Formalisation of a data analysis environment based on anomaly detection for risk assessment : Application to Maritime Domain Awareness

Clément Iphar

THÈSE DE DOCTORAT

de l'Université de recherche Paris Sciences et Lettres
PSL Research University

Préparée à MINES ParisTech

Formalisation of a data analysis environment based on anomaly detection for risk assessment – Application to Maritime Domain Awareness

Formalisation d'un environnement d'analyse des données basé sur la détection d'anomalies pour l'évaluation de risques – Application à la connaissance de la situation maritime

École doctorale n°432

SCIENCES DES MÉTIERS DE L'INGÉNIEUR

Spécialité SCIENCES ET GÉNIE DES ACTIVITÉS À RISQUES

COMPOSITION DU JURY :

M. DEVOGELE Thomas
Université de Tours
Président

Mme. JOUSSELME Anne-Laure
OTAN CMRE
Examinateur

M. NAPOLI Aldo
MINES ParisTech
Examinateur

M. PELOT Ronald
Université Dalhousie
Rapporteur

M. PINET François
IRSTEA
Rapporteur

M. RAY Cyril
École Navale
Examinateur

Soutenue par CLÉMENT **IPHAR**
le 22 novembre 2017

Dirigée par **Aldo NAPOLI**
et **Cyril RAY**

À J.

Remerciements

Mes premiers remerciements vont à mes encadrants de thèse, Aldo Napoli et Cyril Ray. Je remercie particulièrement Aldo pour m'avoir guidé durant les premiers mois de la thèse, puis d'avoir su distiller des conseils sur l'évolution de mes travaux ; et de m'avoir permis de présenter ces travaux dans diverses conférences nationales et internationales. Je remercie particulièrement Cyril pour ses précieux conseils dans le domaine de l'informatique, notamment au cours de la dernière année, qui m'ont fait gagner un temps précieux. Enfin, je vous remercie tous deux pour votre grande disponibilité tout au long de ces trois années, depuis l'élaboration de l'état de l'art jusqu'à la rédaction du manuscrit.

Je remercie les membres de mon jury de thèse, Anne-Laure Jousselme pour son attentive relecture du manuscrit, Thomas Devogele pour avoir présidé la soutenance ainsi que Ronald Pelot et François Pinet pour avoir accepté d'être rapporteurs. Mes remerciements vont aussi à Laurent Étienne et Cyril de Runz, pour avoir accepté d'évaluer mes travaux au cours des comités de passage de fin de 1^{ere} et 2^{eme} année, respectivement, et pour m'avoir distillé leurs conseils avisés.

Je remercie tout particulièrement mes parents pour leur inestimable soutien moral, matériel et financier, sans lesquels je n'aurais pas pu entreprendre les mêmes études, et j'ai aussi ici une pensée pour mes grands-parents.

Je remercie grandement le CRC de MINES ParisTech et son directeur Franck Guarnieri pour m'avoir accueilli durant ces trois ans, et pour m'avoir offert des conditions de travail optimales. Merci à Valérie Sanseverino-Godfrin et Éric Rigaud, responsables successifs de la spécialité doctorale Sciences et Génie des Activités à Risque, à Sandrine Renaud, Myriam Lavigne et Samuel Olampi pour leur aide administrative et technique précieuses. Mes remerciements vont aussi à l'IRENav de l'École Navale pour m'avoir accueilli lors de divers séjours, et tout particulièrement à son directeur, Christophe Claramunt. Enfin, je salue tous ceux que j'ai côtoyé durant ces trois ans, et notamment Martin, Thibaut, Diana, Ragheb, Aissame, Yuki, Cécile, Dahlia, Constance, Luisa et Margaux à Sophia et Loïc, Benjamin, Léa, Thibaud et Eulalie à Brest pour leur sympathie.

J'ai également une pensée pour les laboratoires qui m'ont fait découvrir et prendre goût à la recherche pendant mon cursus en école d'ingénieurs à l'École Nationale des Sciences Géographiques, notamment l'Istituto di Radioastronomia de l'institut national d'astrophysique italien, à Bologne. Je remercie tout particulièrement Pierguido Sarti, ainsi que Monia Negusini et Barbara Neri pour avoir su me soutenir et me guider dans ma première expérience de recherche. Je remercie également Pierre Exertier et Agnès Fienga de m'avoir accueilli et encadré au sein du laboratoire Géoazur à Sophia Antipolis.

Une thèse de doctorat n'est que l'aboutissement d'études supérieures, consécutives aux études primaires et secondaires. J'exprime ma gratitude à l'ensemble de mes professeurs qui y ont contribué au sein de l'enseignement public français, à l'école primaire Michelis II, au collège François Villon, au lycée Marcel Pagnol et au lycée Thiers de Marseille, ainsi que les enseignants de l'École Nationale des Sciences Géographiques. Parmi eux, je remercie particulièrement Alain Lhopital, Jean-Luc Ristori, Nathalie Mercier, Nicole Blanc, Anne Henriet, Michèle Jaume et Daniel Huygue pour la qualité de leur enseignement et leurs conseils.

Dans cette liste de remerciements, je ne peux pas oublier Marcelo Bielsa, digne héritier de Raymond Goethals, que je remercie pour nous avoir fait rêver ainsi que l'ensemble des joueurs de l'Olympique de Marseille pour toujours aller droit au but, être à jamais les premiers, et porter haut le maillot bleu et blanc, les couleurs de la ville. ⊕

Enfin, je remercie mes amis pour les moments partagés de détente et de divertissement, tellements importants dans ces années de thèse. La liste ne peut pas ici être exhaustive, mais je pense à Aurélie qui a traversé en même temps que moi l'épreuve de la thèse, Laura, Anthony et Steven pour les soirées au pub et au stade, Aymeric et François pour nos voyages et Jordy pour l'ensemble de son œuvre. Je pense également à Aurore et Julien pour leur amitié, Jérôme pour les nuits (et les journées) parisiennes, Blandine pour m'avoir accueilli dans son Jülich glacial. Mes pensées vont également à Cyril, Alexandre, William, Florence, Sixtine, Valentin, Quentin et Marie pour les bons moments passés ensemble.

Contents

List of Figures

List of Tables

Abbreviations

- **ADS-B**: Automatic Dependent Surveillance-Broadcast
- **AIS**: Automatic Identification System
- **AMVER**: Automated Mutual-Assistance Vessel Rescue System
- **ANFR**: French National Frequency Agency
- **ANSSI**: French National Cybersecurity Agency
- **ASCII**: American Standard Code for Information Interchange
- **CISE**: Common Information Sharing Environment
- **DGNSS**: Differential Global Navigation Satellite System
- **ECDIS**: Electronic Chart Display and Information System
- **EEZ**: Exclusive Economic Zone
- **ENC**: Electronic Navigational Chart
- **EPLRS**: Enhanced Position Location Reporting System
- **EU**: European Union
- **FAO**: Food and Agriculture Organisation
- **GLONASS**: Russian Global Navigation Satellite System
- **GNSS**: Global Navigation Satellite System
- **GPS**: Global Positioning System
- **IHO**: International Hydrographic Organisation
- **IMO**: International Maritime Organisation
- **ITU**: International Telecommunication Union
- **LRIT**: Long-Range Identification and Tracking
- **MDA**: Maritime Domain Awareness
- **MID**: Maritime Identification Digits

- **MMSI**: Maritime Mobile Service Identity
- **MRCC**: Maritime Rescue Coordination Centre
- **MSI**: Maritime Situational Indicator
- **NATO**: North Atlantic Treaty Organisation
- **OWL**: Web Ontology Language
- **POI**: Point of Interest
- **RDF**: Resource Description Framework
- **S&R**: Search and Rescue
- **SAR**: Synthetic Aperture Radar
- **SOG**: Speed Over Ground
- **SOLAS**: Safety Of Life At Sea
- **SOTDMA**: Self-Organised Time Division Multiple Access
- **SQL**: Structured Query Language
- **SSA**: Sea-domain State Action
- **TSS**: Traffic Separation Scheme
- **UN**: United Nations
- **UTC**: Coordinated Universal Time
- **VHF**: Very High Frequency
- **VMS**: Vessel Monitoring System
- **VOS**: Voluntary Observing Ship
- **VRMTC**: Virtual Regional Maritime Traffic Centre
- **VTS**: Vessel Traffic Service
- **W3C**: World Wide Web Consortium

Chapter 1

Introduction

Chapitre 1 : Introduction

Couvrant 71% de la surface de la Terre, l'océan mondial est un élément fondamental de la vie sur Terre et de l'économie du monde, car 90% du transport international de marchandise s'effectue par voie maritime. Les utilisations humaines de l'océan sont diverses (pêche, marine marchande, plaisance, mise en place de ports, d'industries maritimes, chantiers navals, entre autres), et des conventions internationales ont été établies afin de réguler tout ou partie de cet ensemble.

