS has intrinsic weaknesses

The intrinsic weaknesses of the system are linked to the system itself, without the implication of human interaction. Missing data and message collision constitute the two main families of those intrinsic issues. The system in itself can fail in the proper transmission of information. Some transponders fail to reach all technical requirements set by the International Telecommunications Union, and large blank areas may be displayed by some vessels.

This missing data, as shown in [13], weakens the exploitation of AIS data as it decreases the reliability, but does not totally prevent this exploitation. In addition to problems such as a limited range and a limited bandwidth, the AIS has some critical shortcomings such as a limited capability of retransmission for a few messages and no such capabilities for the majority [63].

Message collision is another weakness of AIS. A message collision occurs when a message is overlapping another one, partially or completely. All AIS signals are not received by the receivers, as there is a loss percentage, particularly in the case of satellite transmission [64]. When the installation is correct, with a good-level hardware and a good weather, most loss is due to VHF transmission. About 2% of messages are lost due to channel overload [14]. But the biggest reason for message loss is the shadowing due to obstacles [14], either located on board the vessel (local masks), or by other vessels hiding more distant ones.

2.2.2. The system broadcasts errors

The crew manually enters a part of the information contained in AIS messages, both at the first use of the system for permanent data and at every new journey for journey-related data. According to the study of [15], both static and dynamic data are subject to errors, as they both require a human intervention for the filling of some data fields.

Thus, the Maritime Mobile Service Identity (MMSI) number is false in an estimated 2% of the cases [15]. The name of the vessel is another issue, as 0.5% does not have a registered name, and some others exceed the allocated space in the field, which is 20 characters. [65] provides the estimation that worldwide, only 41% of the ships report their destinations.

2.2.3. The system presents falsification cases

Intentional falsification of the AIS signal can be performed by the crews on board the vessels in order to modify or stop the message they send, in the very particular purpose of misleading the outside world.

Identity theft also exists in the maritime domain [65]. It corresponds to the fact to navigate with a MMSI number which is not the allocated and internationally recognised one, but with the one of another vessel that actually exists somewhere else.

Destination masking or disappearance is also sometimes a falsification [65]. As sometimes it can be considered as an error, some other cases are about a voluntary deficiency of information, done in order to sidestep the overview of the global ships flows. Disappearances occur when vessels turn off their AIS transponder in order to hide some of their activities, *e.g.* fishing in an unauthorised area, or trade illegal goods [16] with other vessels or on coasts.

In this respect, five main issues are developed by [65]: the identity fraud, the concealing of destination, the fact to voluntarily stop the broadcast, the GNSS manipulation and the spoofing of the system (as shown hereafter in Section 2.2.4), as the ability of an attacker

to control a vessel under autopilot by spoofing the GNSS signal has been analysed and demonstrated in [12].

2.2.4. The system undergoes spoofing

The spoofing of messages is performed by an external actor under the form of the creation *ex nihilo* of false messages and their broadcast on AIS frequencies [66]. Those spoofing cases are performed in order to mislead both the crews at sea and the outer world, by the creation of ghost vessels, of a false emergency message, a false closest point of approach trigger, or even a false cape. Those manipulations can generate contradictory or downright false information to crews, causing possible confusion and verification measures against other systems, sensors, or the naked eye, and give a false maritime picture to the remote stations in charge of monitoring and analysing the marine traffic.

In the scope of spoofing capabilities, a variety of threats can be taken into consideration: ship spoofing, collision spoofing, aid to navigation spoofing, weather forecasting, availability disruption and AIS hijacking threats [66].

Slot starvation, timing attacks and frequency hopping constitute the availability disruption threats. Slot starvation consists in the fact to impersonate a maritime authority to reserve all the slots (AIS messages are transmitted in communication slots, as described in [67]), and therefore all stations within coverage have no remaining slot available for reservation and emission. In timing attacks, the malicious user orders transceivers to delay their transmission, and by doing it repetitively makes the system normal functioning impossible; and on the contrary, the malicious attacker can order transceivers to send updates at a very high frequency, thus overloading the channel. Frequency hopping consists in the fact to instruct the AIS transceivers to change their transmission frequency *i.e.* the channel of communication, as allowed by the protocol specifications in given areas in the World.

3. A methodology for anomaly detection

Since AIS messages present demonstrated weaknesses in their structure and data, leading to the presence of erroneous and falsified information, the necessity of data processing arises so that the increased maritime risks linked to those shortcomings can be assessed. In this respect, a methodology has been set for the discovery of anomalies in AIS data. The proposed method, based on the structure of AIS data presented in Section 2, uses the integrity as the main data quality dimension for the discovery of non-genuine information, through the assessment of items, each item standing for one particular occurrence in which data may present integrity shortcomings [68]. Then, from the results of those items, a series of flags are computed, each flag representing a particular scenario that might occur as an outcome of the AIS issues. In this section, a broad presentation of maritime domain anomalies is done first, followed by the integrity assessment methodology. Then, several falsification scenarios are

presented, before the presentation of the flag computation based on the thorough analysis of each of the scenarios.

3.1. Anomalies in the maritime domain

Anomalies in the maritime domain are various, their spectrum is wide and performing a classification in families and subfamilies is not trivial [69]. As for the study of AIS messages and in accordance to the research presented in [70] and [71], a classification in four main families has been chosen and presented in Figure 1, namely the behaviour, the content, the lawfulness and the quality.

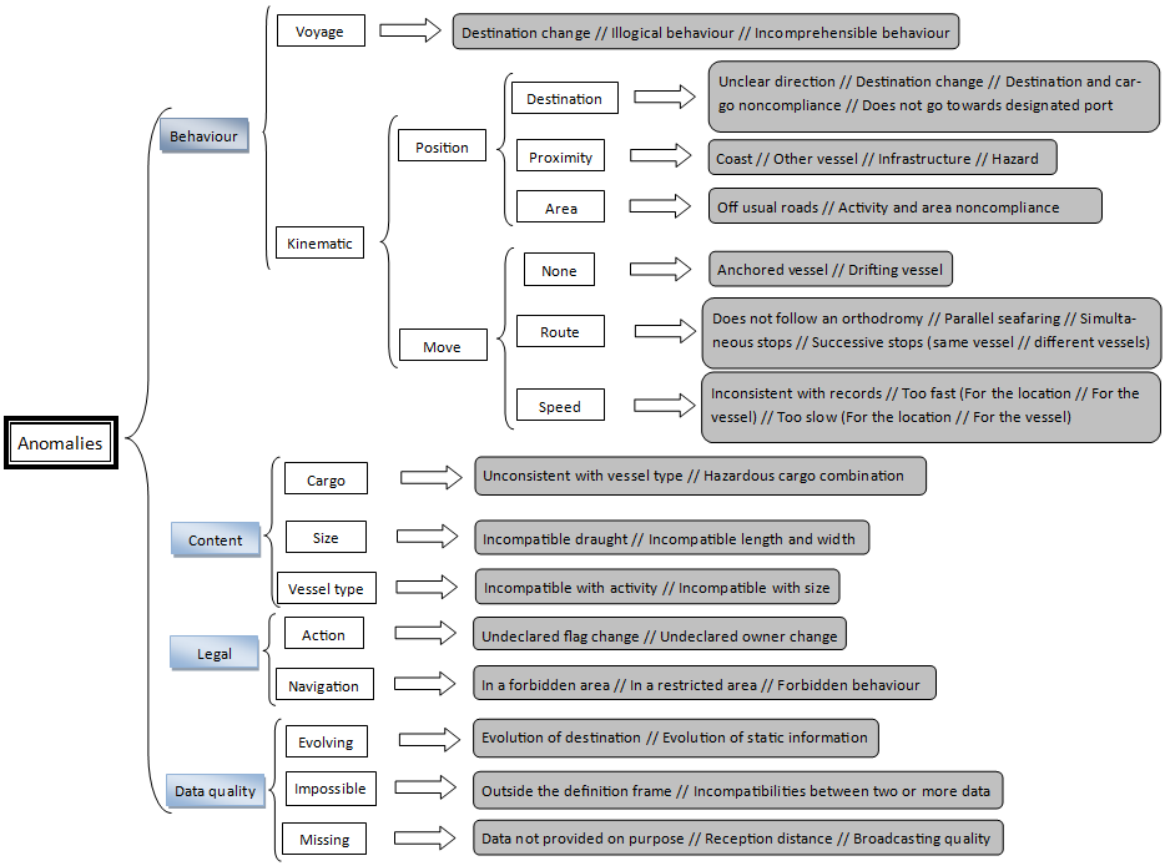

Figure 1: Proposed typology of anomalies

The family of behavioural anomalies is the most diverse one and, in the literature, the most studied one. In it, kinematic anomalies are the main sub-family, itself subdivided in position-based anomalies (about either the area of location or the destination) and movement-based anomalies (about either the route of the vessel or its speed, with or without engine on). The other subfamily consists of the route-based anomalies, that includes unexpected change of destination and non-understandable or illogical behaviour.

We distinguish two main subfamilies for the content anomalies: those in the content

of the messages themselves that do not follow the vessel's behaviour (such as static data, which usually do not change over time) and those about the people on board (either crew or passengers). Concerning static information, the elements concerned are the cargo (*e.g.* if two cargoes that are hazardous together are nearby, we consider the hazardous nature of the cargo according to the AIS technical specifications of Messages 5 and 24), the vessel dimensions (*e.g.* when the declared width is greater than the declared length) or the vessel type (*e.g.* vessel dimensions and declared activity are incompatible). As for the people on board, we can distinguish the passengers (*e.g.* the presence of illegal or hazardous people) and the crew (*e.g.* a number incompatible with the declared activity).

The lawfulness anomalies are split in two sub-families: criminal issues (organised crime or terrorism) and breach-level issues, *e.g.* undeclared change of flag or an unauthorised seafaring behaviour (such as the navigation in a forbidden area or the failure to comply with the right navigation direction in a TSS).

As for the data quality, within anomalies are distinguished the data changing unexpectedly (for pieces of information concerning static information for instance), the impossible data *e.g.* with a piece of information outside of the possible scope for it, or an impossible data case with respect to others pieces of information (if a comparison between various data fields is possible). Also, missing data due to voluntary lack of data provision or poor signal reception is considered.

The use of typologies brings a working framework that enables the categorisation of anomalies. In addition to the typologies of anomalies in the maritime domain, other kinds of typologies have been established on related subjects. Those typologies have as topics the type of vessels, the hazardous behaviours, the environments (navigation conditions, regulated areas), the actors, the stakes and the motion models. Categorisation helps in the creation of links between various elements and can lead to pattern determination. The combinations of elements of those diverse typologies, set according to the technical specifications of the AIS and the issues between conflicting data led to the method of integrity assessment presented in the following of this section.

3.2. Integrity assessment of AIS messages

As presented in section 2.2, AIS messages can present vulnerabilities such as the presence of falsifications in their data and weaknesses in their structure, and that those vulnerabilities can eventually lead to the augmentation of maritime risks, the necessity of a thorough data analysis arises. The structure of AIS is however complex and this complexity must be taken into consideration in our analysis. The system broadcasts 27 different kinds of messages, each one having its purpose according to the technical specifications of the system and displaying various data fields. Some messages are sent by mobile stations (mainly vessels) and other by fixed stations (mainly coastal stations), some are positioning messages (displaying also

the kinematic characteristics of the vessel), other display static data or communications. This variety of messages carrying pieces of information of diverse nature must be taken into account for a throughout study of the system. The variety of nature between the data fields must also be considered. Indeed, six distinct data types exist, as the data field can have a nature of numerical value representing an identifier, date, text, binary field, numerical value representing a choice in a given list of values or numerical value representing a physical quantity.

Taking into consideration the data within the fields of all messages types, four ways to discriminate the inner integrity of those pieces of information can be distinguished. Figure 2 displays those four ways, with their corresponding numbers on the left-hand side of the schema. The first way is constituted of the control of the integrity of each single field of each message taken individually (so excluding all other messages and context). The second way lies at the scale of one single message. In this single message, the integrity of all the fields with respect to one another is assessed. As 27 types of messages exist, the messages of the same family present the same fields and it is therefore possible to compare them and perform an integrity assessment, and this constitutes the third way. Eventually, the fourth way consists of the comparison and integrity assessment of data fields from different messages. Indeed, as pieces of information can come from different message types, it is possible to perform an integrity assessment as some fields are either the same one, similar or linked in some way. In the following, those four ways will be respectively referred as first-order, second-order, third-order and fourth-order assessments. The first-order and second-order assessments rely on only one message, and therefore are invariant with the environment (other messages, outside information), whereas the third-order and fourth-order assessments use several messages in data history (from one other message up to an entire time series for one vessel), and consequently the result of those assessments is expected to vary according to the environment (elements that can make it vary include the sample size or the location of the message within the sample).