Les Nations Unies ont mis en place diverses organisations internationales telles que l'Organisation maritime internationale, le Tribunal international du droit de la mer ou l'Autorité internationale des fonds marins. Des mesures propres à la sécurité et à la sûreté de la navigation maritime ont dû être édictées du fait de la densité du trafic international. Des systèmes électroniques permettant aux acteurs d'avoir une meilleure évaluation de l'environnement maritime ont été développés. À bord, ces systèmes délivrent des informations sur l'environnement du navire et les présentent de façon graphique alors qu'à terre ces systèmes donnent aux états côtiers la situation maritime au large de leurs côtes et améliorant la connaissance de la situation maritime. L'un de ces système mis en place est le système d'identification automatique (AIS).

Ainsi, des actions telles que l'édiction de nouvelles règlementations peuvent être prises à différents niveaux, de l'échelle d'un port à l'échelle mondiale. En France, l'Action de l'État en Mer a été définie, regroupant les moyens opérationnels existant dans les eaux françaises du monde entier, pour des problématiques environnementales et de défense.

Le système AIS a été mis en place en tant que système d'anticollision, mais étant un système offrant un grand nombre d'informations utiles sur les navires, il a été vite utilisé comme système d'enregistrement des positions et activités des navires. Le développement des technologies satellitaires ont accéléré le processus, les positions des navires étant désormais accessibles en ligne sur des sites dédiés. Cependant, ainsi que présenté dans la littérature, et malgré son importance dans la sécurité de la navigation, le système présente un faible niveau de sécurisation, et la présence d'erreurs, de falsifications et de piratage des données est avérée par la littérature. Dans cette optique, il est particulièrement

important d'évaluer les informations transmises par ce système afin de s'assurer de leur authenticité et de s'assurer que des décisions prises sur ces données le soient avec une bonne connaissance de l'authenticité de ces informations.

Cette recherche se base sur trois postulats qui sont : (1) Le système AIS ne transmet pas que des informations parfaitement authentiques, car des falsifications ont été montrées, (2) les falsifications du système sont dues à des êtres humains, sont imparfaites et donc sont détectables et (3) les erreurs et falsifications de l'AIS peuvent avoir un impact sur le monde réel.

À cette fin, trois hypothèses ont été proposées, qui sont : (1) une évaluation de l'intégrité des données, rendue possible par l'existence d'anomalies, permet l'évaluation d'un message et de son information, (2) il est nécessaire d'effectuer des analyses sur tous types de messages, afin de détecter des anomalies de toutes sortes, sans se restreindre aux messages spatio-temporels et aux analyses spatiales et (3) une détection des anomalies du système permet l'évaluation des risques associés au domaine d'étude.

Cette thèse a pour but de répondre à ces hypothèses en définissant une méthode pour l'analyse des données AIS comprenant une évaluation rigoureuse des messages eux-mêmes et une évaluation des risques maritimes pouvant émerger du fait des erreurs, anomalies et falsifications qui sont présentes dans le système. Il est donc nécessaire de modéliser le système et ses possibles erreurs et falsifications, de considérer l'analyse de données et la gestion des données dans de la donnée non totalement fiable, de distinguer le vrai du faux dans un flux de données et d'évaluer les risques associés. Tous ces objectifs nécessitent la création d'un système d'information pour la gestion des données incertaines.

1.1 The maritime context

1.1.1 The human uses of the ocean

Covering 71% of the surface of the planet, the World Ocean is a major feature of the life and the economy of the World. Most of its surface, 64%, is outside the sovereignty of any state, and in the remaining 36% the sovereignty is divided between the countries in several areas, the most famous one being the Exclusive Economic Zone (EEZ).

Several conventions exist in order to have an international coherence in this matter, especially concerning straits and channels, which often have their own regulations. Conventions on territorial sea, contiguous zone, international waters, continental shelf and the fishing activities were established in Geneva in 1958 (United Nations, 1958). Then in 1982 the Montego Bay convention established rules for archipelagic waters, EEZs and seabed. Some local conventions also apply, such as the Barcelona convention for the Mediterranean or the Nouméa convention for southern Pacific. Straits also have *ad hoc* conventions, such as Gilbratar's (1912) or Dardanelles' and Bosphorus' (1936).

In the coastal zones, the applicable law is the one of the coastal country while in international waters it is the one of the ship's flag, causing the problem of the flag of convenience which fits out three vessels out of five. A certain amount of countries propose

convenience flags such as, amongst others, Liberia, Cyprus, Bolivia, Panama, Mongolia. The problems are mainly on the right of workers, the tax benefits and the low security requirements for the seafaring of vessels.

As 90% of international transportation is done by the oceans, it has a central place in the economy of the World. The crowded areas are often regulated by the use of traffic separation schemes (TSSs) in order to prevent accidents. International goods transportation in cargoes is not the only activity at sea, as fishing boats (about 50 million fishermen in the world), cruising boats, military boats and some specialised boats are widespread all around the world.

The actors of the ocean are various, and include the fisheries, the merchant navy, the boating and pleasure cruising activities, the ports, the industries at sea, the shipyards and the specialised activities, such as Search & Rescue, tugs or icebreakers.

International organisations have been set by the United Nations, such as The International Maritime Organisation (IMO), the International Tribunal for the Law of the Sea, or the International Seabed Authority. As the international traffic is dense, safety and security measures must be put in place. Electronic systems that enable people to better understand their environment were progressively developed. On-board, they can provide information about surrounding environment and display it graphically; on-shore, they can give information to the coastal authority about the state of its own sea, improving its maritime situational awareness. One of the currently used systems is the **AIS**, standing for **Automatic Identification System**.

1.1.2 Maritime watch: actors and tools

1.1.2.1 Actors of the safety and security at sea

In order to increase the security and safety, actions are taken at several level, from the global to the local. New laws of the sea can be set up, for instance, by the International Maritime Organisation, for a global use. In the chain of maritime surveillance, several organisations are in charge of the management and the surveillance of traffic, the aid to mariners and the security interventions. Those means are set from the level of one port (harbour master) to international level. In France, at a national level, the Sea-domain State Action (SSA, for *Action de l'État en Mer*) gathers the organisational means put in place in the French seas all around the World for defence, environmental protection and environmental safeguard purposes. Led by the French Prime Minister and its representative the maritime prefect (*Préfet Maritime*), the SSA embraces administrations such as the French Navy, the French national Police force, the directorate of maritime affairs, the customs, amongst others.

In the frame of the SSA, seven Maritime Rescue Coordination Centres (MRCCs) are put in place along the French shores, in order to ensure the surveillance of strategic maritime spaces. In addition to those control centres, research units specialised in maritime accidents are dedicated to the study of past accidents in order to understand the context under which the accident took place and learn lessons from them. Such units are managed by coastal states, with the BEAmer (*Bureau Enquêtes des Accidents de mer*) in

France or the MAIB (Maritime Accident Investigation Branch) in the United Kingdom. In those groups, analysts have to study past data, among which manoeuvres of vessels, geographical context, exchanges between the vessel and the control centre. A detailed description of the archived moves and the condition of the vessels is led. The purpose is to find the causes of the problem and to get from them recommendations and lessons for the improvement of maritime security. Some papers such as (Lavigne et al., 2011), (Glandrup, 2013) or (Riveiro and Falkman, 2011) underline the part of such experts in analysis and modelling of risks and behaviours.

Some specialised organisations have been put in place by some governments, according to the type of threat. For instance, the CeCLAD-M (*Centre de Coordination de la Lutte Anti-drogue en Méditerranée*, for Mediterranean area anti-drug enforcement coordination centre), allows the struggle against illegal drug traffic, thanks to a collaboration between intelligence agencies. Another example is EUROSUR for the surveillance of illegal immigration into the states of the European Union. All those actors of SSA and maritime surveillance work together for the defence and the protection of the international maritime space, and must use several tools and databases to successfully complete their missions. Those tools will be the subject of the next section.

1.1.2.2 Tools for the security of navigation and maritime surveillance

In the surveillance domain, data concerning the movement of the vessels, acquired via active or passive sensors, are used as basic data from which is extracted all relevant information. The IMO set a system called Automatic Identification System (AIS), based on the exchange of messages between vessels via VHF, including position messages with route, cargo and destination data, coming from GNSS receiver working in DGNSS mode and on-board sensors. The messages are sent on a regular basis and ensure knowledge of the surroundings; however, all vessels are not fitted out with this system. Historically, radar were the primary source of information for maritime surveillance and today it offers complimentary information to other sources, such as AIS or LRIT, and can also detect vessels that are not obliged to be fitted out with the systems. Similarly, AIS allow the knowledge of some areas that could be masked by topography using radar.

Several data sources enable us to follow the maritime traffic in real-time, either from a surveillance centre (Maritime surveillance systems, VMSs, VTSs) or from the vessels (aid-to-navigation systems, anti-collision systems). In addition to vessel movement data, cartographic data are required in order to know the geographic, topographic or regulatory context. For this reason, electronic navigational charts (ENC), consisting of vectorial charts, form a cartographic database for the display of maritime pieces of information (bathymetry, regulated areas, amongst others), managed by the International Hydrographic Organisation (IHO). Those charts can be visualised using the Electronic Chart Display and Information System (ECDIS), which must follow norms put in place by the IMO on representation of maritime databases. ECDISs provide position information of nearby vessels, hazards, ephemerides and maritime traffic signals. Unfortunately, those systems are often flooded with data, which makes their display complicated and their understanding hard, if not impossible. Moreover those tools are not fitted with traffic analysis features (Glandrup, 2013).

The Web technologies providing open access to the public to AIS data enabled the Maritime traffic surveillance tools. Websites such as *marinetraffic.com*, *shipfinder.com* gather AIS data from all stations in partnership with them. Today, those websites only offer visualisation features, and no movement analysis or movement interpretation with the purpose of anomaly or hazard detection. In parallel, some maritime surveillance systems have been developed with the peculiar purpose of finding out anomalies or hazardous behaviours.

1.1.3 Maritime cyber-threat and cybersecurity

Since the inception of digital global networks, new threats have arisen as well, and the means to provide and ensure security of digital communications is the cybersecurity.

This term covers all the policies, laws, tools, concepts for security in a digital environment, as well as the risk management systems, the risk mitigation practices, and all kinds of action, good practices and technologies usable to protect people, electronic components or larger organisations like businesses or states from harm from a cyber source.

Each day in the World, 144 billion e-mails are sent, each second 30 Gb of data are generated, and information systems are now key elements of the World economy. On the one hand this data carry innovative concepts and new opportunities, on the other hand they represent a target and are responsible for new threats.

In 2014, the worldwide cost of cybercriminality was about 445 billion US$, and the protection must be put in place to prevent any harms on people, assets and national interests.

Systems can undergo several kinds of threat linked to cyberactivities, such as eavesdropping, denial of service attacks, malwares, trojans, acute vulnerability, computer-related crime or viruses, to the benefit of activists, vandals, spying states, thrill-seekers or criminals, with or without financial gain. Of course, the threat will vary according to the target, and an individual at home or a military facility will face different kinds of threat.

At the state level, France created the National Cybersecurity Agency of France (ANSSI, for *Agence nationale de la sécurité des systèmes d'information*), an agency ensuring the mission of national authority security of information systems. In this respect, ANSSI is responsible for the proposition of rules for the protection of state information systems and for the verification of the implementation of measures adopted. As for cyber defence, it provides a monitoring, detection, alerting and reaction feature to computer attacks, particularly on the networks of the State[1]. At the European level, the European Cybercrime Centre is in charge of the coordination of the international law enforcement for computer crime facts.

In the maritime environment, telecommunications are important as they ensure a proper knowledge of the surroundings of a vessel, particularly in conditions where the naked eye is not sufficient (such as night, poor weather, wide range or physical mask). It is particularly important to make sure that the information received by the vessel is

[1] from www.ssi.gouv.fr/en/mission/audiences-and-activities

genuine, and that the information sent from the vessel is properly transmitted, *i.e.* to the targeted locations and untouched.

It is therefore necessary to check the genuineness of the communications between the vessels, as their importance in the World economy is huge, and the consequences of any incident at sea can easily be terrible, from a human, economical or environmental point of view. Rescuing people at sea, particularly in remote location, is a difficult task, and distress calls are mainly made from electronic messages, which is another factor to consider maritime cybersecurity of telecommunications.

Successful recorded attacks on maritime targets are few, but with the rise of the global cyberthreat their number is expected to rise. One of them is the attack to the Antwerp port by hackers during a 2-year period between 2013 and 2015, when they infiltrated a cargo-tracking system and facilitated the importation of drug in container cargo from South America to Europe (Marin, 2014).

1.2 Research problem

1.2.1 AIS vulnerability

As seen before, at sea, various systems enable the mariners and vessel crews to be aware of their environment, and for the coastal states to be aware of the traffic incoming, leaving and passing by, as well as being able to know where is located every single vessel bearing its pavilion. One of those systems, the Automatic Identification System, was put in place by the IMO at the beginning of the 2000's (IMO, 2004). Albeit officially designed for security purposes and anti-collision, the system, very powerful vector of knowledge on vessel identity, vessel characteristics and vessel navigation with its numerous features, became a tool used by on-shore bodies (ship owners, but also coastal states and surveillance centres) as a control, surveillance and decision-support tool. The development of satellite technology later enabled online websites to provide a picture of the worldwide maritime traffic in near-real-time, as data sent remotely from any coast is stored in the satellite and downloaded to coastal stations once the satellite reaches it.

The AIS system, despite its importance in maritime anti-collision awareness, is weakly secured, and bad quality data have been demonstrated, such as error in the messages, data falsification and data spoofing (Ray et al., 2015), with particular cases demonstrated such as identity theft (The Maritime Executive, 2012b), disappearances (Windward, 2014), the broadcast of false GNSS coordinates, the statement of a wrong activity (Katsilieris et al., 2013), or the *ex nihilo* creation of made-up AIS messages (Balduzzi, Pasta, et al., 2014) as shown in Figure 1.1. Those activities are performed with the purpose of misleading the outer world and crews at sea, by the concealing of actual location, movements, activities, the creation of ghost and fake objects, vessels, false closest point of approach triggers or false emergency messages. According to a study done by (Harati-Mokhtari et al., 2007), it is estimated that circa 1% of the vessel voluntarily broadcast falsified or concealed data.

Figure 1.1: Spoofing case: *ex nihilo* creation of a trajectory, from (Balduzzi, Wilhoit, et al., 2014)

1.2.2 Associated risk assessment for decision-making

As seen before, MRCCs are in charge of the monitoring of coastal navigation, the surveillance of behaviours and the commitment of rescuing units, with the managements of engaged means. In order to properly monitor the maritime traffic, those workers need to have a clear understanding of what is happening at sea. Nowadays, the communication systems enable several systems to be used, AIS, LRIT and radar, amongst others, provide pieces of information to the workers, enabling them to assess the situation, judge the level of risk associated with a given situation and mobilise the proper amount of people and means to a given case, ensuring that several problems can be treated at the same time by people and means management. However, those actions need a good maritime picture to be taken properly. A distorted view of what is happening at sea can imply a poor management of people and means, potentially leading to harmful situations.

In this scope, it is particularly important to assess maritime information in order to check its genuineness and assist the decision-making process, so that the right amount of people and means is used for each mission.

1.3 Hypotheses and objectives

In order to work on this research problem, some postulates are stated:

Postulate 1: *The AIS does not carry perfectly genuine data, falsifications have been proved.*

Several cases have been reported in the literature and presented before, demonstrating that the system has failures and can display non-genuine data, either voluntarily broadcast or not.

Postulate 2: *AIS falsifications are owed to human beings, are non-perfect and therefore are detectable.*

A perfect falsification is not detectable, as it would pass through all integrity assessment

checks, however, it would require a tremendous mastering of the AIS and other systems with which cross-checks can be performed.

Postulate 3: *AIS errors and falsifications can have an impact on real-life.*

The fact to emit false information, on purpose or by carelessness, can impact real-life as other people or automatic tools receiving and processing this information might take erroneous or biased ranging from the bad management of goods to the accident with pollution or risks on human life.

In addition to postulates, hypotheses are set:

Hypothesis 1: *A data integrity assessment, made possible by the existence of anomalies, allows for the assessment of a message and of its data*

Hypothesis 2: *It is necessary to process analyses of all sorts on messages, in order to detect anomalies of all sorts, without restricting oneself to spatial temporal messages and spatial analyses.*

Hypothesis 3: *An anomaly detection of the system enables the assessment of the risks associated to the field of study*

Objectives: This thesis aims to answer these hypotheses by defining a methodology for AIS data analysis incorporating a thorough assessment of the messages themselves and an assessment of the maritime risks that can emerge because of the errors, anomalies and falsifications that are present in the system. It is therefore necessary to model the system and its possible errors and falsifications, to consider data processing and data management in non-fully reliable data, to distinguish the true from the false in a data stream and to assess the associated risks. All these objectives imply the fact to create an information system for the management of uncertain data.