The data integrity assessment is done through integrity items, which consist of simple and unambiguous statements involving one or several data fields. Each of the statements is either about one field, several data fields in the same message or several data fields in several messages in which data could present a deviation from the expectations of the technical specifications or in which cases where data within the data fields could disagree can be spotted, *i.e.* displaying at least two pieces of information that are not expected from being displayed in a proper or expected functioning of the system. A total number of 935 of those integrity items have been identified throughout the 27 AIS messages types. We individuated all those items by a careful and throughout review of the AIS system, the study of the technical specifications and the pairwise comparison of all data fields from all 27 message types. As an example, four items (one from each order of analysis) are

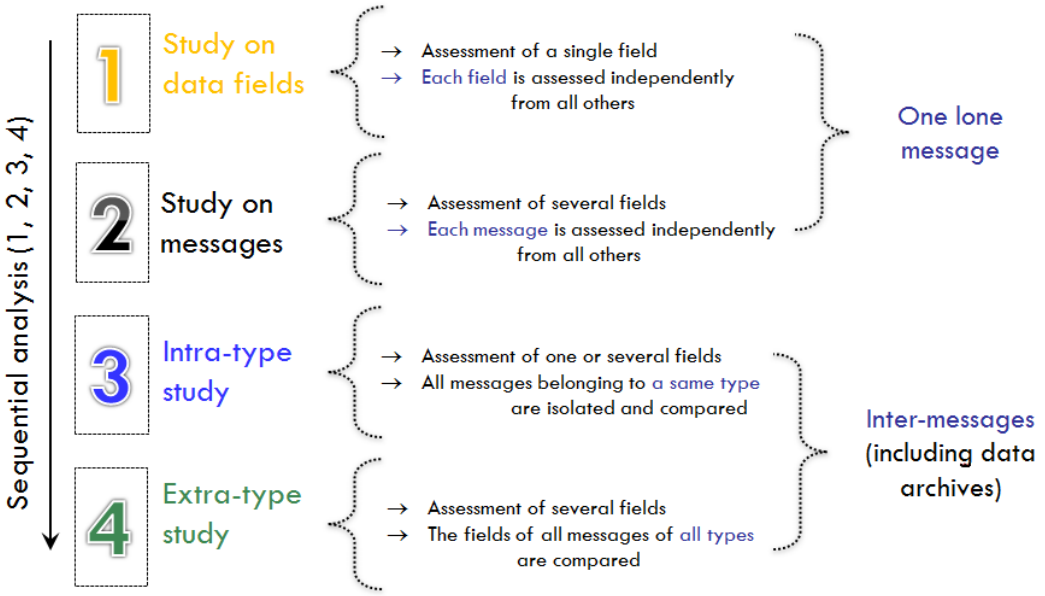

Figure 2: The four-order assessment

presented here: (1) "*Latitude value is not within the [-90,90] interval, and is not 91 (default value)*" as an example of first-order item, (2) "*Vessel displays using Loran-C as position fixing device but displays coordinates incompatible with the use of Loran-C*" as an example of second-order item, (3) "*The evolution of displayed coordinates in consecutive messages is not coherent with the displayed values of kinematic fields (speed over ground, course over ground and rate of turn)*" as an example of third-order item, and (4) "*Two vessels displaying a communication with messages number 7 display coordinates in messages number 1 that are too remote for this communication to occur*" as an example of fourth-order item. In those cases, (1) only involves one message and one data field, while (2) needs two data fields (the position is split into latitude and longitude fields). (3) needs a series of messages of the same type, for instance schedules position reporting messages (number 1), while (4) needs one message number 7 and two messages number 1 to be assessed.

Once the list of items is determined, each of the item must then be assessed following a rigorous process so that the coherence or the conformity of the data fields within can be checked. The value allocated to the item for the assessed message is assigned as Boolean, thus taking the value True or False, considering the value as the answer to the question: Is the statement expressed in the item demonstrating an AIS-data integrity violation? The value associated to this item for this message is then True if the item states something which occurs to end in an integrity problem, else it is False.

A logic-based formalism based on predicate logics is used for this study, this choice allowing to produce a deterministic result that is computed in a rigorous and unambiguous way. These assessments are then based on three elements: the syntax of the logic-based

formalism, the data fields values and the expert values, which are particularly important in the establishment of thresholds.

In this respect, the values of all relevant thresholds for the computation of the items were decided by a merchant navy officer after he was presented all the situations in which his expertise was required. This expert, licensed merchant marine unlimited chief officer Thibaut Eude, was at that time with the Centre for research on Risks and Crises (CRC), along with two of the authors of this article. All other experts involved in this paper also reviewed the knowledge provided by Dr. Eude, largely validating it and marginally modifying it.

3.3. Misuses scenarios

The integrity analysis of the system implies the use of falsification scenarios, which enumerate a given number of use cases. As systems in general can undergo falsification, it is crucial to be able to point out the different cases in which such a falsification can happen in order to adapt and proportionate the response. As a falsification consists in the fact to transmit erroneous data or to trick the system by forcing it to behave in a way it is not supposed to do, a falsification case will represent one particular scenario, one particular way to change data, force the system to behave the wrong way or input false data.

In the case of AIS falsification and spoofing several falsification scenarios are possible, and this section presents a non-exhaustive list of falsification scenarios, but which corresponds to those chosen in our implementation. Those scenarios are presented in the Table 2.

Case #	Scenario name	Description
1.1	MMSI	Station has an irregular MMSI number
1.2	Identity issue	Vessel displays an identity incompatible with complementary data sources
1.3	Identity change	Vessel has changed one of its identity data fields
1.4	Ubiquity issue	Station displays various whereabouts at the same time
2.1	Wrong position	Vessel displays an impossible location
2.2	Kinematic inaccuracies	Vessel positional values are in disagreement with kinematic values
2.3	Disappearing/Reappearing vessel	Vessel has unexpectedly disappeared for an unusual time frame
2.4	Spontaneous unexpected appearing	Vessel has appeared in an unexpected area
3.1	Message 22 alert	Station broadcasts a message number 22
3.2	Message 23 alert	Station broadcasts a message number 23

Table 2: Considered falsification scenarios

The first category of cases addresses static information and vessel identity data (*i.e.* scenarios 1.x of Table 2). In this category are gathered the issues related to the MMSI number, the identity issues such as identity change and the ubiquity issues (which consists in receiving positions too remote only seconds or minutes apart from a single MMSI). The second category gathers cases based on spatio-temporal information of AIS messages (*i.e.* scenarios 2.x of Table 2), amongst which the scenarios selected are about kinematic inaccuracies, the

wrong position of a vessel (such as a vessel reporting a location on a landmass), the fact to disappear and reappear in unexpected location or the fact to spontaneously appear in an unexpected location. A third category is about two AIS channel management messages which are particularly peculiar messages of the system: the messages number 22 (defined as channel management) and 23 (defined as group assign command). Those messages, only sent by base stations (coastal stations monitored by coastal maritime authorities), send operational parameters to mobile stations in their range which are of paramount importance: those messages assign and can change the frequency of transmission in the case of message 22, or impose a transmission interval or even a forced quiet time to mobile stations in the case of message 23. Those two messages can be sent to specified vessels (in assigned mode) or to all vessels in coverage (in broadcast mode). In this latter case, a variable amount of vessels (depending on the density of the local traffic) can be affected by a single management message.

In order to perform the assessment of those scenarios, the use of the sole AIS data is not enough. Additional data, mainly contextual, must be integrated into the study. This enables the fact to take into consideration environmental data. Indeed with the use of only AIS data, some cases can appear where some situations may look normal whereas with contextual values we can point out potential issues. Similarly, some situations may look anomalous but the addition of contextual data can explain the behaviour. AIS and contextual data will be presented in section 5.2.

A series of indicators, called flags, have been set as the output of the scenario assessment. Their nature and the way they take their values are presented in section 3.4.

3.4. Flag generation

3.4.1. Definition of a flag

Inside the scenarios themselves, there are several ways to assess data, and several ways to point out the problems in the data, the discrepancies or cases of unreliable data. In this frame, a basic element for anomaly detection has been defined. This element is part of a scenario, and assessed during the assessment of the scenario in question.

As their value is either "*No*" or "*Yes*", those basic elements have been called *flags*, and will be referred as such in the following sections of this document. Each one of those flags stands for a fundamental explicit case of integrity breach in the data assessed.

Two main families of flags can be discriminated: flags directly linked to the integrity items previously computed and flags linked to assessments with data coming from outside the system. The flag is a Boolean value, and its initial value is False. Then, if the scenario in which the flag is located is assessed then its value can be changed to True if the conditions for this particular case to raise the flag are gathered. The number of flags assessed actually depends on the number and type of available databases, as the flags linked to the integrity

assessment items do not vary over time.

In this section, in the scope of the study of the AIS system, three kinds of flags are presented, one being the family of the flags linked to integrity assessment items (so which number does not vary over time): the integrity assessment items flags ; another one being the family of the flags developed specifically for the scenarios, based on contextual data (so for which the number of flags varies with respect to available data): the scenario-specific flags ; and a last family gathering all the other flags, those linked to the vessel itself and its relationships with its environment (through maritime situational indicators, or MSIs).

The origin of the various flags and flag families is shown in Figure 3 and presented in more details in Section 3.4.2.

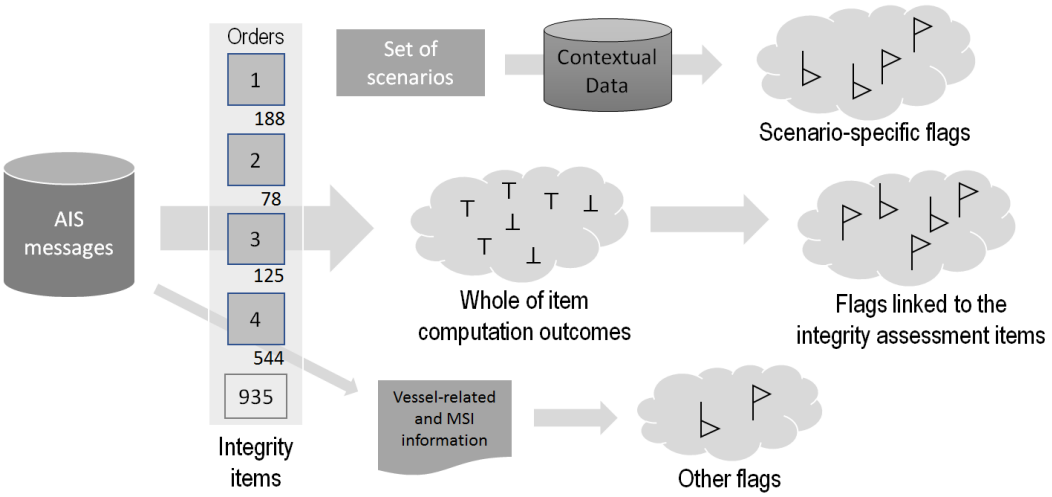

Figure 3: Generation of various flag families

3.4.2. Flag assessment

As for the flags linked to the integrity assessment items, in Section 3.2 was defined a method for determining the integrity status of every single integrity assessment item. However, this method processed data fields separately and it was not possible to easily drag any information from it. The purpose of an efficient flag assessment is to extract from each set of items corresponding to each message type issues that are humanly easily understandable, which are the flags.

Each one corresponds to a specific issue in the analysis of AIS messages. For instance, one of the flags is called "*remoteness*", and corresponds to the fact to have two communicating vessels despite the fact that the location they pretend to have makes the distance too high for their communication. The distances are computed using the Haversine formula (commonly used for the computation of maritime distances, e.g. [72]). It is expected that two vessels communicating are within reception range of one another and display their whereabouts in accordance. Occasional ionospheric super-refraction is possible in a distance range exceeding

the direct reception range, but repeated communication is deemed as unlikely to display a genuine behaviour.

As stated before, a flag is a Boolean that takes the value False if no problem is spotted and True if a problem is spotted according to the relevant associated items. The False value is the default value, and the True value is triggered as soon as one of the associated items has a False value.

For each of the items in each scenario, a list of corresponding integrity assessment items have been established, the results of which must be queried and assessed in order to get the outcome of the flag computation. The list of integrity items for each flag is fixed, and the list of flags which directly use integrity items results is fixed for each scenario, therefore the list of integrity items needed for each scenario can be easily obtained by gathering all items of every single flag of the given scenario.

For example, for the case of the "*remoteness*" flag, there are 17 different items corresponding to this flag in the case of message type number 1. If only one of those items display a True value (so an integrity issue is spotted), then the "remoteness" flag will be set to True.

As for scenario-specific flags, those ones are totally dependent on the available external datasets, and each flag will be tied on the content of the dataset. Therefore there is no fixed list of those scenario-specific flags, as it will vary according to the available datasets. The fact to use such datasets is particularly important in order to be aware of the environment of the system, and the assessments provided are as various as data coming from the system enable it.

Each flag is associated with one particular assessment type involving both system data and non-system data (*i.e.* it is necessary to query both AIS and non-AIS data before assessing the item), then the computation of the result is done in a specially designed algorithm, as if the system side of the computation is fully known, the non-system side of the computation is subject to vary with respect to the database used. Therefore it is not possible to write a general assessment program but it is necessary to adjust the program to the data structure and type of the non-system dataset. Similarly as for the flags determined from integrity items, the default value is False, and it is changed to True whether the conditions set on the values coming from the databases by the algorithms are gathered.

As for the other flags, the vessel type flags allow to discriminate vessels, so several vessel types have been set, and each one of those types has a flag which is False if the vessel is not of the type in question and True if the vessel is of the type in question. As the data type is part of AIS static message information, it is possible to assess it easily. In addition, flags have been set to describe maritime situations occurring at the time of the message. Those flags, backed on Maritime Situational Indicators (MSIs) [73] allow to take into consideration the environment of the vessel, its location and the surrounding environment in order to get a more comprehensive analysis.

4. Risk assessment

In this section, we build on the integrity analysis performed in Section 3.2 that led to the establishment of a series of flags presented in Section 3.4, of which the purpose is to describe the state of a vessel at the instant the message was sent using humanly understandable features. The next step is then to assign to those messages a particular risk nature and representative risk levels, so that an operator can have additional information for decision support. However, in order to perform such a risk assessment, a discrete and finite set of maritime risks must be isolated, which is the purpose of the first part of this Section. Then, a method involving the flags, purely deterministic in this paper, has to be implemented, so that each message is allocated risk levels with respect to a variety of parameters such as the type of the vessel, the type of risk and the nature of the implication (on humans, infrastructures or the environment in our case), which is presented in the final parts of this section.