1.4 Research agenda

Although independent from other maritime surveillance tools, this work is inspired by several common roots with other studies, with an operational purpose. The general methodology is presented in Figure 1.2, in which can be seen the workflow derived from the literature and selected points of interest.

First, a state-of-the-art study was performed in the scientific fields that are connex to our interests, such as the notion of data, the notion of information, the typologies, the ontologies, the maritime domain in general and the maritime domain security in particular, the risk level determination and the anomaly detection.

This bibliographic step enabled the understanding of the research context in which this thesis takes place, and to define hypotheses and objectives for the research problem, refined by a thorough analysis of the AIS system performed in parallel. This first step led to the second year admission committee, where the work was assessed and criticised.

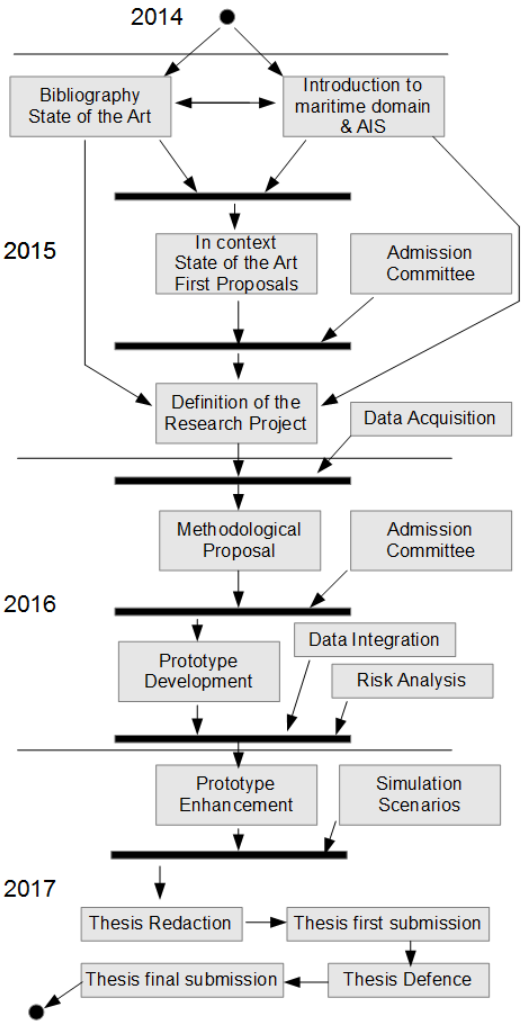

Figure 1.2: Activity diagram of the thesis

During the second year, a system for data assessment was designed, based on the structure of AIS data and on the state-of-the-art bibliographic survey performed, that underlined the use of data quality dimensions. Therefore, such dimensions were applied to the peculiarities of AIS data, with the support of AIS specification and actual AIS data received in the Brest antenna. This system was presented at the third year admission committee, where it was evaluated and criticised.

During the third year, after the validation of the model by the committee, the model was implemented in a prototype which uses AIS data as input and provides a risk level assessment for several designated risks as output. The prototype uses Python language and SQL language for the database queries of the Postgres/Postgis AIS database, extended with some non-AIS data.

1.5 Document layout

In this first introducing chapter, we presented the applicative context of this thesis which is the maritime domain awareness, and enabled us to understand the current limitations

of this awareness due to the weaknesses of the Automatic Identification System. The chapter 2 is a state-of-the art study of the concepts of data, information, the data quality dimensions, the data formalisation methods and the knowledge discovery methods. Then the chapter 3 is also a state-of-the-art chapter, but concentrating on the AIS.

Then the chapter 4 presents our proposition for the integrity assessment of AIS messages, in a formal methodology leading to the assessment of messages with respect to falsification cases. Chapter 5 presents the implementation of this proposed methodology in a program using real AIS data as study base, and finally chapter 6 treats the notion of maritime risks, and more particularly the relationships between the results of the data integrity assessment presented in chapter 4 and the associated risks for maritime navigation.

Eventually in the conclusion we precise the contributions of our thesis to the domain of maritime awareness and provide some prospects and perspective about it.

Chapter 2

Data integrity assessment for anomalous event detection

Chapitre 2 : Évaluation de l'intégrité de la donnée pour la détection d'évènements constituant des anomalies

Dans ce chapitre, des notions liées à la détection d'anomalie sont présentées. En premier lieu, les notions de donnée et d'information, depuis la science de l'information jusqu'aux dimensions de qualité de la donnée, ouvrant la voie à la découverte de connaissances et à la détection d'évènements à l'aide de méthodes de formalisation de la connaissance. C'est dans ce domaine que l'on trouve la détection d'anomalies étant donné que la formalisation de connaissances est utilisée, couplée à des métriques pour évaluer la nature des informations données à l'analyse.

Aujourd'hui, la donnée prend une place centrale dans nos sociétés, où le numérique s'impose. Les volumes de données augmentant, il a fallu faire face à la gestion de volumes de données massives, appelées mégadonnées. Traditionnellement, quatre caractéristiques sont associées aux mégadonnées : le volume, la vélocité, la variété et la véracité, le volume étant en lien avec la quantité de données à traiter, la vélocité représentant la capacité à rassembler et à traiter les données, la variété couvrant les diverses formes que peuvent prendre les données (image, texte, signal par exemple) et la véracité témoignant du rapport au monde de la donnée, de sa capacité à correctement caractériser l'état de l'objet décrit.

Dans la qualité de la donnée, deux grandes familles peuvent être décrites : la qualité interne qui est une qualité technique et absolue, permettant de déterminer la qualité intrinsèque de la donnée, et la qualité externe qui représente l'adéquation de la donnée à l'utilisation qui en est faite, qui est donc relative étant donné qu'elle dépend du milieu d'étude. Différentes dimensions de la qualité des données ont été sélectionnées pour leur adéquation à notre étude, il s'agit de la justesse, de la précision, de la fiabilité, de l'actualité, de la complétude, de la cohérence et de l'intégrité.

La détection d'anomalies s'effectue en trois étapes principales qui sont l'identification des caractéristiques et des comportements récurrents, la détermination de métriques pour le calcul de distance à cette normalité et la détermination de critères de seuillage pour discriminer la normalité de l'anomalie. Les métriques sont nombreuses et doivent être adaptées au type d'étude en question, ainsi, des distances de Minkowski peuvent être utilisées, ainsi que des distances moyennes, de Fréchet ou de Hausdorff pour les trajectoires spatio-temporelles, ou des distances d'édition pour des valeurs textuelles. Des mesures de similarités peuvent également être utilisées à cet effet.

Diverses méthodes de formalisation des données sont utilisables : les typologies permettent d'étudier un domaine complexe en le subdivisant en sous-parties constitutives mutuellement exclusives et collectivement exhaustives. En classifiant les objets d'une grande classe mère par rapport à leurs caractéristiques, il est alors possible d'appliquer des traitements similaires aux objets présentant des catactéristiques similaires. Les ontologies enrichissent les typologies par les liens qui unissent diverses classes d'objets, l'usage d'un moteur d'inférence permettant alors d'en faire ressortir les règles. Enfin, la logique de description permet la représentation des rapports entre des individus d'après une approche déterministe où les concepts et les rôles ont une description structurée.

Introduction

In this chapter, notions related to tools for anomaly detection are displayed. In particular, the notions of data and information, starting from information science all the way to the data quality dimensions, that drive the path to knowledge discovery and to event detection with a proper knowledge formalisation. Anomaly detection lies within this range as it uses knowledge formalisation, enhanced by metrics to assess the nature of pieces of information. The first section of this chapter is dedicated to integrity as a data quality dimension and to information-related concepts, the second section is about anomalous events and anomaly detection, the third part about knowledge formalisation methods and the last one about knowledge discovery methods.

2.1 Integrity in the scope of data and information concepts

This section focuses on the concepts of data and information, and in particular on the importance of integrity as a data quality dimension that could be used for further data assessments. First, the information side is deepened, with presentation of notions such as information science and information theory. Further developments are done on the notion of information coherence and on the trust in information. Then, developments on data are presented, on the importance of data in modern-world societies, on the importance of data quality and on the definition of dimensions with the purpose of describing the quality of data. The determination of the quality of data is being done through data quality dimensions, amongst which integrity has to be discriminated as particularly important.

2.1.1 From the concept of information to information science

In this first section a focus is done on information, with etymological background and dictionary definition, leading to a common sense perspective presentation. Communication is then distinguished from information in the fact that communication is interested in the link between the sender and the receiver, while information is raw. The various media that can support information are then displayed, before an introduction to information science with its story, its processes and its aspects.

2.1.1.1 Etymology

The word information comes from the Latin word *informatio, onis, f.* According to (Gaffiot, Félix, 1934), this word has two meanings:

1. *Draw, sketch*
2. *Idea, design ; representation of an idea by the representation of a word ; explanation of the meaning of a word by its etymology*

In this latin word, we can see that the meanings put the stress on the idea of conveying facts by drawing, sketching or describing, rather than embodying the proper facts, as the word "information" does.

It must be noticed that the verb *informo, as, are, avi, atum*, also exists, but its meanings: "*to shape, to model, to describe*" (Gaffiot, Félix, 1934), do not differ so much from the "*informatio, onis*" ones.

2.1.1.2 Definition

The word information, according to (Oxford, 1989), has two meanings:

1. *Informing or being informed*
2. *(on/about sb/sth) facts told, heard or discovered (about sb/sth)*

The dictionary also puts a definition of information science: "*Study or use of processes (esp. computers, telecommunications, etc) for storing, retrieving and sending information of all kinds (e.g. words, numbers, pictures).*"

The definition of the word is very simple, however, it covers a large amount of concepts, presented hereinafter.

In general, information can be considered as being both the proper message to communicate and the symbols used for this communication to be understandable. The code

used does carry a meaning, and this code is composed of letters, numerals, ideograms or pictograms. Put together, elements of this code form sentences which interpretation is left to the receiver. The context influences the way information is understood. A direct implication is that the interpretation of information is unique to each person, despite the fact that the piece of information is the same. Without the context, it only represents the vector of data (as shown hereinafter in the theory of information). Information can both be built, like a book, or self-made, as light is. Information is a means of organisation in our human societies.

2.1.1.3 Discrimination between information and communication

On the one hand, generally speaking, information is only a part of general communication, and that is why misunderstandings are so common in human interactions (Lautier, 2007). On the other hand, the fact that information was for a long time rare and difficult to spread put together the notions of information and communication. But the development of technological means of communication, from the rotary press in the nineteenth century to the Internet boom in the early twenty-first century, progressively reduced the time between the production and the consumption of information, favouring the creation of more information, mainly quantitatively.

Communication is interested in the relationship between the provider and the receiver, whereas information itself is only the raw juxtaposition of mutually intelligible signs (Wolton, 2004).

Several means of communication can convey the same idea, those means having a very wide range of length, quality and complexity. For instance, the same information can take up one or several pages of a newspaper, 5 minutes in a news broadcast on television, one article on the Internet and a given amount of signs in a tweet (140 as of 2017). Whereas the antique ways of communication were efficient because of the difficulties to convey information, the new ways of communication, far more easy, allow almost everyone to communicate on almost every topic of its interest, and are therefore less efficient, the ratio of brand new information (from the receiver point of view) having radically diminished.

As shown in the Introduction, the AIS messages are broadcast using VHF radio signals that can be falsified or spoofed. The nature of the falsification or spoofing relies on the medium, in this case an electromagnetic wave, but the deep nature of the action of falsify does not rely on a sole medium, and specific ways to falsify information were developed for previous media, are currently used for present-time media and will be developed for the future media.

2.1.1.4 The information science

The information science finds its genesis in the important phenomenon of the transgression of the limits of the traditional subjects of research. As some of the new work was done by researchers who were external to the proper field, collaboration between scientists has become necessary, leading to mutual enrichment and the sharing of a common goal: to ease the improvement of knowledge and the evolution of humankind.

After the second World War, the automation of research tools led to the creation of the idea of finding the right document whenever needed. This encouraged the creation of new methods of documentation, notably with the creation of the key-word (Fondin, 2005). In these years, with the beginnings of computer science, the scientific and technique information increased dramatically.

The first definition of information science was proposed in a lecture organised by the United States' Georgia Institute of Technology, in 1961, which stated that: "*Information Science is a science that investigates the properties and the behaviour of information and the means of processing information for optimum accessibility and usability. The processes include the organisation, dissemination, collection, storage, retrieval, interpretation and use of information*".

(Dragulanescu, 2003) proposed a model in three fundamental cyclic processes: the construction of information, the process of information and the use of information. In this paradigm, the construction of information aims to obtain or generate information and to generate its supporting media, the process of information aims to obtain added value from the information to the user and the use of information aims to spread and make use of information the most usefully possible, in order to turn it into knowledge.

The current fields of research on information science are various. These domains were divided by (Dragulanescu, 2003) into the seven categories, that can be then gathered in three main categories: computer science (CS), human science (HS) and library science (LS). Those seven categories are presented in the list hereafter with their corresponding main characteristics.

- The need of information, the way information is used and spreads (LS)
- The structure of signs and their working in the communication processes, the languages and their automated or not analysis (HS)
- The classification, indexation and document analysis systems, the computer as a storing machine, the structure of databases and the computerisation of libraries (LS)
- The analysis and evaluation of the operations involving information (CS)
- The recognition of signs, analysis of speech and images, artificial intelligence and signal compression (CS)
- The economic, legal and social aspects of information (HS)
- The instruction and the professions of information (HS)

In this frame, a model of information science similar to a Greek temple was proposed, including the infrastructure of information science (the base), the instruments of the proper language (the columns) and the effects expected (the roof).

The concept of documentation was a trending topic between the 1950's and the 1980's, and became far less important with the wide diffusion of computers and the presence of

the Internet in many households. However, this situation could change, and the documentation aspect could become significant again with the forecast development of the semantic web.

The information science gives priority to the practical and technical approaches of the information transmission whereas communication science puts the stress on the speech enunciation and the construction of information by the media. There are currently neither strict boundaries to this subject nor consensus on its structure.

However, all the aspects of the concept of information are not studied by information science, particularly those used by the mathematicians in the frame of the information theory, which is the subject of the section 2.1.2.

2.1.2 Information theory

Mostly, the information theory refers to the theory developed by Claude Shannon in (Shannon, 1948). His theory is a probabilistic theory enabling its user to quantify the mean information content of a group of messages, when the computer code follows a given statistic distribution.

In this theory, only mathematical and communication aspects matter, the form or the cognitive content is ignored. Originally, the goal of this theory was to transmit information, the faster and the safer way possible, by developing methods in order to minimise the probability of error in the message recognition. It was then necessary to put forward the notion of information measuring, from a mathematical point of view. His postulate is that information has basically a mainly random nature, so there is a part of uncertainty. It is this uncertainty which is taken as an indication of information. Notions of information and uncertainty are combined, in this frame the more a piece of information is uncertain, the more it is interesting in the frame of information theory-based studies. The reasoning is done in a probabilistic point of view: a certain event holds no inner information.

The measurement of the entropy of information for subadditivity is done using the formula $H = -p \cdot log(p)$. The logarithmic measure is used because of its better convenience: it is more useful (parameters tend to increase in ratio with the logarithm of the number of possibilities), it is more intuitive and more suitable from a mathematical point of view. The choice of the base of the logarithm depends on the utilisation: in computer science, as binary digits are used, the base 2 is used whereas when decimal digits are used the base 10 should be used.

A way to measure how uncertain is the outcome of an experiment, the notion of entropy can be introduced. Having a set of n possible events of which probabilities are $p_1 \dots p_n$, the entropy H would be computed as: $H = -K \cdot \sum_{i=1}^{n} p_i \cdot log(p_i)$, where K is the Boltzmann's constant, expressed in $m^2 \cdot kg \cdot s^{-2} \cdot K^{-1}$ in physical systems and normalised to $\frac{1}{ln(2)}$ Sh in information systems taking the logarithm base 2 and normalised to 1 nat in information systems taking the natural logarithm. The higher the entropy is, the bigger the disorder will be, obtained for a uniform distribution. Similarly, a well-known phenomenon would have a close-to-zero entropy.

A communication system as described in (Shannon, 1948) is made of five components:

- An information source: the message is produced here, it can be a sequence of letters, a single function of time, a function of time and other variables, functions of several variables, and various combinations signals.
- A transmitter, which takes the message from the information source and transforms it into a signal suitable for a transmission by the channel.
- The channel, which is the medium of transmission. It can be a wire, a cable, a radio frequency, a beam of light ....
- The receiver undoes the work of the transmitter, turning the signal into the message.
- The destination, which is the final operator, for whom the initial message is intended.

In a complete assessment of information, all parts of the information system must be treated.

2.1.3 Information coherence

A common definition of coherence is presented in (Hartmann and Bovens, 2001) as "*when we gather information from less than fully reliable sources, then the more coherent the story that materialises is, the more confident we may be,* ceteris paribus".

Some factors can affect the confidence we have in a piece of information. Three can be distinguished: how surprising is the information, how reliable are the sources and how coherent is the information (Hartmann and Bovens, 2001). For instance, if pieces of information are both halfway surprising and halfway coherent, the global confidence will rely on the reliability of the sources: we will be more likely to increase our degree of confidence as the source is more referenced as truth-teller rather than randomiser. Similarly, if the pieces of information are halfway coherent and come from halfway reliable sources, we will rely on the surprise factor in order to assess the degree of confidence, which will be as high as the piece of information is more rather than less expected.