4.1. The risks in the maritime environment

At sea, people are exposed to risks that are various and have evolved with time and the evolution of ship building techniques, electronic communications and medicine. Three main families of those risks can be discriminated: the natural risks, the environmental risks and the anthropic risks. Natural risks include weather-linked hazard such as storms, that endanger mariners at sea, workers on shores and harbour infrastructures. Thanks to weather forecast some of them are predicable, but others are unpredictable, such as tidal waves or collisions with a cetacean. Anthropic risks include risks related to submerged mines and ammunition, which are a direct threat to fishermen and the environment, and an indirect threat to seafood consumers. The fact that a great amount of vessels are under a flag of convenience is also a concern for the security of navigation, as those states are less cautious about the health state of the vessel. Environmental risks include diseases linked to the fact to navigate (for instance scurvy in past times) and to be in a confined and physically isolated place. However, the isolation has been reduced since the introduction of the Internet and telemedicine is now possible. Amongst the environmental risks, oil slicks are the one with the global best awareness, as the consequences are both at sea and visible on shore.

Maritime risks are linked to the use of vessels by humans. In this paper, as maritime risk we intend any kind of hazard that is the consequence of maritime navigation and the human exploitation of the sea, either directly to the crew, to other human beings, to the environment or to coastal infrastructures. Collisions are maritime risks, as they can be caused by carelessness, bad visibility when two vessels have secant trajectories or priority denial. Another risk for a ship is to run aground, and can be a result of bad manoeuvres, a bad or not up-to-date documentation or an erroneous estimation of the water depth. Other risks include fires, leaks or terrorism. The consequence is that the vulnerabilities are

various, for instance in the case of energy transportation, which has geostrategic importance, particular care should be taken, as some areas vitally require their energy income from the sea. All kind of transportation by the means of vessels implies the existence of the risks associated with the goods transportation. In addition, some energy transportation is done via lines (between offshore platforms and the shore or between countries), laying themselves open to sabotage. Offshore platforms are vulnerable to piracy because of their immobility and isolation, as well as vessels for ransom of the crew, the cargo or of the vessel itself. The vulnerability increases with the transportation of hazardous goods in fragile environment. In strategic points such as straits or canals, or off the coasts of weak states (because of piracy risk) the vulnerability of the global maritime traffic is particularly important. International cooperation in the matter intends to reduce the danger linked to those vulnerabilities.

In our study, it was decided to concentrate around five main risk families, namely collision, grounding, illegal fishing, piracy and terrorism, and illegal transportation, all of them presented in Table 3.

Family	Risk of interest	Description
Navigation Hazards	**Collision**	Unintentional physical encounter between two vessels
Navigation Hazards	**Grounding**	Unintentional case of a vessel running aground
Illegal Activities	**Illegal Fishing**	Case of illegal, unreported and unregulated fishing
Illegal Activities	**Piracy & Terrorism**	Piracy or terrorism threat to the vessel
Illegal Activities	**Illegal transportation**	Case of illegal transportation of goods or people

Table 3: An overview of the considered maritime risks

This choice of reduction of the possibles to a shortlist is done in order to restrict the risk study to the risks that are actually relevant to the particular case we study, and in order to remain in a closed world. The fact to set a fixed number of risks makes the computation of risk levels possible (by making things correspond to general foreseen cases) and prevents the final user from having trouble to comprehend the maritime situation by restricting to risks known by users.

This list is obviously not exhaustive, as other risks do exist while at sea (such as illnesses that can endanger people and bring diseases to new places). Also, only the risks that could reasonably be spotted out by the study of AIS messages were selected, as they can be susceptible to be triggered by an error or a falsification of the AIS. Also, this paper, by its nature, focuses on the sole vessels that do have an (at least partly) active AIS transceiver on-board. A noticeable amount of vessels worldwide do not comply with the international regulations or are not required to carry the system [55], amongst which a number is performing illegal activities. Those vessels do not represent the focus of this paper.

4.2. A risk analysis of the AIS

The issues on the AIS presented in the section 2.2 and formalised in section 3.2 have an actual impact on the navigation and on the safety at sea, as both coastal authorities and

mariners use these pieces of information about their surroundings as decision-support tools in navigation and monitoring cases. Consequently, an imperfect displaying of the real maritime picture can therefore result in poor decisions that can have a variety of consequences.

In this respect, we performed a risk analysis of the AIS with a naval officer [74]. This expert (Lieutenant Erwan) who achieved the risk analysis is a operational expert from the French Navy. The expert followed a specific training on cyber defense and developed skills on AIS analysis. The expert used the EBIOS method that have been developed by the ANSSI (French National Agency for the Security of Information Systems), and which is compliant with ISO norms 27001 [75], 27005 [76] and 31000 [77]. This method proposes an approach of risk evaluation that clarifies the entities of the system, their vulnerabilities and the possible threats, and that contributes to the evaluation of the correct level of security that must be put in place to reach the required specifications. The procedure, as shown in Figure 4 consists of a series of five modules, processed sequentially and in charge of the context study, the study of dread events, the study of threat scenarios, the study of risks and the study of security measures.

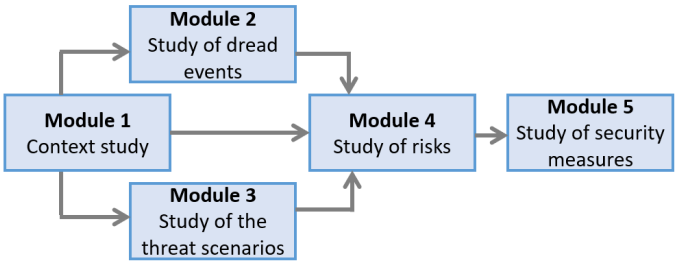

Figure 4: The EBIOS procedure in modules

Based on an preliminary analysis of AIS vulnerabilities [78], the risk analysis lead to the identification of circa 350 threat scenarios. This study of threat scenarios include the identification of essential goods (e.g. positioning and route-based data), essential functions (e.g. transmit AIS data) and support goods (e.g. GNSS device), the establishment of lists of threat sources (e.g. piracy) and dread events (e.g. static data are accessible to an opponent), the identification of risk of intolerable level (e.g. risks linked to the dynamic data integrity) have been realised, as well as the discrimination of the most plausible threat scenarios (*e.g.* the use of the computer for other tasks, the identity change of the transceiver, the branching of a non-legitimate input, the unexpected data according to the norm, the injection of false data for the spoofing of reporting tools and the villainous use of maritime traffic surveillance).

This analysis was then used as a basis for the determination of analysis flags in their process of association towards the determination of maritime risks as presented in the remaining of this section.

4.3. From analysis flags to risk determination

A link between the flags and the risks must be established in order to link the cases that resulted of the flag analysis, taking into consideration both system and non-system data. It is indeed necessary to process the outcome of the flag analysis by turning it into a risk assessment. Figure 5 show the workflow from the set of flags that have been activated by the processes presented in Section 3 and the assessment of the risk levels. The five boxes of the central column of Figure 5 are the steps of this workflow, and each of the four transitions will be addressed in a dedicated Section 4.3.1, 4.3.2, 4.3.3 or 4.3.4.

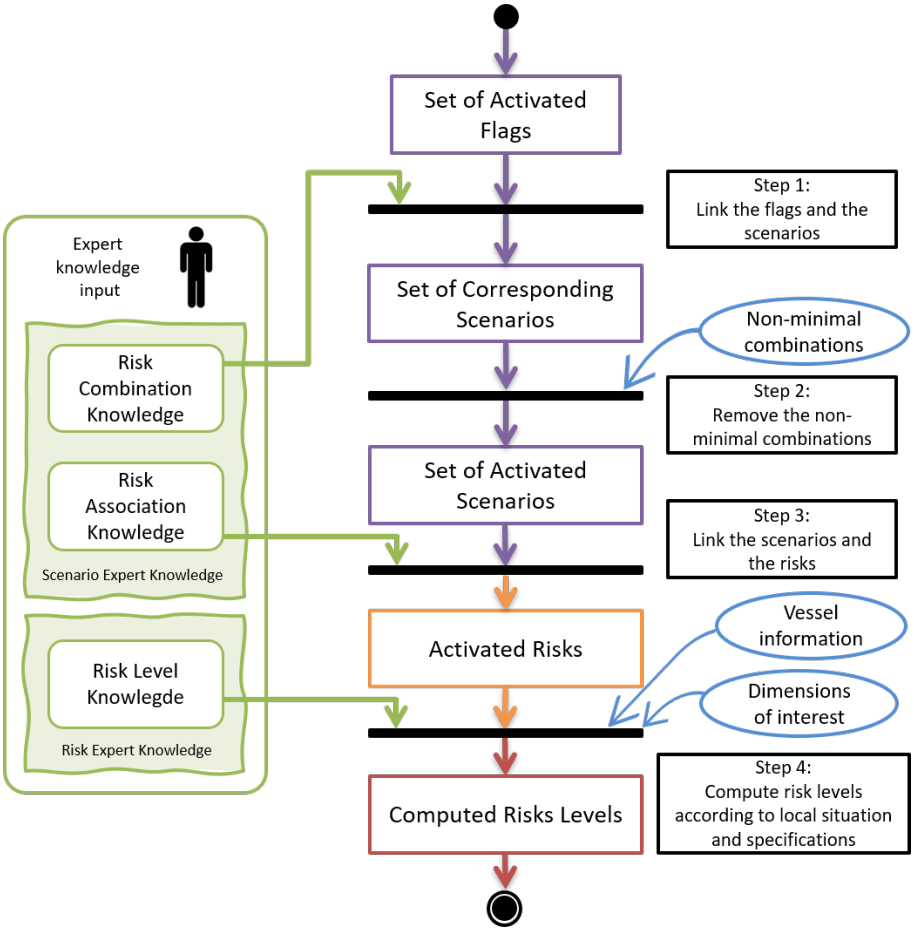

Figure 5: Workflow of the risk level determination

As in this workflow, some elements required experts knowledge, we performed the establishment of risk combinations, risk associations and risk levels with two French navy officers. These experts (Lieutenant Dominique-Marie and Lieutenant Louis) directly provided their knowledge in the process of the establishment of scenarios, during a short in-person stay. They also provided guidance for the determination of the elements of interest to be presented in an interface that would act as a final tool to display the maritime traffic and the issues that are spotted by the analysis presented in this manuscript.

4.3.1. From the set of activated flags to the set of corresponding scenarios

In the case of AIS, different possible risks have been presented in Section 4.1, and every single flag, as developed in Section 3.4, represents its own kind of information about the state of maritime traffic, either on falsification scenario cases with all-AIS data or non-AIS data for the determination of the neighbourhood of the vessel. Thus, as each flag represents a given situation, it must be linked to at least one of the risks described in Section 4.1. But as several flags can occur on the same vessel, the notion of flag combination must be addressed. Indeed, the combination of a variety of flags can be performed and this combination can highlight either a given risk or a group of risks. In the following of this section, a flag combination designates a finite whole of flags selected in such a way as their combination consists of a given situation that leads to a designated risk or a group of designated risks (*cf.* Section 4.3.3).

A large variety of flag combination have been established by maritime domain experts in our study (and therefore considered as expert data), in the frame of the processing of AIS messages. Figure 6 is a schematic representation of the various flag combinations that have been established, under the form of a table of which each column represents a given scenario, each line represents a specific flag, and the scenario is activated if all the flags associated with it (represented by black cells in Figure 6) are been triggered by the item assessment. As an evolving system, any expert can modify, add or remove a scenario. In Figure 6, the flags are named f_x for illustrative purposes (so without representing specific flags individually), and three families of flags have different notation to underline their different nature. This table is a result of the deterministic approach we chose, for which a fixed frame must be used and filled with various flag combinations taking the role of rules which are told and can be modified by an expert.

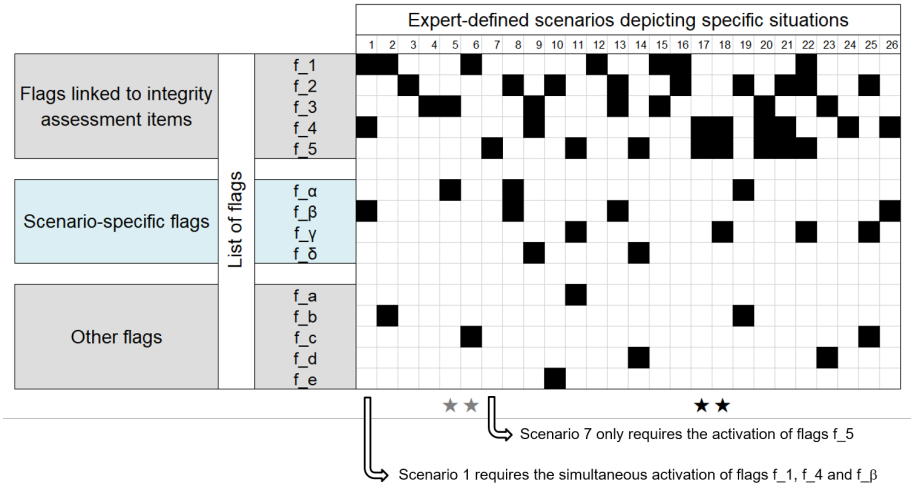

Figure 6: Combination of flags in expert-defined scenarios

4.3.2. From the set of corresponding scenarios to the set of activated scenarios

In most cases where the number of flags triggered is non-insignificant, a collection of flag combination and therefore a collection of scenario will be activated.

Since a variety of scenarios have been developed, some of them only slightly differ. Let us take into consideration the scenarios 17 and 18 of Figure 6: $S_{17} = \{f_4, f_5\}$ and $S_{18} = \{f_4, f_5, f_\gamma\}$. In this case, $S_{18} \subset S_{17}$, so we can say that S_{18} is a particular case of S_{17}. Therefore only S_{18} for future computation, and particularly for the incoming risk analysis, since a more accurate scenario is expected to provide a better risk assessment by focusing on a more relevant risk type. Another similar example is shown in Figure 6 where $S_4 \subset S_5$. Only the scenarios with the largest amount of flags, describing a more accurate situation are kept for further analysis and are considered activated.

4.3.3. From the set of activated flags to the activated risks

Mirroring the scenario selection table presented in Section 4.3.1, a risk selection table has been set by maritime experts in order to select, for each of the scenarios set, the list of risks to be considered as activated. A schematic representation of this table is presented in Figure 7, where the columns represent the exact same scenarios that in Figure 6, and the five rows represent the five selected risk families (presented in Section 4.1). Whether a scenario is activated, it triggers all the risks marked with a black cell. A collection of scenarios is likely to trigger a variety of risks, and sometimes several times the same one. Multiple triggering are not taken into consideration and the activated risk is not treated differently with the number of scenarios it has been triggered by.

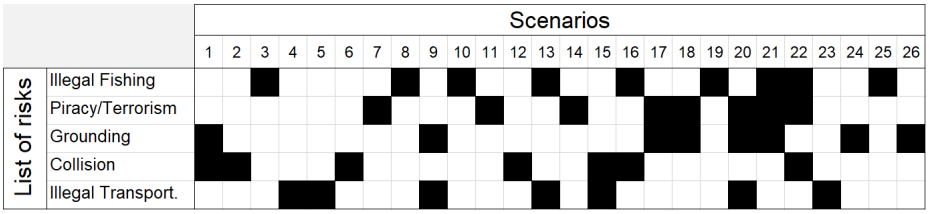

Figure 7: Schematic representation of the relations between scenarios and risks

4.3.4. From the activated risks to the computed risk levels

Once the risks determination has been performed, the nature of the level for each of the selected risks must be determined. As it depends on both the environment and the stakes, various cases must be discriminated so as to to provide to the relevant authorities trustworthy data. In our case, the maritime domain, this environment covers the type of dimension in which the risk expends, and the type of vessel involved, which are presented hereafter. The level of risk is then computed for each of the selected risks and in each of the dimensions, following the values set by an expert of the domain and presented in Figure 9.

The risk level is assigned according to tables, each risk having its own table, as shown in Figure 8. The risk level table is more complex in the particular case of collision, as it involves two elements: the vessel of interest and the object with which it collides, which can be a vessel (of various size and hazardous natures) or an infrastructure (port feature or offshore platform that the vessel of interest can damage or endanger). In this case, some assessments require the knowledge of the nature of the collided object in order to apply suitable risk levels.

In order to have tables with proper values, we have been assisted by maritime experts for the elaboration of those tables. In general, this part of the work shall be done by experts of the maritime environment because of their knowledge of maritime navigation and of its dangers. As those tables contain expert data, they may evolve and be adapted to a new situation.

Grounding	H	I	E
T/C	2	3	2
T/C - H	2	3	4
P	4	2	1
PI/F/S	2	1	1

Piracy/Terr.	H	I	E
T/C	4	2	2
T/C - H	4	2	4
P	4	1	1
PI/F/S	4	1	1

Illegal Trans.	H	I	E
T/C	2	3	1
T/C - H	2	3	2
P	4	1	1
PI/F/S	4	1	1

Illegal Fishing	H	I	E
Fishing Ves.	1	1	3
Other	1	1	1

	T/C			T/C - H			P			PI/F/S			I			
T/C	2	4	4	2	4	4	1	4	3	3	4	1	4	4	4	Inducted
	2	4	4	2	4	4	4	3	2	1	2	2	2	3	4	Undergone
T/C - H	2	4	4	2	4	4	1	4	4	3	4	4	4	4	4	H / S/I / E
	2	4	4	2	4	4	4	3	2	1	2	2	2	3	4	
P	2	4	4	2	4	4	4	3	1	2	3	1	2	2	2	
	4	3	1	4	3	4	4	3	1	4	2	1	4	3	2	
PI/F/S	1	3	3	1	3	4	4	2	1	2	2	1	1	1	1	
	4	4	1	4	4	4	2	3	1	2	2	1	3	4	1	

Boarding / Collision: two elements involved (I = infrastructure)

Figure 8: Values of expert-based risk levels for each of the five risks of interest, according to the vessel type and the risk dimension of interest. In the case of the collision risk, the table has an additional entry, being the nature of the collided object (vessel or infrastructure)

Vessel types taken into consideration. For the risks of illegal fishing, piracy and terrorism, illegal transportation, as well as grounding, four kinds of vessel types are discriminated, as shown in Figure 9:

- **T/C** which stands for all cargo vessel, including tankers, for which the variety of goods carried in their tanks forces us to closely look at it. In this section, no vessel carry hazardous goods
- **T/C - H** which stands for the vessels that could belong to the T/C category but which currently carry hazardous (after the definition given in the AIS specifications)

goods

- **P** for passenger vessels
- **Pl/F/S** which stands for pleasure crafts, fishing vessels and service vessels

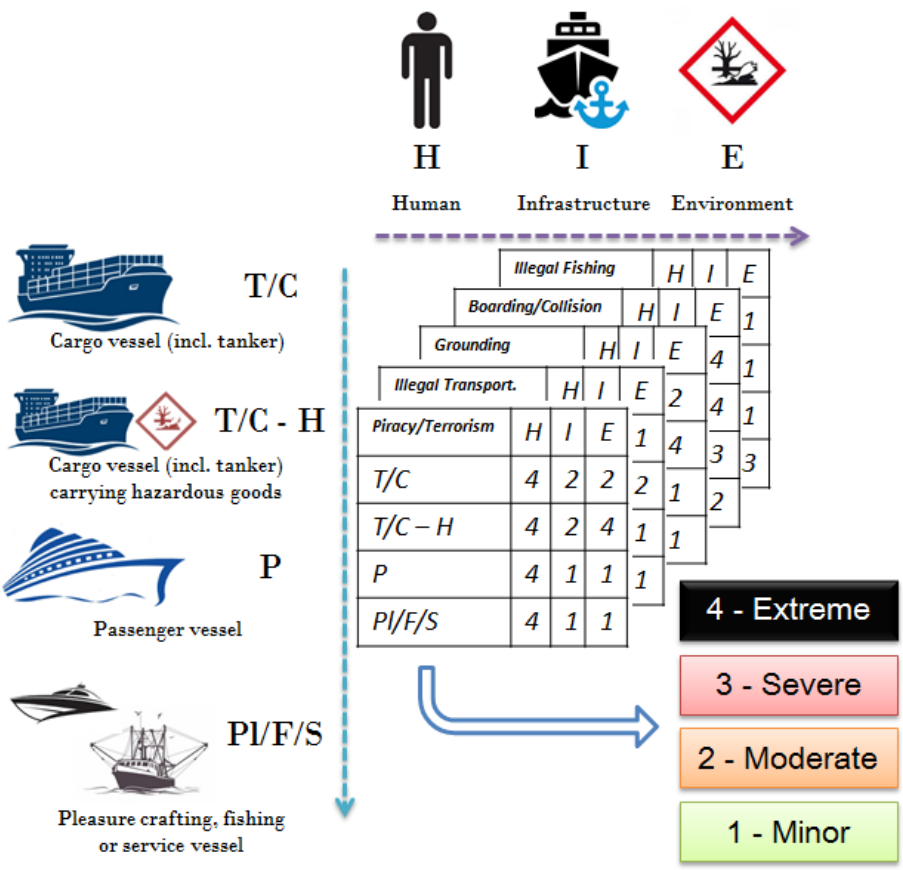

Figure 9: Risk level assignment with respect to vessel type and dimension of interest

Dimensions in which the risks spread. Vessels can represent a hazard on various subjects and upon various situations. In our study we discriminate the families of hazards in three dimensions, as shown in Figure 9:

- **H**: Human: risks linked to the endangerment of the human life at sea
- **I**: Infrastructure: risks linked to both the structure of the vessel itself, as well as risks linked to potential damages on the coastal and offshore infrastructures
- **E**: Environmental: this dimension encompasses all kinds of environmental risks

A scale of risk levels. Several risk levels have been established, as shown in Figure 9, and they have been defined after an excerpt from the CISE (Common Information Sharing Environment) as follow:

- **1**: Minor risk
- **2**: Moderate risk, *i.e.* injuries, light structure and infrastructure damages, small scale pollution
- **3**: Severe risk, *i.e.* major injuries, major structure and infrastructure damages, substantial pollution
- **4**: Extreme risk, *i.e.* death, structure and infrastructure destruction, environmental disaster

Computation of risk levels. As we presented in section 4.3.3, one or several risks can be triggered by the completion of one or several combinations. If only one risk is triggered, the corresponding values for H, I and E risks are taken as values to be displayed. If two or more risks are considered, for each of the dimensions of assessment (H, I and E), the result to be displayed is computed and consists in the maximum value of the corresponding risk level for the considered risks. With $\mathbb{A}$ being the whole of all risks, $\mathbb{A}^*$ the whole of the activated risks, $\mathbb{D}$ being the dimension of the risk, $\mathbb{D} = \{H, I, E\}$, then $Risk(\mathbb{D}) = \max_{r \in \mathbb{A}^*, \mathbb{A}^* \in \mathbb{A}} Risk_r(\mathbb{D})$ Similarly, if the vessel does not specify its type, or if there is a strong uncertainty about the genuineness of the type self-reported by the vessel, the highest possible risk value in all vessel types is assigned by default to the vessel in question. This enables further computations and the assignment of a risk level in spite of the fact that the vessel type is missing or doubtful.

5. Experiments and results

The proposed method for integrity assessment of AIS messages (presented in Section 3) and the consequent risk analysis (presented in Section 4) have been experimented using a set of real data. This section features a short presentation of the implementation of the method, the data prepared, and a set of experimental cases. Four experimental scenarios are selected for further in-depth analysis, from the initial data to the risk raised by the processing of corresponding AIS messages.

5.1. System implementation

In this section, we present the general architecture of the implemented prototype, including the fact to receive and parse the message, to populate a database and to analyse all messages received in an ordered way.

5.1.1. Reception and parsing

Upon reception from a dedicated antenna, the AIS message (a raw frame of data) must be processed in order to extract exploitable data and shape it accordingly with the technical specifications set by the ITU (International Telecommunication Union). This step, called

parsing, occurs in a parser. As our study require full handling of all dimensions of the process, we chose to design our own AIS parser, derived from an already existing one [1], despite the existence of software built-in parsers.

As AIS messages do not inherently carry temporal information, a timestamp is added by the parser to the message upon reception, allowing the creation of time series of messages, and enabling temporal analyses.

The AIS is a global system, therefore an encompassing analysis of the messages require the use of several stations (that can possibly receive the same message, but that will timestamp it individually). Whereas we only work with our data from one single station, the extension to several antenna possibly receiving the same message several times have been foreseen. This opens the possible creation of a fifth dimension of integrity item (in addition to the four presented in Section 3.2), proposing a receptor-based order based on inter-receptor identity checks.

5.1.2. An analysis with historical or real-time data

AIS message processing is organised by performing successive evaluation loops as shown in Figure 10. A loop stands for the succession of the complete processing of messages (*i.e.* item assessment, flag computation and risk level assessment) and and include a potential waiting time before the next loop begins which allows to control the recurrence of executions. This waiting time, left at the will of the user, is necessary as the processing of messages received in a timespan of p seconds needs less than p seconds.

This architecture allows the real-time processing of messages, as messages are processed by blocks (which eases studies on time series). During a loop are processed all messages that were received during the timespan of the former loop (which itself processed messages received during the one loop beforehand).

An analysis on historical data is also possible, following the same processing principles. In that case, the user can choose a times interval on which the analysis applies. The only difference is that there is no waiting time in this case, as we do not have to wait until enough messages have been received to trigger a new processing loop.

5.1.3. Implementation choices

The program was developed in Python for its ease of handling, its computational abilities and the fact that it enables database querying with embedded SQL, as well as convenient handling of query results. This is linked to the use of a relational database management system for data storage and querying. The choice of the widespread system PostgreSQL was made, with the adjunction of its spatial extension, PostGIS, enabling the convenient processing of spatial features.

[1] https://github.com/tbsalling/aismessages

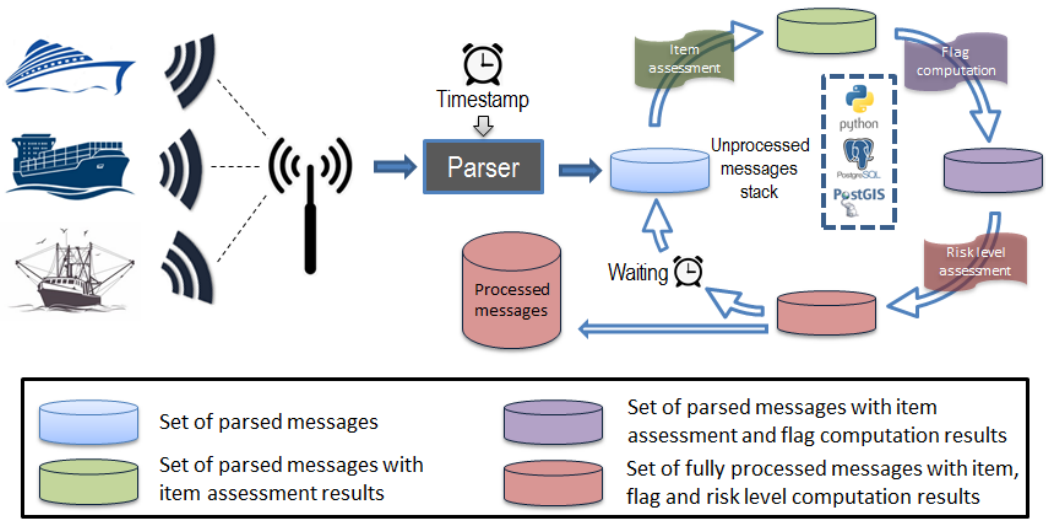

Figure 10: Loop-based mechanism for data processing

The user interactions are kept minimal, as the sole input outside the database is the list of items the user wants to see assessed by the program. However, as the AIS system can evolve, as other datasets may become available, and as users may want to see some particular functions implemented, the program has been coded in an opened way, enabling easy changes and upgrades to be performed.