As the construction of a model to define measures of expectance and reliability is quite easy, it is far more complex to do it for coherence, as a quantitative measure of coherence does not exist as such. In (Hartmann and Bovens, 2001), a measure of partial coherence between information sets was defined, as well as for the first two factors.

The expectance measure is directly linked with the prior joint probability of the propositions, which is lower for less expected information and higher for more expected information.

The reliability measure is directly linked with the likelihood ratio $\frac{q}{p}$, p being the probability for a proposition for being true and q the probability for the same proposition to be false. $p = q$ in the case of randomiser and $q = 0$ in the case of truth-tellers. The reliability can be defined as $r = 1 - \frac{q}{p}$, being minimal for randomisers and maximal for truth-tellers.

The coherence measure is far more complex. S and S' being two information sets, S is more coherent than S' if and only if $f_x(S, S') > 0$, x ranging from 0 to 1, and $f_x(S, S')$ being a difference function built as $f_x(S) = c_x(S) - c_x(S')$, x ranging from 0 to 1. $C_x(S)$ is a measure of the coherence of the set of information S with respect to a similar set in which coherence of information would have been maximal. So $c_x(S)$ is a rate, defined as $c_x(S) = c_x(R_1 \dots R_n) = \frac{P \cdot (R_1 \dots R_n)}{P_{max} \cdot (R_1 \dots R_n)} = a_0 + \overline{a_0} \cdot \frac{x_n}{\sum_{i=0}^{n} a_i \cdot x_n}$, where R_i is the i^{th} proposition, n is the number of propositions, a_i is the joint probability of all combinations of the values of the n R variables to have i negative and $n - i$ positive values.

Another point of view of the information coherence concept is presented in (T. Wang et al., 2010), where it is defined as following: "*Coherence is a stationary process analog to the traditional correlation coefficient, taking values between 0 and 1 at any given frequency*". Coherence is seen as a measure of the linear dependence of two processes at a given frequency. If it is equal to zero, it means that one process cannot be used to predict linearly the other. If it is equal to one, it means that one process allows a full linear prediction of the other one. A significant over-zero value means an association between the two processes. However, coherence can be inadequate to measure a general association, because it can be equal to zero when two series are related actually. This does not occur for the coefficient of mutual information. The latter takes the value zero if, and only if, two variables are statistically independent. This concept was introduced by Shannon (Shannon, 1948), and consists of the amount of information that a random variable has with respect to another random variable. Another model, called Lin-Lin model, allows an identification of a causal linear relationship between two sequences of events. The causal part was not supported by the previous methods.

Those three methods, pure coherence, mutual information and Lin-Lin are mathematically developed and compared in (T. Wang et al., 2010). As a result, it can be seen that coherence is useful as a diagnostic process in order to detect associations when is considered the problem to whether or not a output series can be predicted through a linear relation from an input series. Mutual information calculates the strength of the correlation parameter between two series, independently from any statistical point of view. It forms a test of dependence. The Lin-Lin model offers the possibility to determinate, between two processes, which one is driven by the other one, or if they are mutually driven, or if they are both driven by some other process.

A subjective logic view for the coherence of information as seen in (Ceolin et al., 2013) can be divided in four main components: belief, disbelief, uncertainty and *a priori*. Belief value represents how much the statement is true, disbelief value summarises how much the statement is false, uncertainty quantifies the correctness or the truthfulness of a given statement, *a priori* represents the prior bias that the source has against one of the possible outcomes. An *a priori* value close to zero means higher bias towards disbelief and an *a priori* value close to one means higher bias towards belief. Generally speaking, the uncertainty increases as the belief and disbelief decrease, however, in case the source is known as being non reliable or potentially malicious, another operator (*ad hoc*, defined by the user) can be used, which increases the disbelief rather than the uncertainty.

Another branch of the information coherence field is the developments on Scott information systems (Scott, 1982), in which coherence of information is evaluated in (Karadáis, 2013). This is a part of the domain theory.

2.1.4 Trust in information

Before the discussion about trust in information, trust in itself is assessed in the first place, then, as information come from sources, and as it is an important subject since the rise of computer science rose new concerns about it, the particular trust in information sources is developed, with an additional part on the perception of trust in information technology.

2.1.4.1 General considerations on trust

Trust is a widespread word, and can mean several things according to the point of view of the user. However, trust was identified as playing a key role in capital investment, sales, relationships, cross-cultural communication, cooperation and learning (Blomqvist, 1997). In this scope, trust as a part of human interaction can be considered as one of its basic variables. However, a general conception of trust is hard to establish, because of the number of disciplines in which trust is studied, each one defining it from its own scope. (Blomqvist, 1997) develops the way different disciplines such as social psychology, philosophy, economics, contract law and marketing perceive and study trust.

As stated in (Denize and Young, 2007), in the process of communication and decision making, trust is thoroughly embedded. It gives people the possibility to open one's mind to others, and both develop personal and professional relationships. In human relationships, trust plays a key role, as it includes a kind of calculation of benefits, costs and risks for a given situation.

The concepts which are close with trust are as various as credibility, sincerity, competence, confidence, faith, hope, loyalty or reliance (Blomqvist, 1997). In addition, trust being considered as both a social and a psychological phenomenon, is located on four levels: individual, interpersonal, relational and societal (Kelton et al., 2008).

On trust, as a whole, one can say that there is no clear definition of trust, as it must be put into a context. Economists see it on rational points, philosophers adopt a more attitudinal and ethical point of view, whereas social phycologists emphasise inter-personal aspects. Generally speaking, trust is necessary to be trusted, and is critical to form and maintain relationships. However, trust remains personal, and the scale of trustworthiness of people can vary a lot from one person to another, the extreme examples being the naive people, willing to trust and believe anyone on any subject, and the paranoiac people, who are not willing to trust anyone.

2.1.4.2 Trust in sources of information

The notion of trust in the information source is important, as people demonstrate a lot of attention on the trustworthiness of the different sources. Those sources can be a document (oral or written), humans or virtual, easy or hard to access. The sources can also be first-hand or be recommended by acquaintances. The simple access to the source is not enough to assess trustworthiness, the way in which people access the sources must enable them to assess its trustworthiness, because people need to form an opinion about the source

(Hertzum et al., 2002). If the user cannot get information about the source, an absence of trust or even distrust can appear.

With the development of computers and services attached like the World Wide Web, people rely more and more on the Internet in order to find information. One can find abundant information about a wide range of subjects, and the Internet is generally considered as a vast library in which the modern societies are more and more dependent. On the Internet, a lot of information is available and sometimes some pieces of information hold contradictory opinions with respect to other pieces of information about the same topic. So people have to seek for hints to assess the trustworthiness of online information. They will treat in different ways the message they feel coming from a person who have a strong social relationship in the place where the message is written rather than the message written by a person they feel having a weak social relationship (Pan and Chiou, 2011). The perception of positive and negative messages also varies depending on their kind. *Ceteris paribus*, a negative message tends to affect more strongly the information-seeker than a positive message does. So when seen on an online opinion platform, costumers trust negative information more than positive information (Pan and Chiou, 2011). However, the overall trust in information provided by other consumers will positively affect the attitude of the consumer toward the product, in the positive or negative way.

As there are different kinds of goods, the consumer will not react the same way. Experience goods and credence goods are compared in (Pan and Chiou, 2011), the latter having a weaker strength of the relationship between the statements (positive or negative) and the attitude for the consumer than the experience goods. Experience goods being characterised by attributes that cannot be determined before the purchasing, and credence goods are characterised by attributes that cannot be stated by the consumer (for instance education). Another category is search goods, which attributes can be fully determined before the purchasing. The purchasing of credence good is seen riskier than the purchasing of search or experience goods, because of the lack of knowledge and the lack of capacity for the evaluation of information attributed to these goods. When facing a risky situation, consumers will be conservative towards the online information they receive and hence the effects of the use of this information is more important for search and experience goods than for credence goods.

An example of application is given in (Frewer et al., 1996), where the trust in information given about food-related hazards is compared: if sources are seen as self-serving or biased, the pieces of information they provide will not be trusted. So the source characteristics are important because the attitude of the receiver towards the source and towards information provided will change. In this study, two dimensions have emerged as being important for the trust determination: the competence, so the level of expertise in the proper subject, and the trustworthiness, so the degree in which will the speaker be truthful (Costé et al., 2016).