At this stage, some expert knowledge is desirable to be able to grasp the possible needs in terms of user interaction and result display features. Therefore the implementation was performed partly with the support of two French navy officers. These experts (Lieutenant Kevin and Lieutenant Joseph) contributed themselves to input their knowledge, using their skills in the knowledge of the maritime navigation during a short in-person stay. Their contribution has been for instance valuable in order to fix values and thresholds in assessment algorithms.

5.1.4. System general architecture

In simple terms, the general architecture of the system lies on two elements: the database and the program. The purpose of the database, besides to contain AIS contacts, is to store data of various natures: AIS data, vessel-oriented data and geographic data (which will be presented in Section 5.2) and intermediate results of the computation, those results being used by another phase of the program. As shown in Figure 11, the database is composed of three main sections: the AIS messages, in which all messages are stored (one table by message type, and one table for corrupted messages), the contextual information (used at the scenario level) and the analysis data, with all intermediate results, as well as temporal or fixed parameters of the computation. The purpose of the program is to query the database, to assess the data and to return the result of the assessment, whether it is on items, on flags

or on risks, to the database through another query.

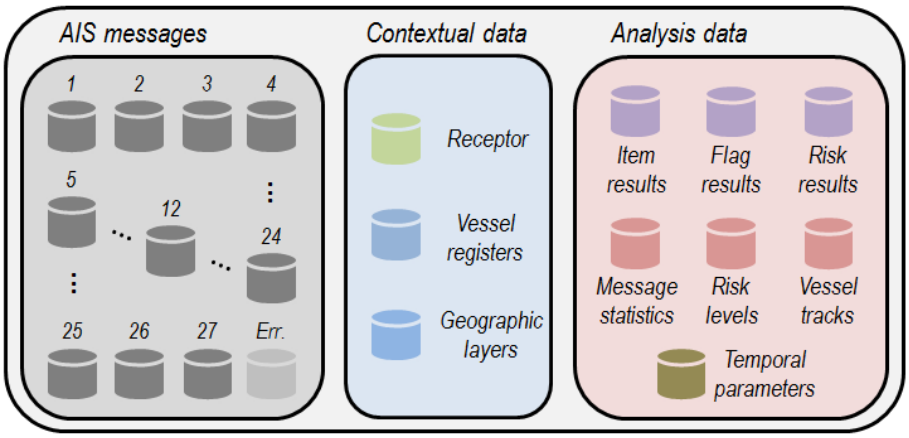

Figure 11: Composition of the database

5.2. Data prepared for the experiments

A set of real data has been prepared and organised for the conduct of experiments. The dataset contains three categories of data: AIS data ("*AIS messages*" part of Figure 11), vessel-oriented data and geographic data ("*Contextual data*" part of Figure 11). It covers a period of six months, from October 1^{st}, 2015 to March 31^{st}, 2016 and provides ship messages issued from the Celtic sea, the North Atlantic ocean, the English Channel and Bay of Biscay (France).

AIS data. The core of the data used for experiments is based on the 27 AIS messages received by a terrestrial station located in the Brest roadstead (France). The receiving station (VHF antenna, AIS receiver, Linux computer) collects AIS messages from a majority of the roadstead, from the entering and exiting traffic and on the passing-by traffic in the Ushant Traffic Separation Scheme (TSS). Figure 12 shows on the left, the location of the receiver (red star) and its theoretical range (blue polygon). The right part of the Figure shows the actual spatial extent of AIS messages (that feature latitude and longitude data fields) during a time span of six months. The data (all messages) received by this antenna from October 1^{st}, 2015 to March 31^{st}, 2016 are used for our study.

The dataset consists of circa 24 million messages, 94% of them being geolocalised messages and 5% being static information messages, as shown in Table 4, which also display the number and percentage of messages per type of emitting station and families of messages. Message number 1 is by far the most used, representing 62% of all messages, before messages number 3 (13%), number 4 (12%), number 18 (4%) and number 5 (4%), which are the only messages to have a frequency greater than 3%. In our dataset, 71% of the messages number 1 are within 10 km of the reception antenna.

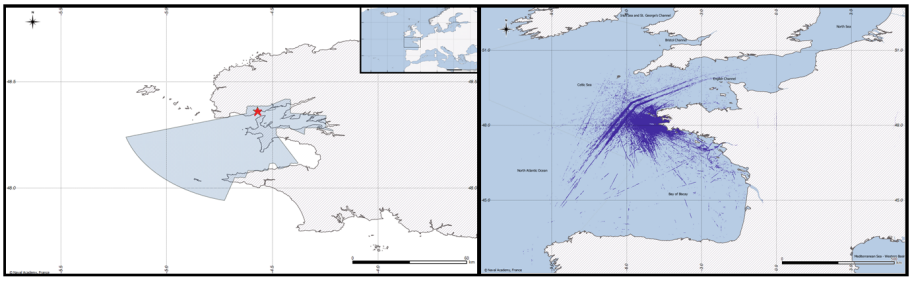

Figure 12: A view of the location of the geolocalised points in our AIS dataset messages

Message family #	Number	%
Total	24033893	100
Geospatial	22493074	93.6
Communication	2798	0.01
Static	1084275	4.5
Mobile station only	20369720	84.8
Base station only	2803972	11.7
Mobile and base stations	860201	3.6
Standard	20570972	85.6
AToN	505764	2.1
Timing	2807055	11.7
Safety	46	ε
Binary	150044	0.6
Other	12	ε

Table 4: Number of messages per family type

Falsified AIS data. Genuine AIS messages of the dataset natively contain errors and misconfigurations. They also contain several falsifications (*cf.* Section 2.2). However, some behaviours involve rare or never received messages, other require a condition on data which is rare (for instance a trajectory having a given path or displaying a given behaviour). In order to test, evaluate and validate algorithms and specific scenario cases under reference data, controlled degradation of data has been also performed. Our approach relies on two degradations: first, original AIS data has been manually or automatically modified. Second, some AIS frames or sequences of AIS frames were created intentionally and injected in the dataset. Figure 13 shows a typical fake trajectory specially designed to activate many items and flags at once (wrong speed, heading, ubiquity,...).

The built and use of those fictive frames allows to generate any falsification scenario. Thanks to an emitter platform based on a Software Defined Radio (SDR) that we designed similarly to [66], false messages can be broadcast live with real AIS flow. During experiments, because of their potential threat to navigation and because of our neighbourhood with a sub-surface ballistic nuclear basis, all falsified messages have been either broadcast within a laboratory platform with very low power or piped directly within our reference database (in the middle of real historical messages).

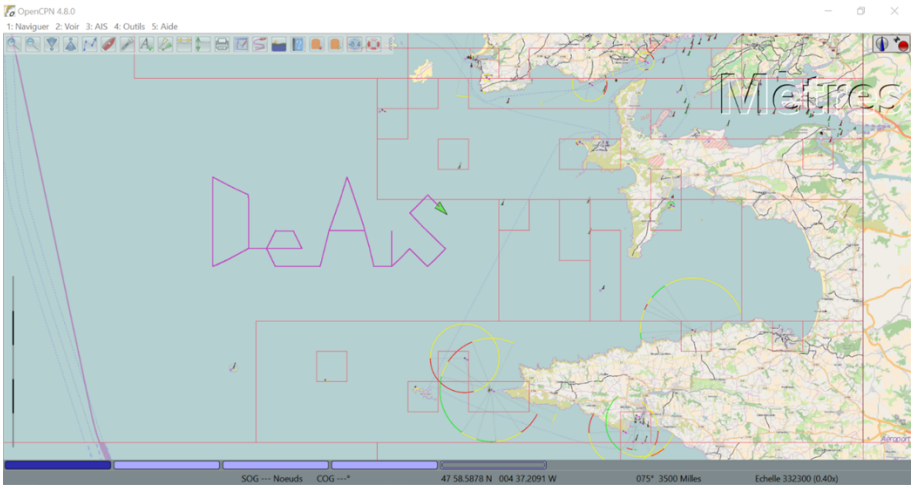

Figure 13: A fake trajectory (*visualisation based on OpenCPN (opencpn.org) and OpenStreetMap (openstreetmap.org)*)

Vessel-oriented and geographic data. As for non-AIS data, we concentrate on two kinds of complementary data: environmental (*e.g.* marine protected areas) and vessel-oriented (*e.g.* fleet registers). In the case of our study because we use data from a Brittany-based station, some dataset have a limited spatial extent around our point of interest, while other are at larger scale, possibly worldwide. Of course, such datasets must be in accordance with the temporal and the spatial extent of the data assessed. Data prepared for our study includes, for instance, Natura2000 protected areas, anchorage and restricted areas, polygons of Brest port and roadstead, two fleet registers, the location of ports, the coastline and the Ushant traffic separation scheme. An extended release of this dataset also including local weather conditions and sea state is available [79] and described in [80].

5.3. Exemplification through the assessment of experimental cases

The purpose of the implementation presented in Section 5.1 is to experiment several use cases of possibly hazardous situations through scenarios, allowing to demonstrate the potential of the approach. More specifically, scenarios can be designed and ran in order to evaluate the outcome against actual or synthetic data, and assess the accuracy of the detection. Considering that data are unreliable, many assessment cases have been designed on a tailored basis (*cf.* Section 5.3.1) in order to demonstrate that the analysis procedure is able to handle confusing scenarios and thus providing information to identify both hazardous and falsified situations.

5.3.1. A variety of experimental cases

Several assessment cases can be set, following the variety of scenarios presented in Section 3.3, and a total of 13 experimental cases have been established. Table 5 presents all the

cases, the number of the scenario they belong to (*cf.* Section 3.3) and a short description of the case.

Exp. #	Sce. #	Description
A	1.1	A vessel shows an impossible MMSI
B	1.2	A vessel displays an identity which is non compliant with our fleet register
C	1.3	A vessel unexpectedly changes one of its four identity features
D	1.4	A MMSI number transmits from two different locations at the same time
E	2.1	A vessel transmits from a landmass
F	2.2	A vessel is spoofing its whereabouts
G	2.2	A vessel displays an inconsistent trajectory
H	2.3	A vessel has an important temporal gap between two messages
I	2.3	A vessel has an important spatial gap between two messages
J	2.4	A vessel suddenly appears in an unexpected area
K	2.4	A vessel suddenly appears in an expected location
L	3.1	A message number 22 is broadcast
M	3.2	A message number 23 is broadcast

Table 5: Description of the experiments

Out of those 13 experiments, 4 that are noticeably different will be presented in the following of this section: the experiments B, D, E and J.

5.3.2. Presentation of selected cases

If each of the following four cases, nine AIS contacts will be assessed. In the case of experiment B, the contacts come from nine different vessels, therefore the contacts and their order are not related to one another, whereas in the cases of experiments D, E and J, the nine contacts represent nine consecutive AIS messages from the same MMSI, therefore supposedly coming from the same vessel and constituting a time series. Those nine messages will be assessed, whether they are actual contacts or syntetised ones for the need of the experiment.

Experiment B: A vessel displays an identity which is non compliant with our fleet register

This experiment deals with a case where the values extracted from messages sent by a vessel are not in accordance with some other data, for instance fleet register, that might be available. This experiment requests a fleet register dataset, and more particularly a fleet register which has common data fields with the AIS, to that the vessels can be individuated. Most matches will be performed using the MMSI number or the call sign of the vessel. Generic comparisons will focus on the name of the vessel, its gross tonnage or its length. In the case of our study we use the ANFR (French National Agency for Frequencies) fleet register, enabling a matching through the call sign and a comparison on two dimensions: the name of the vessel and its dimensions.

As this case involves an external dataset, it is directly linked to scenario-specific flags (described in Section 3.4.2). Integrity is assessed between the fleet register and the AIS datasets,

and the first assessment concerns the fact to actually belong to the fleet register dataset (if it is not the case whereas it should, it will result in the raising of the *f_isNotInFleetRegister* flag), and the second assessment is about the comparison between the values of the two datasets. If an integrity violation is spotted, the flag *f_fleetRegisterConsistency* is raised. Figure 14 displays the process flow for this experiment. As only static AIS information is needed, only messages number 5 are assessed. In order to take into consideration small discrepancies between strings of characters and rounding errors, a distance of 5 have been empirically set for the Levensthein Edit distance assessing the name field and a total difference of 2 meters in both length and width have been considered as the maximal admissible value. Figure 15 shows the verbose version of erroneous messages after they undergone the processing. The number on the left-hand side of the Figure label the nine lines of errors and will be referred later in flag and risk assessment.