In (Frewer et al., 1996) it appears that trust is linked with perceptions of knowledge, accuracy, and concern towards public welfare. Surprisingly, expertise and freedom do not convey trust on their own. It also appears that distrust is associated with the source being a provider of erroneous information and a perception of deliberate information distortion.

2.1.4.3 The perception of trust in information technology

Trust is an intuitive notion for a man in his everyday life. Manifestations of trust happen very often, but are actually noticed only when trust starts to lack. Its nature consists of the tension felt by someone about another person or technical device to ensure oneself of the performance of the other.

Table 2.1 lists the characteristics of trust and matches each one with the corresponding characteristic in the field of trust in information.

Component	Trust	Trust in Information
Preconditions	Uncertainty	Lack of standards and controls
	Vulnerability	Potential harm from using poor information
	Dependence	Decisions, knowledge, writing
Development processes	Prediction	Experience with source
	Attribution	Confirmation with multiple sources
	Bonding	Evocation of emotional response
	Reputation	Authority, certification, reviews, references
	Identification	Resonance with style, arguments, objectives
Trustworthiness	Competence	Accuracy, currency, coverage, believability
	Positive intentions	Objectivity
	Ethics	Validity
	Predictability	Stability
Influences	Propensity	Disposition to Information
	Context	Relevance
	Social Trust	Recommendations
Elements	Confidence	Confidence, reliability, validity
	Willingness	Freedom to accept or discard information

Table 2.1: A framework for trust and information, from (Kelton et al., 2008)

With the development of digital technologies, people rely more and more on information given by electronic devices, and behave towards them in a way close, but not similar to, the one they would have behaved with another human being.

A person and an information technology can both act in predictable and consistent ways. But for a person, it can be added that its behaviour is reliable, predictable or easily forecast, whereas for an information technology, the system is predictable (by its nature) and operates reliably, *i.e.* doing what needs to be done without unreasonable delays, crashing or unexpected results (McKnight, 2005). As the capability is a common point, the willingness is only for humans.

For the fundamental preconditions of trust, which are uncertainty, vulnerability and dependence, trust in information matches the lack of standards and controls (leading to uncertainty of the source), the potential harm from using poor information (leading to vulnerability) and decisions and knowledge, which are equivalent to dependence. In the trustworthiness part, predictability is linked to the stability of the information, and the positive intentions in human relationship matches the objectivity of the trust in information. In another scope, propensity to trust is equivalent to disposition to information and the freedom to accept or discard information twins the willingness to trust.

2.1.5 Data in our societies

Data holds a central place nowadays, as computer science technology enabled the acquisition, storage and processing of tremendous amounts of data. Data is widespread and thus

used in almost every aspect of our lives. In addition, the development of numeric devices had created even more data, at a point where traditional methods (used for analog data) could no longer be used. This phenomenon, called Big Data, changed the perception and the modelling of data processing. In this section, the different uses of data are displayed and an overview on Big Data issues is presented.

2.1.5.1 Etymology

The word data comes from the Latin word *datum, i, n.* According to (Gaffiot, Félix, 1934), it is mainly used in the plural form (*i.e. data*) and means gifts, present. Its meaning mainly stems from the verb *do, das, dare, dedi, datum*, which meanings are numerous but is mainly used as "*to give*". It is its supine form that led to the current name.

2.1.5.2 Use of data

With the development of computer science, human societies rely more and more on data stored in and manipulated in or by computers. As there is no clear definition of the word data, it is not easy to define clearly what this word stands for. There are several fields in which the word data is used, in which the word has its proper meaning.

For the determination of the relevance of each proposition of definition for trust, several criteria must be assessed. (Fox et al., 1994) determined a number of six criteria, three linguistic and three of usefulness, hereafter listed, about what data must be:

- Clear and simple, which is required for a good definition
- Should not mention information, in order to avoid a circular definition
- Agree with the common usage, so be coherent with the common idea of what data is
- Approach both conceptual and representational facets of data
- Widely applicable, the range of data to which the approach can apply should be wise, especially concerning databases
- Quality dimensions, suggestions of important dimensions for the quality of data

One possibility is to follow the Latin etymology and define data as a set of facts. However, a fact is something that actually occurs, and is true by nature. Such a definition would lead to consider data as being indisputably true. So data cannot, in the scope of (Fox et al., 1994), be considered as a set of facts, but only that data is about facts.

Another approach tends to consider data as being the result of an observation or a measurement. Observation and measurement are doubtlessly important sources of data, however must also be considered data acquired by other ways such as assignment methods

(for instance the name or the phone number are data assigned to people, and neither observed nor measured). So data cannot be reduced to the means used to get it.

Another way to consider data is to define it as the raw material from which, once refined, information is extracted. This point of view puts the problem of the circular definition between data and information. Moreover, it is not clear whether to consider where data stops and where the information begins, and what is the process that enables one to turn into the other one.

A common way to consider data in databases is to define classes. Those classes can have links with others, and contain entities (e) which have attributes (a). Those attributes have a value (v), and it is the triplet value-attribute-entity ($v-a-e$) which can be considered as data. However, the value of an attribute of an entity is not strictly speaking a datum. A representation of data must be settled in order to standardise the possible input, as the same datum can be represented in various forms. Alongside with the representation of data, the recording of data is crucial to keep a record of it.

In this scope, data is defined by (Fox et al., 1994) as being triplets of value-attribute-elements with recording and representation clearly defined.

2.1.5.3 On big data

Big Data is a concept that has emerged in the late 90's, forecasting the stored information explosion of the 2000's, which is on-going in the 2010's, and which is due to the development of digital storage capabilities through servers, CDs and hard disks, with respect to analog storage. As the processing of this data became interesting, *ad hoc* methods needed to be implemented, as the traditional ones no longer worked with such an amount of data. In a nutshell, "*Big Data can be seen as all information that cannot be handled with traditional techniques and hardware*" (M. Chen et al., 2014).

2.1.5.3.1 The properties of Big Data Traditionally, four properties are associated with Big Data, which are called the four V's: Volume, Velocity, Variety and Veracity. The Volume is in relation with the amount of data to be handled, for instance, it is estimated that companies like *Walmart* collects more than 2.5 petabytes of data per day from their customers, and the total amount of data created each day overcomes the exabyte (McAfee and Brynjolfsson, 2012). The Velocity is the gathering and processing effectiveness, as the velocity of gathering and exploiting data is even more important than the Volume, as it is more applicative, enables researches to be done more quickly, or enable companies to be more competitive. The Variety property covers the fact that data in Big Data takes several forms, which can be images, text, messages, sensor data, updates on social media, signals from networks (such as wi-fi or GPS), amongst others (McAfee and Brynjolfsson, 2012), and most of those data sources are mainly recent. The Veracity is a challenge as it is not linked to the quality of the data but with its relation to the world. It represents the fact for a datum to be truthful, *i.e.* to correctly depict the world in the way that it is expected for it to do.

Other properties later emerged (Katal et al., 2013) (Jagadish et al., 2014), such as

Variability (which are the inconsistencies of data flow), Complexity (which is the ability to correlate and connect the relationships, the hierarchies and the data linkages between data coming from various sources (Katal et al., 2013)), Value (which is the intrinsic value of data, the value of data that can be extracted from it). Those properties are associated with challenges, which are Scale, which is the ability to manage ever increasing data volumes (Jagadish et al., 2014), Timeliness, which is the fact to process data real-time, Privacy and Data Ownership concerns, as some valuable data are electronic health records or location-based services having an unclear sharing of data. Last, visualisation and collaboration methods must be developed properly as the end users are humans which are only able to process little amount of refined data.

2.1.5.3.2 The challenges of Big Data The challenges of big data are numerous (M. Chen et al., 2014) (Sagiroglu and Sinanc, 2013): data representation (as heterogeneity is present, in type, structure, granularity, semantics, organisation) shall be efficient for an effective data analysis; redundancy reduction and data compression, as datasets generally display a high level of redundancy, in order to reduce the cost of storage and processing, and data can be compressed to reduce the storage by orders of magnitude; data life cycle management, in order to know if the data is up-to-date, as out-of-date data must be discarded, for storage and computational reasons; analytical mechanism, which shall process an amount of data (heterogeneous) in a limited amount of time; data confidentiality, as some data are private information about people, or credit card numbers; energy management, as storing, processing and transferring data will consume more and more electrical power; expandability and scalability, as present but also future datasets must be supported; cooperation, as the harvest of interesting data may require the simultaneous work of experts in different fields (Claramunt et al., 2017).

The technologies related to the understanding of big data are cloud computing, the internet of things, the concept of data centres (M. Chen et al., 2014). The collection of data can be done via log files, sensing or network data acquisition methods (such as in the Web). Before use and for a better processing, it is better to clean data and to remove redundancies. According to (Franke et al., 2015), some strategies for Big Data analysis are data wrangling (which is the fact to handle data in a convenient way for computational tasks), visualisation, reduction of dimensionality, sparsity and regularisation, optimisation, measuring distances, representation learning or sequential learning. Some Data Mining techniques are presented in section 2.4.1.