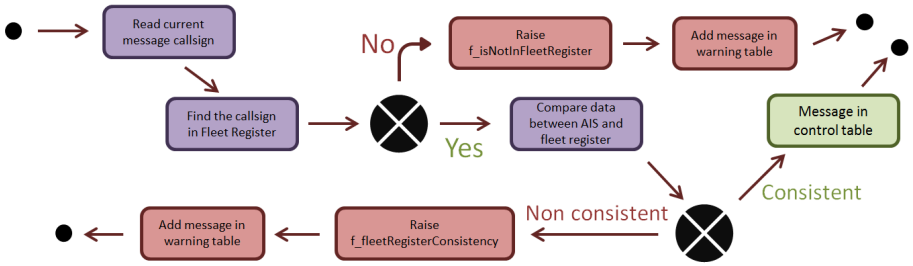

Figure 14: Assessment of fleet register cases

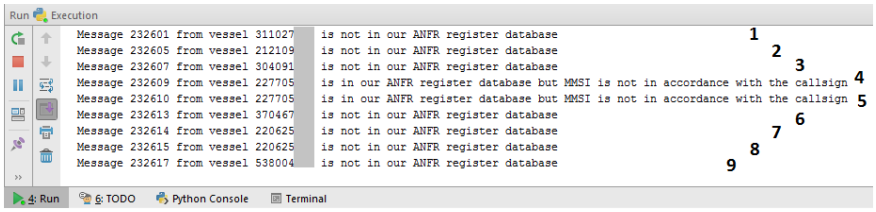

Figure 15: Output of the software in verbose mode

Experiment D: A MMSI number transmits from two different locations at the same time

This scenario consists in the fact to have more than one vessel using the same identity (MMSI number) at the same time. We call this phenomenon ubiquity, and it can be caused by various reasons: a GNSS malfunction, the voluntary or involuntary use of the same identifier without intent to harm, or more probably the identity theft of another vessel (which can happen when a vessel wants to conceal its information, for illegal activities, in case of troubled areas or in order to conceal embargo violation). As an example of this ubiquity case, the experiment consists in the synthesis of 9 points, temporally numbered from

1 to 9 that simulate two different vessels navigating some kilometers apart near the Brest roadstead, sharing the same MMSI field value. As illustrated in the top-right of Figure 16, one of the synthetised vessels has a southwestwards trajectory, exiting the Brest roadstead and the other goes northwards inside the roadstead. The odd-numbered points belong to the first trajectory and the even-numbered one to the second trajectory. The messages are ordered numerically by their timestamp and the interval between two consecutive message does not exceed 5 seconds (therefore making the fact that all those messages could have been produced by the same physical station impossible).

Figure 16: Data contacts for experiments D, E and J are respectively shown in the top-right, bottom-left and bottom-right corners. The top-left corner shows the location of the experiment at a larger scale. The dotted area is the Atlantic Ocean, the grey area the landmass, the light-blue area the Brest roadstead and the light-red area the port of Brest

Experiment E: A vessel transmits from a landmass

This experiment takes place in the frame of cases of a wrong position for a vessel, *i.e.* the fact for a vessel to display a position which is either out of the scope of possible values (*i.e.* latitude in [-90,90] and longitude in [-180,180]), or the fact for a vessel to send a message while being located on a landmass (bodies of water such as rivers or lakes excluded). In the frame of this experiment, a set of 9 points has been synthetised, which starts in the Brest roadstead and goes North, crossing the restricted military area and finishing on land (the trajectory is displayed in the bottom-left corner of Figure 16). Kinematic values such as the speed, the heading and the distances between the points have been set consistently so that no flag related on kinematic issues would be raised.

Experiment J: A vessel suddenly appears in an unexpected area

This experiment is part of a larger case involving various spontaneous appearances. In order to assess the normality of the location of the first contact for a vessel, areas of high and low probability of vessel appearance, taking into consideration the local antenna and the landmass elevation that can constitute masks to signal transmission. This study can be conducted on coastal antennas, which have a coverage area. In those cases, the first contact from an arriving vessel is expected to be located around the theoretical range of the vessel, or in the port if the vessel is outgoing.

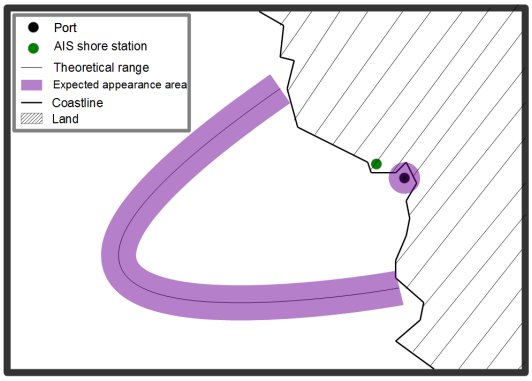

Figure 17: Location of expected appearance areas

Figure 17 shows the locations where we expect a vessel to transmit its first AIS contact that will be received by this station. In order to perform this experiment, a set of 9 synthetic messages have been set, corresponding to a simple eastwards trajectory located in the Brest roadstead, in a location where a first contact with the Brest AIS coastal station is not expected to happen. The nine messages are shown in the bottom-right corner of Figure 16, where the blue points are located in the green geometry of the Brest roadstead, in front of the red geometry of the Brest port. Kinematic values such as the speed, the heading and the distances between the points have been set consistently so that no flag related on kinematic issues would be raised.

5.4. Result Analysis

The four experiments presented in section 5.3.2 provide flags and trigger risks, according to the deterministic relations that rule this study. Those flags and those risks are presented in Table 6. Throughout the four scenarios, amongst the implemented flags, the ones that have been triggered at least once are summarised in Table 7.

As various flag combinations trigger different risks, the same scenario can lead to various risk levels displayed to the user in charge of the monitoring of the traffic. Indeed, the nature of the vessel is of paramount importance in the assessment of the risk, as various vessel natures will lead in different situations at sea. Table 8 shows the various risks levels

Exp. B	1	2	3	4	5	6	7	8	9
f_isNotInFleetRegister	√	√	√			√	√	√	√
f_fleetRegisterConsistency				√	√				
Collision									
Grounding									
Illegal Fishing				√	√				
Piracy - Terrorism	√	√	√	√	√	√	√	√	√
Illegal Transportation	√	√	√	√	√	√	√	√	√
Exp. D	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_ubiquity		√	√	√	√	√	√	√	√
f_trajectory		√	√	√	√	√	√	√	√
f_nextPoint		√	√	√	√	√	√	√	√
Collision		√	√	√	√	√	√	√	√
Grounding									
Illegal Fishing	√	√	√	√	√	√	√	√	√
Piracy - Terrorism	√	√	√	√	√	√	√	√	√
Illegal Transportation	√	√	√	√	√	√	√	√	√
Exp. E	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_restrictedArea				√	√				
f_isInLand						√	√	√	√
f_coastProximity					√				
f_headingTowardsPort	√	√	√						
Collision	√	√	√						
Grounding					√				
Illegal Fishing	√					√	√	√	√
Piracy - Terrorism	√	√	√	√	√	√	√	√	√
Illegal Transportation	√					√	√	√	√
Exp. J	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
Collision									
Grounding									
Illegal Fishing	√								
Piracy - Terrorism	√								
Illegal Transportation	√								

Table 6: For each of the four experiments presented, the flags and the risks activated (√) are displayed, for each point of the series of nine AIS contacts

f_isNotInFleetRegister	Raised when the vessel cannot be found in the available fleet registers
f_fleetRegisterConsistency	Raised when the vessel transmits data that are not consistent with data retrieved from available fleet registers
f_suddenapp	Raised when a vessel appears in an area from which it is not expected to receive the first message thereof
f_ubiquity	Raised when messages from a single MMSI number are received at the same time from different locations
f_trajectory	Raised when the whole trajectory of a vessel is not consistent
f_nextPoint	Raised when the position data of a vessel are not in line with the position data, the kinematic data and the timestamp of the former message received from this vessel
f_restrictedArea	Raised when the vessel is located in an area for which navigation is restricted
f_isInLand	Raised when the vessel transmits from a location on a landmass
f_coastProximity	Raised when the vessel is in the neighbourhood of the coastline and heads towards the shore
f_headingTowardsPort	Raised when the vessel is moving towards a port registered in an available port list

Table 7: Short description of all the flags presented in Table 6

computed in the case of experiment E, taking into consideration the vessel family. The variability of the results according to the vessel type is shown in Figure 18.

In the case of collision, the nature of the collided object matters as well. In this case we assume that the considered vessel is a tanker carrying hazardous goods (colliding with a fishing vessel for the sake of the collision case). Also, if any vessel type is not known, the worst case result applies.

Human dimension	1	2	3	4	5	6	7	8	9
Collision	3	3	3						
Grounding					2				
Illegal Fishing	1					1	1	1	1
Piracy - Terrorism	4	4	4	4	4	4	4	4	4
Illegal Transportation	2					2	2	2	2
Infrastructure dimension	1	2	3	4	5	6	7	8	9
Collision	4	4	4						
Grounding					3				
Illegal Fishing	1					1	1	1	1
Piracy - Terrorism	2	2	2	2	2	2	2	2	2
Illegal Transportation	3					3	3	3	3
Environment dimension	1	2	3	4	5	6	7	8	9
Collision	4	4	4						
Grounding					4				
Illegal Fishing	1					1	1	1	1
Piracy - Terrorism	4	4	4	4	4	4	4	4	4
Illegal Transportation	2					2	2	2	2

Table 8: For each of the three dimensions of the risk, risk levels are computed when the corresponding risk is activated for this point (*cf.* part "*Exp. E*" of Table 6). Vessel type is fixed to cargo vessel

The program is able to output a variety of scores according to the needs of the final user. The impossibility to output a single value to take into consideration the complexity of the real-world situation and the various interest at stake naturally pushed towards the use of multiple outputs with respect to the vessel type, the risk considered and the dimension of interest.

In this program, each data contact is treated separately and given individual risk levels. Although individual, the computed risk values might vary with respect to the environment (*i.e.* the other messages) as some components (*e.g.* flags) are computed on time series and the computation of the same item of the same message might end up with different results according to the set of messages assessed. This is not an issue as we consider this study as a focus on datasets (*i.e.* complete sets of messages) and not on messages taken individually.

As in some cases, the interest of the user can lie on various vessel types, dimensions or risks and the notion of a specific level for a vessel type, a dimension and a risk can be extended to a risk level for a whole encompassing one or several vessel types, one or several risks and one or several dimensions. In this case, the easiest way to assign a risk level is to take the maximal risk level of all sub-combinations. More complex combinations can be

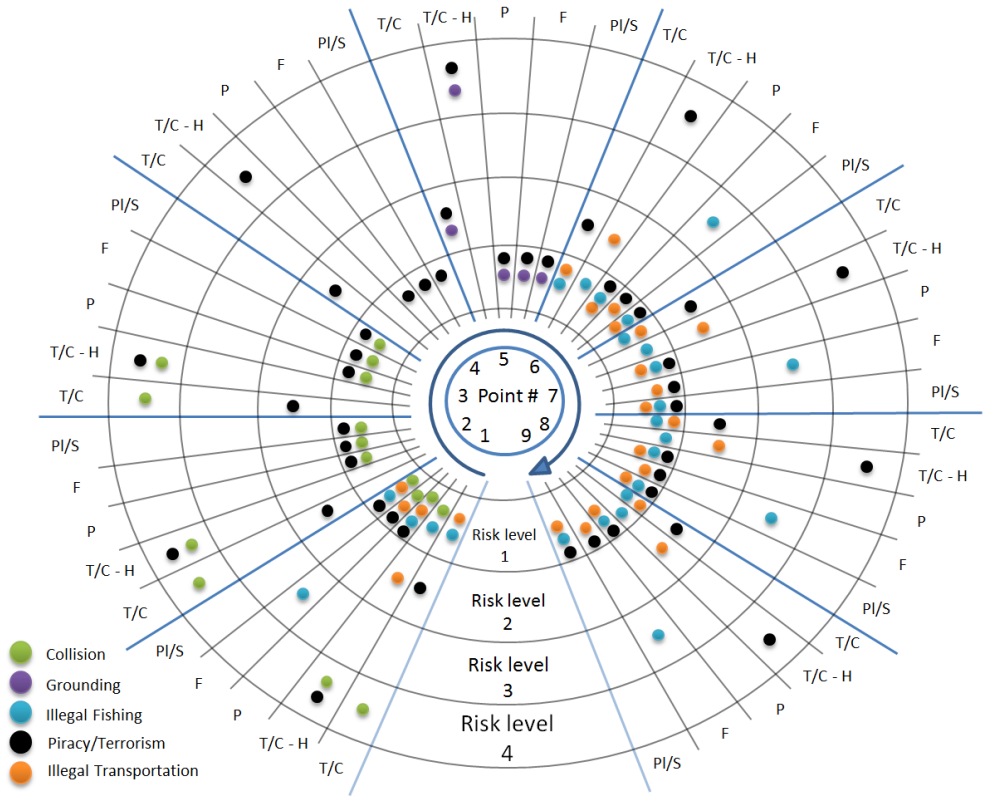

Figure 18: Graphical representation of the risk levels computed for each of the 9 points when the corresponding risk is activated for this point (*cf.* part "*Exp. E*" of Table 6), that vary accordingly with the type of risk (coloured disks) and the vessel type. Risk levels are figured in concentric rings. T/C is for cargo vessel, T/C - H for cargo vessel carrying hazardous goods, P for passenger vessel, F for fishing vessel and Pl/S for pleasure and service vessels. For the sake of simplicity in this representation, collisions are intended with two vessels of the same type, although a risk level is computed for each possible pair of vessel types

considered in specific cases, such as the mean, the median or some quantile-based threshold, according to the number of possible cases.

As shown in Figure 18, the vessel type is important for the determination of the right level of risk, as the analysis of the same messages, resulting in the same activated risks, will be assigned various risk levels according to the type of the vessel of interest. These variations can more particularly be seen in the case of the T/C and T/C - H vessel types, which are the only ones to display level 4 alerts, for collision (points 1, 2 and 3), piracy/terrorism (all points) and grounding (point 5). Furthermore, a level 3 illegal fishing is triggered for fishing vessels only (point 1 and 6 to 9). In this respect, the proper definition of various vessel types is important as it provides widely varying results in the risk analysis.

As shown by Table 8, the dimension of interest is important for the determination of the right level of risk, as the same activated risks from the same message will result in various risk level assignments with respect to the dimension of interest in the study. These variations can more particularly be seen in the piracy/terrorism risk for which the human

and environmental risks are maximal, but the infrastructure risk is moderate. The values of the grounding risk in point 5 varies from a moderate human risk, goes through an important infrastructure risk and ends in a maximal environmental risk. In our study, we considered a T/C - H vessel, which explains the high environmental value, but those values all vary with respect to the vessel type.

6. Discussion and conclusions

6.1. Discussion on results and limitations of the approach

Our approach has been validated by a prototype, with the support of a variety of scenarios that intend to mimic the issues that a vessel can deal with in the case of a falsification or a cyberattack. The scenarios are different so that to cover a wide spectrum of cases but the contexts and the risks are similar.

An interface, aiming at offering the people in charge of maritime monitoring a comprehensive overview of the maritime situation in their area of watch, has been developed and based on the results of our analysis. The result of the flag analysis, stored in a dedicated table in the database, is the input for the visualisation interface. This feature displays all the vessels for which at least one flag has been raised on a map. The vessels are shown in different colours according to their vessel type and the user has several options, being able to display all the vessels in the neighbourhood of the selected vessel or the elements relative to the vessel itself. The user is also able to discard the vessel if he/she judges that the raising of the flag does not demonstrate a situation worthy to be looked after. The corresponding entry in the database is not erased from the table, but is tagged as discarded and is not shown on the screen any longer.

This information system has been made as a decision-support tool for the user, which could be a private ship-owning company, but more probably a state-established civilian or military facility in charge of the monitoring of the maritime traffic off the coasts of the country and in inland waters. The purpose is to bring to people in charge of maritime traffic supervision to a concrete understanding of the situation, and to decrease their cognitive load. As the flags stand for maritime possible issues, the program helps in presenting those issues is a optimised way for the people in charge, however it remains the duty of the personnel to determine the normality or the abnormality of a situation, to consider a case as particularly hazardous or to discard it.

This work uses description logics, that enables the implementation of a rule-based inference system to assess data quality. Item computation and risk level assessment are straightforward and strictly follow the rules set by the domain experts. Thus, the approach suffers from the flaws of deterministic approaches, and if the data processing method enables a fast processing of data through True and False values, the uncertain nature of some pieces of information is not taken into consideration. The use of probabilistic models would probably

enable a more precise modelling of the domain of interest. However, such an implementation is not straightforward and would require the involvement of a number of domain experts. The very nature of cyberthreats would yet remain an obstacle, if not the main impediment of the setting of a probabilistic model, as few cases are reported, and the reported cases might be biased for business interest, or second-handed. Therefore, the building of a knowledge base using machine learning methods is an important challenge.

Besides the very nature of the approach, the one that was chosen has some intrinsic limitations linked to the number and nature of computational flags, maritime risks, risk levels and considered vessel types. An increase of the number of flags, linked either to a deeper understanding and use of binary fields of AIS messages or to the extensive use of contextual databases is to be encouraged, as it will foster a more complex and precise understanding of the maritime situation, bringing a more accurate comprehension of the risks at stake. However, those additional implementations are time-consuming and the real-time nature of the processing must be safeguarded.

A question that can arise is whether or not a more complete set of maritime risks shall be used. In our study, we focused on five families extracted from our study of the maritime environment and the risks linked to the human uses of the oceans. The fact to expand the list of risks will allow a more precise understanding of the maritime situation. However, it brings several drawbacks: on the one hand, it might be difficult for the program to discriminate between two risks that would have similar patterns, and on the other hand the multiplication of possible outcomes might have a negative impact on the person in charge of traffic monitoring as it could be too directive and elude the step of the human understanding of the situation.

The problem of the scale of risk levels also arises. In our study, we choose a 4-level scale, in accordance with the common information sharing environment. The gradation of the risks has its importance, as the right amount of levels must be chosen, in accordance with several factors such as the possibility for the events to cover a wide spectrum of gravity. The difference between two levels must be high enough to imply a significant difference between the levels, with significant differences in actions to be taken for the operator.

The fact to take into consideration different vessel types is important, as the size, the purpose and the manoeuvrability of the vessels vary considerably from one vessel type to another. The Automatic Identification System has, in its technical specifications, 58 different possible types. However, some of those vessel types are so close that it would be unreasonable to consider treating them separately. Thus, for the sake of simplicity, families of vessel types were defined. It is questionable whether the division in four vessel types we did based on usage and vessel size is enough to cover the diversity and complexity of maritime navigation. This choice was made as a first simple draft, enabling a first step of diversification, but yet to be improved with the help of maritime experts.

6.2. Conclusions

The work presented in this paper is part of the research in the fields of risk assessment with mobile data, through data integrity and veracity assessment, knowledge discovery and data science, with a domain exemplification in maritime situational awareness and maritime safety in the frame of cyber risks. The operational issue is a consequence of research questions raised after the demonstration that maritime navigation systems were prone to attacks, and an holistic understanding of data that those systems provide must be achieved. In our use case, a global maritime location system which is intended to provide additional safety to navigation as well as useful information to the surroundings vessels and coastal stations was easily falsified. The objective was then to propose a methodology that points out cases of non-genuine data and provide a risk assessment to those cases.

In order to do so, an approach based on the data quality dimensions was studied. Indeed, as information systems are data-based, they natively have data quality dimensions available to assess them. More precisely in the diversity of data quality dimensions, integrity was discriminated as particularly important for a reliable assessment of data-based systems, and the assessment methodology is based on the development of integrity-based features assessing data veracity. The approach we propose has been prototyped and experimented to fit the requirements of a near-real-time automated data processing system.

As such an integrity-based assessment requires a profound understanding of the mechanisms that rule the system in question, a thorough analysis of the system have been performed, taking into consideration the primary purpose of the system and the uses that have later appeared in order to understand the wills of the people which wrote the specifications. The technical part of the system was studied as it provides precious information about the inner construction thereof, and the data part of the system was scrutinised in order to find any kind of combination of pieces of information that could result in an integrity breach.

From those integrity study results, and with the addition of non-system data such as fleet register data or navigation zones, flags were created and then were converted into risks using an expert set of rules, and the risks themselves, divided in five main areas of interest, are given a risk level, computed from another set of expert rules. The system considers here the risk to be present or absent, without nuances. In this respect, the system is realising clusters of risk and non-risk cases, according to the outcome of the deterministic approach.

The purpose of this assessment being to point out data with issues with explicit statements, enabling the displaying of those vessels in a interactive map, allowing the user to concentrate on those vessels and use visual analytics tools to find a proper solution to the problem displayed, by reducing the cognitive load and focusing on anomalous cases.

In the frame of this work, expert knowledge from the fields of civil activities such as merchant navy and military activities has been involved, with the collaboration of officers of the French navy and cadets of the French naval academy, for a total of 6 individuals that

were involved in 4 different steps of the methodological process, and with the collaboration of Cerema, a French cluster of public experts. This heterogeneous group of experts provided support for the risk analysis of the AIS (Section 4.2), the definition of credible maritime situations, the setting of thresholds in data analysis (Section 3.2), the elaboration of falsification cases which have been implemented and presented in this paper with the establishment of risk indicators including risk combination, risk associations and risk levels (Section 4.3), and provided guidance for the needs of the final use and the efficient display of maritime risks (Section 5.1).

Although the approach has been design in an iterative way with professional domain experts, a limitation of this work is that no tests with operational personnel were performed, which would be necessary for an operational validation. However, this paper validated the approach in terms of performance or response quality, in which all inventoried falsification cases are linked to their corresponding detectors, enabling the assessment of the scenarios presented in Section 5.3.

A next step in this research question would be to be able to get rid of the deterministic approach and involve enough expert knowledge to build a solid knowledge base that would enable the probabilistic processing of such risk assessment. This would enable to bring the risk assessment to a qualitative level, whereas it stays at a quantitative level with such a deterministic approach. The absence of reliable base on which build a knowledge implies the only use of expert knowledge, in several fields, and the assessment of whether or not a knowledge base would meet the requirements to be used in a probabilistic risk assessment is a research question on its own. Nevertheless, such studies, if successfully achieved, would be another step forward in the support of operators for decision-making at sea.

Acknowledgments

The research presented in this paper has been supported by The French National Research Agency (ANR) and co-funded by DGA (Directorate General of Armaments) under reference ANR-14-CE28-0028, in the frame of the DéAIS project, labelled by French clusters Pôle Mer Bretagne Atlantique and Pôle Mer Méditerranée. The authors would express their gratitude towards all the experts involved in this study, and particularly towards lieutenant Erwan for his stay with the naval academy research institute and towards Thibaut Eude for the valuable knowledge he continuously provided during his 3-years stay in MINES ParisTech.

References

[1] W. Toumsi, H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks, Computers & Security 72 (2018) 212–233. doi:10.1016/j.cose.2017.09.001.

[2] T. Rid, B. Buchanan, Attributing cyber attacks, Journal of Strategic Studies 38 (2015) 4–37. doi:10.1080/01402390.2014.977382.

[3] T. J. Holt, M. Stonhouse, J. Freilich, S. M. Chermak, Examining ideologically motivated cyberattacks performed by far-left groups, Terrorism and Political Violence (2019). doi:10.1080/09546553.2018.1551213.

[4] E. Amir, S. Levi, T. Livne, Do firms underreport information on cyber-attacks? evidence from capital markets, Review of Accounting Studies 23 (3) (2018) 1177–1206. doi:10.1007/s11142-018-9452-4.

[5] L. Maglaras, M. A. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, S. Rallis, Threats, countermeasures and attribution of cyber attacks on critical infrastructures, EAI Endorsed Transactions on Security and Safety 5 (16) (2018). doi:10.4108/15-10-2018.155856.

[6] A. Arabo, Cyber security challenges within the connected home ecosystem futures, Procedia Computer Science 61 (2015) 227–232. doi:10.1016/j.procs.2015.09.201.

[7] G. Comert, J. Pollard, D. M. Nicol, K. Palani, B. Vignesh, Modeling cyber attacks at intelligent traffic signals, Transportation Research Record 2672 (1) (2018) 76–89. doi:10.1177/0361198118784378.

[8] J. Petit, S. E. Shladover, Potential cyberattacks on automated vehicles, IEEE Transactions on Intelligent Transportation Systems 16 (2) (2015) 546–556. doi:10.1109/TITS.2014.2342271.

[9] M. Waheed, M. Cheng, A system for real-time monitoring of cybersecurity events on aircraft, in: Proceedings of the IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), 2017.

[10] B. Costé, C. Ray, G. Coatrieux, Trust measurement in an information system for the sake of security, Advances in Knowledge Discovery and Management (AKDM) 8 (2019) 159–181.

[11] C.-S. Yang, Maritime shipping digitalization: Blockchain-based technology applications, future improvements, and intention to use, Transportation Research Part E: Logistics and Transportation Review 131 (2019) 108–117. doi:10.1016/j.tre.2019.09.020.

[12] J. Bhatti, T. E. Humphreys, Hostile control of ships via false gps signals: Demonstration and detection, NAVIGATION, Journal of The Institute of Navigation 64 (1) (2017) 51–66.

[13] L. Lecornu, J. Montagner, J. Puentes, Reliability evaluation of incomplete AIS trajectories, in: Proceedings of the COST MOVE Workshop on Moving Objects at Sea, 2013.

[14] P. Last, M. Hering-Bertram, L. Linsen, How automatic identification system (AIS) antenna setup affects AIS signal quality, Ocean Engineering 100 (2015) 83–89. doi:10.1016/j.oceaneng.2015.03.017.

[15] A. Harati-Mokhtari, A. Wall, P. Brooks, J. Wang, Automatic Identification System (AIS): A Human Factors Approach, Journal of Navigation 60 (3) (2007) 373–389.

[16] F. Katsilieris, P. Braca, S. Coraluppi, Detection of malicious AIS position spoofing by exploiting radar information, in: Proceedings of the 16th International Conference on Information Fusion, 2013.

[17] gCaptain, Ais problems revealed in East China Sea, published the 27 December 2018, by Laura Kovary (2018).
URL https://gcaptain.com/ais-problems-revealed-in-east-china-sea/

[18] Wired, When a tanker vanishes, all the evidence points to Russia, published the 21 September 2017, by Matt Burgess (2017).
URL https://www.wired.co.uk/article/black-sea-ship-hacking-russia

[19] Llyodslist, Seized UK tanker likely 'spoofed' by Iran, published the 16 August 2019, by Michelle Wiese Bockmann (2019).
URL https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran

[20] C. Kooij, M. Loonstijn, R. Hekkenberg, K. Visser, Towards autonomous shipping: Operational challenges of unmanned short sea cargo vessels, in: P. Kujala, L. Lu (Eds.), Marine Design XIII, 2018, pp. 871–880.

[21] J. Montewka, K. Wróbel, E. Heikkilä, O. Valdez-Banda, F. Goerlandt, S. Haugen, Challenges, solution proposals and research directions in safety and risk assessment of autonomous shipping, in: Proceedings of PSAM 14 - Probabilistic Safety Assessment and Management Conference, 2018.

[22] A. Komianos, The autonomous shippig era. operational, regulatory, and quality challenges, TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation 12 (2) (2018) 335–348. doi:10.12716/1001.12.02.15.

[23] M. Hadzagic, A.-L. Jousselme, Contextual anomalous destination detection for maritime surveillance, in: M. Vespe, F. Mazzarella (Eds.), Proceedings of the Maritime

Knowledge Discovery and Anomaly Detection Workshop, JRC Conference and Workshop Reports, 2016, pp. 62–65.

[24] H. Yaghoubi Shahir, U. Glasser, N. Nalbandyan, H. Wehn, Maritime Situation Analysis: A Multi-vessel Interaction and Anomaly Detection Framework, in: Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, IEEE, 2014, pp. 192–199. doi:10.1109/JISIC.2014.36.

[25] G. Pallotta, M. Vespe, K. Bryan, Vessel Pattern Knowledge Discovery from AIS Data: A Framework for Anomaly Detection and Route Prediction, Entropy 15 (6) (2013) 2218–2245. doi:10.3390/e15062218.

[26] C.-H. Chen, L. P. Khoo, Y. T. Chong, X. F. Yin, Knowledge discovery using genetic algorithm for maritime situational awareness, Expert Systems with Applications 41 (6) (2014) 2742–2753. doi:10.1016/j.eswa.2013.09.042.

[27] A. Alessandrini, M. Alvarez, H. Greidanus, V. Gammieri, V. Fernandez Arguedas, F. Mazzarella, C. Santamaria, M. Stasolla, D. Tarchi, M. Vespe, Mining vessel tracking data for maritime domain applications, in: Proceedings of the 1st International ICDM Workshop on Maritime Domain Data Mining (MDDM 2016), Institute of Electrical and Electronics Engineers - IEEE, 2016, pp. 361–367. doi:10.1109/ICDMW.2016.20.

[28] S. Wang, R. Yan, X. Qu, Development of a non-parametric classifier: Effective identification, algorithm, and applications in port state control for maritime transportation, Transportation Research Part B: Methodological 128 (2019) 129–157. doi:10.1016/j.trb.2019.07.017.

[29] L. Zhang, Q. Meng, T. Fang Fwa, Big ais data based spatial-temporal analyses of ship traffic in singapore port waters, Transportation Research Part E: Logistics and Transportation Review 129 (2019) 287–304. doi:10.1016/j.tre.2017.07.011.

[30] F. Goerlandt, J. Montewka, Maritime transportation risk analysis: Review and analysis in light of some foundational issues, Reliability Engineering & System Safety 138 (2015) 115–134. doi:10.1016/j.ress.2015.01.025.

[31] J. R. W. Merrick, R. Van Dorp, Speaking the truth in maritime risk assessment, Risk Analysis 26 (1) (2006) 223–237. doi:10.1111/j.1539-6924.2006.00708.x.

[32] M. Przywarty, Models of ship-ship collision. qualitative assesment, Scientific Journals of the Maritime University of Szczecin 18 (90) (2009) 128–135.

[33] F. Kaneko, Models for estimating grounding frequency by using ship trajectories and seabed geometry, Ships and Offshore Structures 7 (1) (2012) 87–99. doi:10.1080/17445302.2011.594572.

[34] J. Ylitalo, Modelling marine accident frequency, Dissertation, Aalto University, School of Science and Technology, Faculty of Information and Natural Sciences (2010).

[35] P. Silveira, A. Teixeira, C. G. Soares, Use of AIS Data to Characterise Marine Traffic Patterns and Ship Collision Risk off the Coast of Portugal, Journal of Navigation 66 (06) (2013) 879–898. doi:10.1017/S0373463313000519.

[36] E. Klemola, J. Kuronen, J. Kalli, T. Arola, M. Hanninen, A. Lehikoinen, S. Kuikka, P. Kujala, U. Tapaninen, A cross-disciplinary approach to minimising the risks of maritime transport in the gulf of finland, World Review of Intermodal Transportation Research 2 (4) (2009) 343–363. doi:10.1504/WRITR.2009.026212.

[37] J.-F. Balmat, F. Lafont, R. Maifret, N. Pessel, A decision-making system to maritime risk assessment, Ocean Engineering 38 (1) (2011) 171–176. doi:10.1016/j.oceaneng.2010.10.012.

[38] A. Bouejla, X. Chaze, F. Guarnieri, A. Napoli, Bayesian Networks in the Management of Oil Field Piracy Risk, in: C. Brebbia (Ed.), 8th International Conference on Simulation in Risk Analysis and Hazard Mitigation, WIT Press, 2012.

[39] Y. Huang, L. Chen, P. Chen, R. R. Negenborn, P. van Gelder, Ship collision avoidance methods: State-of-the-art, Safety Science 121 (2020) 451–473. doi:10.1016/j.ssci.2019.09.018.

[40] P. Chen, Y. Huang, J. Mou, P. van Gelder, Probabilistic risk analysis for ship-ship collision: State-of-the-art, Safety Science 117 (2019) 108–122. doi:10.1016/j.ssci.2019.04.014.

[41] X. Qu, Q. Meng, L. Suyi, Ship collision risk assessment for the Singapore Strait, Accident Analysis & Prevention 43 (6) (2011) 2030–2036. doi:10.1016/j.aap.2011.05.022.

[42] Z. Liu, Z. Wu, Z. Zheng, A novel framework for regional collision risk identification based on ais data, Applied Ocean Research 89 (2019) 261–272. doi:10.1016/j.apor.2019.05.020.

[43] M. Perkovic, L. Gucma, M. Przywarty, M. Gucma, S. Petelin, P. Vidmar, Nautical Risk Assessment for LNG Operations at the Port of Koper, Strojniški vestnik – Journal of Mechanical Engineering 58 (10) (2012) 607–613. doi:10.5545/sv-jme.2010.265.

[44] T. Chai, J. Weng, D.-q. Xiong, Development of a quantitative risk assessment model for ship collisions in fairways, Safety Science 91 (2017) 71–83. doi:10.1016/j.ssci.2016.07.018.

[45] Z. Liu, Z. Wu, Z. Zheng, A novel model for identifying the vessel collision risk of anchorage, Applied Ocean Research 98 (2020). doi:10.1016/j.apor.2020.102130.

[46] Y. Wang, J. Zhang, X. Chen, X. Chu, X. Yan, A spatial–temporal forensic analysis for inland–water ship collisions using AIS data, Safety Science 57 (2013) 187–202. doi:10.1016/j.ssci.2013.02.006.

[47] O. S. Ulusçu, B. Özbaş, T. Altiok, I. Or, Risk Analysis of the Vessel Traffic in the Strait of Istanbul, Risk Analysis 29 (10) (2009) 1454–1472. doi:10.1111/j.1539-6924.2009.01287.x.

[48] L. Huang, Y. Wen, X. Geng, C. Zhou, C. Xiao, Integrating multi-source maritime information to estimate ship exhaust emissions under wind, wave and current conditions, Transportation Research Part D: Transport and Environment 59 (2018) 148–159. doi:10.1016/j.trd.2017.12.012.

[49] B. Dragović, E. Tzannatos, V. Tselentis, R. Meštrović, M. Škurić, Ship emissions and their externalities in cruise ports, Transportation Research Part D: Transport and Environment 61 (2018) 289–300. doi:10.1016/j.trd.2015.11.007.

[50] S. B. Kotsiantis, I. D. Zaharakis, P. E. Pintelas, Machine learning: a review of classification and combining techniques, Artificial Intelligence Review 26 (3) (2006) 159–190. doi:10.1007/s10462-007-9052-3.

[51] F. Baader, I. Horrocks, U. Sattler, Description Logics, Springer-Verlag Berlin, 2004, pp. 3–28.

[52] F. Goerlandt, J. Montewka, A framework for risk analysis of maritime transportation systems: A case study for oil spill from tankers in a ship–ship collision, Safety Science 76 (2015) 42–66. doi:10.1016/j.ssci.2015.02.009.

[53] J. Nordström, F. Goerlandt, J. Sarsama, P. Leppänen, M. Nissilä, P. Ruponen, T. Lübcke, S. Sonninen, Vessel TRIAGE: A method for assessing and communicating the safety status of vessels in maritime distress situations, Safety Science 85 (2016) 117–129. doi:10.1016/j.ssci.2016.01.003.

[54] C. Guedes Soares, A. Teixeira, Risk assessment in maritime transportation, Reliability Engineering & System Safety 74 (3) (2001) 299 – 309. doi:10.1016/S0951-8320(01)00104-1.

[55] IMO, International Convention for the Safety of Life at Sea, 160 pages, 2003 update (2003).

[56] R. Kerbiriou, L. Lévêque, A. Rajabi, A. Serry, The automatic identification system (ais) as a data source for studying maritime traffic, in: Proceedings of the International Marine Science Conference, 2017, pp. 1–17.

[57] EMSA, Emsa facts and figures 2018, Annual activity report., European Maritime Safety Agency (2019).

[58] F. Natale, M. Gibin, A. Alessandrini, M. Vespe, A. Paulrud, Mapping Fishing Effort through AIS Data, PLOS ONE 10 (6) (Jun. 2015). doi:10.1371/journal.pone.0130746.

[59] J. K. Tunaley, Utility of Various AIS Messages for Maritime Awareness, in: 8th ASAR Workshop, Longueuil, Canada, 2013.

[60] M. Lundkvist, L. Jakobsson, R. Modigh, Automatic identification system (ais) and risk-based planning of hydrographic surveys in swedish waters, in: Proceedings of the FIG Working Week 2008, 2008.

[61] C. Iphar, B. Costé, A. Napoli, C. Ray, R. Devillers, Integrity and Trust of Geographic Information, Wiley, 2019. doi:10.1002/9781119507284.ch4.

[62] M. Balduzzi, K. Wilhoit, A. Pasta, A Security Evaluation of AIS, Tech. rep., Trend Micro (2014).

[63] P. A. McGillivary, K. D. Schwehr, K. Fall, Enhancing ais to improve whale-ship collision avoidance and maritime security, in: Proceedings of the OCEANS 2009 Biloxi Conference, IEEE, 2009.

[64] T. Eriksen, G. Høye, B. Narheim, B. J. Meland, Maritime traffic monitoring using a space-based AIS receiver, Acta Astronautica 58 (10) (2006) 537–549. doi:10.1016/j.actaastro.2005.12.016.

[65] Windward, AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea, Tech. rep., Windward (2014).

[66] M. Balduzzi, A. Pasta, K. Wilhoit, A security evaluation of AIS Automated Identification System, in: Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC'14, ACM, New York, NY, USA, 2014, pp. 436–445. doi:10.1145/2664243.2664257.

[67] L. Chang, Study of AIS communication protocol in VTS, in: 2nd International Conference on Signal Processing Systems, IEEE, 2010, pp. 168–171. doi:10.1109/ICSPS.2010.5555594.

[68] C. Iphar, C. Ray, A. Napoli, Data integrity assessment for maritime anomaly detection, Expert Systems With Applications 147 (2020). doi:10.1016/j.eswa.2020.113219.

[69] M. Riveiro, G. Pallotta, M. Vespe, Maritime anomaly detection: A review, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 8 (4) (2018). doi:10.1002/widm.1266.

[70] J. Roy, M. Davenport, Exploitation of maritime domain ontologies for anomaly detection and threat analysis, in: Proceedings of the 2010 International Waterside Security Conference (WSS), IEEE, 2010. doi:10.1109/WSSC.2010.5730278.

[71] J. Roy, Anomaly detection in the maritime domain, in: C. S. Halvorson, D. Lehrfeld, T. T. Saito (Eds.), Optics and Photonics in Global Homeland Security IV, Vol. 6945 of SPIE Proceedings, 2008. doi:10.1117/12.776230.

[72] G. Spiliopoulos, K. Chatzikokolakis, D. Zissis, E. Biliri, D. Papaspyros, G. Tsapelas, S. Mouzakitis, Knowledge extraction from maritime spatiotemporal data: An evaluation of clustering algorithms on big data, in: Proceedings of the 2017 IEEE International Conference on Big Data (BIGDATA), 2017, pp. 1682–1687. doi:10.1109/BigData.2017.8258106.

[73] M. Zocholl, C. Iphar, M. Pitsikalis, A.-L. Jousselme, A. Artikis, C. Ray, Evaluation of maritime event detection against missing data, in: Proceedings of the 12th Quality of Information and Communications Technology (QUATIC), 2019, pp. 273–288.

[74] C. Iphar, A. Napoli, C. Ray, E. Alincourt, D. Brosset, Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety, in: T. B. Lesley Walls, Matthew Revie (Ed.), Proceedings of the ESREL 2016 Conference, Taylor & Francis, 2016, pp. 606–613.

[75] ISO, Information security management, International Standisation Organisation, norm ISO 27001 (2013).
URL https://www.iso.org/isoiec-27001-information-security.html

[76] ISO, Information technology - security techniques - information security risk management, International Standisation Organisation, norm ISO 27005 (2018).
URL https://www.iso.org/standard/75281.html

[77] ISO, Risk management, International Standisation Organisation, norm ISO 31000 (2018).
URL https://www.iso.org/iso-31000-risk-management.html

[78] C. Ray, C. Iphar, A. Napoli, R. Gallen, A. Bouju, DeAIS project: Detection of AIS Spoofing and Resulting Risks, in: Proceedings of the OCEANS 2015 Genova Conferece, IEEE, 2015. doi:10.1109/OCEANS-Genova.2015.7271729.

[79] C. Ray, R. Dréo, E. Camossi, A.-L. Jousselme, Heterogeneous integrated dataset for maritime intelligence, surveillance, and reconnaissance (version 0.1), data set. Licence CC-BY-NC-SA-4.0. Zenodo (Feb. 2018). doi:10.5281/zenodo.1167595.

[80] C. Ray, R. Dréo, E. Camossi, A.-L. Jousselme, C. Iphar, Heterogeneous integrated dataset for maritime intelligence, surveillance, and reconnaissance, Data in Brief 25 (2019). doi:10.1016/j.dib.2019.104141.