2.1.5.4 From bad data and errors to quality

Bad data can be considered as a virus because one erroneous datum put into a database at a given time will not only imply consequences on the future use of the proper database, but as this database will be replicated, and perhaps used in dozens of other, this error will carry on and can impact several databases in different fields (Huh et al., 1990). As inspecting methods are not perfect, the best way to keep an healthy database is to prevent bad data from getting into it.

Some errors can affect data. These errors are traditionally divided into two main parts: acquisition errors and processing errors, those parts being afterwards divided in subclasses

(Devillers, 2004). The acquisition errors can be collection or gathering errors, such as calibration, experimental, precision errors, and the processing errors can be digitalisation, generalisation, interpolation or format conversion errors.

At those errors can be added the errors arose from the use of data, or the misuse of data due to a lack of understanding leading to a state of doubt for the operator, equally called uncertainty. This uncertainty can be of four orders. In the first order, the conceptual uncertainty is linked to the confusion during the ascertainment of an observed reality; the second order descriptive uncertainty is linked to the lack of accuracy during the ascertainment of the value of an attribute of an observed reality; the third order is an location uncertainty, which is a lack of accuracy in the spatio-temporal ascertainment of an observed reality; and the fourth order, which is a meta-uncertainty, *i.e.* the uncertainty of the knowledge of the other uncertainties (*i.e.* the three first orders) (Devillers, 2004).

Quality can be defined as matching the requirements, a satisfaction scale for the need of the user, and the fitness for use of all the characteristics of the product for the fulfilment of explicit and tacit needs of the customer. So the quality of a set of data is not a unique absolute value, but varies from one user to another.

2.1.6 Data quality and its dimensions

As data can be poor, as errors can be found in it, it is necessary to be able to define quantities to describe data (so create data on data, *i.e.* create *metadata*). Those quantities, clearly defined, enable the user to have a summary of the data considered as a whole, so that the confidence in it can be defined according to the user's frame and data used with full knowledge of the facts. Those quantities are called data quality dimensions and are introduced in this section. Notions on the assessment of the quality of data are also presented, alongside with means for the improvement of data quality that can be used and the problems which can be met with the use of poor quality data.

2.1.6.1 Internal and external quality

The qualities of a product can be divided in two parts, the external quality, which is the quality from the point of view of the user and internal quality, which is the qualities from the point of view of the supplier. External quality covers ease of use, robustness, openness, reliability, accuracy, conformity to the expectations, among others, so external quality can be considered as being the fitness for use. Internal quality lies on concision, cohesion, clarity, generality and simplicity, among others (Devillers, 2004).

(R. Y. Wang and Strong, 1996) divided data quality into twenty dimensions, separated in four categories:

- the accuracy of data: believability, accuracy, objectivity, completeness, traceability, reputation, variety of data sources
- the relevancy of data: relevancy, timeliness, value-added, ease of operation, flexibility, approximate amount of data

- the representation of data: interpretability, ease of understanding, concise and consistent representation
- the accessibility of data: accessibility, access security and cost-effectiveness

In order to assess internal quality, a comparison must be done between two sets of data. The first set is the set of data actually provided by the supplier and the second set is a virtual ideal set the supplier would have produced (without any error), called the domain of discourse. The identification of similar patterns enables the identification of the same phenomena in the two sets. As an absolute comparison is almost impossible, some criteria must then be chosen in order to assess the quality of data such as data genealogy, spatial, temporal and semantic accuracy, completeness, or consistency (Devillers, 2004). Data genealogy being the description of the history of a data, its life cycle if known, from the acquisition or data input to its compilation with other data, and the varieties of its current form (Certu, 2010).

For the transmission of data quality information, *metadata* are often used, however their use and understanding is not easy, even for experts.

Internal quality can be described by answering the question: "*how can I measure the quality of my data and how can I signify it?*" It is the intrinsic quality of a data set established through rules. It is an absolute technical quality.

External quality can simply be defined as the fitness for use, which worth answering the question: "*what are the needs of the user on data quality and information quality and how can I give it in order to prevent them from having an abusive use of them?*". External quality is more difficult to assess because of the multiple and various needs, and the purpose of linking data and their use, data producers' concerns and users' expectations. External quality is the ability to fulfil a particular need, and is a relative use quality.

External quality is defined by (Pierkot et al., 2011) as "*the suitability of the specifications to the user's requirements. It is measured by the difference between the resource wished for by the user and the resource which has actually been produced*".

It is a close concept to data relevance. On the one hand, a proper assessment of data external quality requires some information about data usage, and on the other hand, external quality can be defined "*as the proximity between data characteristics and needs of a user for a given application at a given time*" (Pierkot et al., 2011).

In the literature, two approaches are used for an external quality assessment: the risks of the use of inadequate data and the analysis of the use of *metadata*.

2.1.6.2 Quality dimensions of data

Considering an attribute a of an entity e, its standard value is v. The accuracy of a v' value would be the degree of closeness of $(v' - a - e)$ with respect to $(v - a - e)$. If the value $v' = v$, the accuracy is maximal and the value is said to be correct. As it is possible to determine accuracy, it is also possible to determine inaccuracy, which would be the degree of difference between the actual value and the correct value.

One problem of the determination of accuracy is the notion of correct value. Sometimes, the correct value may not be defined in a unique way, or it can be undefined. Even when a standard value is possible, the calculation of the accuracy may not be obvious, for instance with the words, or the binary values. Sometimes the determination of accuracy with numbers can cause some problems. So the quantification of accuracy or inaccuracy of a value is a non-trivial task (Fox et al., 1994).

The precision of data does not directly refer to data but to the model in which data is displayed. It is a measurement of the degree of detail of the classification of possible values for data. For instance, when a temperature is measured, is the value rounded at the unit level, or at the one-tenth of degree level; or when a height is measured, it is using feet or inches; or when a colour scale is used, does this scale have 16 or 256 possible values.

The reliability of data in a database is defined in (Brodie, 1980) as "*a measure of the extent to which a database can be expected to exhibit the externally-observable structural properties specified for a database*". It is the process of validation that leads to reliability, *i.e.* the checking that the values in the base obey to the rules defined in the outline. It is a measure of robustness, which is the assessment of absence of system failures.

As for the currentness, a datum, by its nature, represents a value at a given time. As most objects evolve with time, the value can evolve as well. A datum true at a given time t is either up-to-date or out-of-date at another time t'. The change over time of a value can create inaccurate out-of-date data in data, and the notion of currentness can measure the degree of how far out-to-date the datum is (Fox et al., 1994). This property can be expended to an entire database for the measurement of its currentness. False data is neither up-to-date nor out-of-date.

A distinction must be done between data evolving by nature (such as the age of a living person), data likely to evolve (such as a salary), data that may change (such as name or address), data unlikely to change (gender or country of birth) and permanent data (date of birth, blood type).

Given the age of a datum, the probability for it to remain up-to-date after a certain time will depend on which category it belongs, among other parameters.

The completeness of a database represents the proportion of triplets where a value which is supposed to exist is actually filled in. It can be seen in a binary mode, *i.e.* yes if every single possible value is filled in and no otherwise; or in a measure of completeness by measuring the fraction of filled in fields with respect to the highest possible number of filled in fields (Fox et al., 1994).

In databases, a special element called *null* is used when an attribute in non-applicable (maiden name for a male person), when the attribute is of unknown applicability (the name of spouse field requires the marital status), or when the attribute is applicable but the value unknown (for instance the marital status, always applicable).

Completeness is linked to the fact for a database to contain all the relevant data (Huh et al., 1990) for a given use.

The duplication is the fact, for a database, to have identical triplets, or to have triplet

with the same entity and attribute, but different values (Fox et al., 1994). Some of those triplets can be irrelevant. The proportion of duplicate values can be measured as a characteristic of the database.

In a database, the values of the different terms must agree. The consistency is part of this agreement. A consistent database should have consistent values within, as well as unnecessary *null* values should be avoided. The consistency of the database can be measured in a binary yes/no mode, and the database will be consistent if all the constraints are fulfilled. A measure of the consistency can also be done by the measure of the fraction of consistent triplets in the database. The development of data dictionaries is one part of the consistency improvement, helping to the creation of translation rules between different representations of the same data or of closely linked data (Huh et al., 1990).

Moreover, the data can be accessible (the user can get access to the data, or not), interpretable (understandable from a syntax and semantic point of view), useful (for a user to be used in a decision process) and believable (R. Y. Wang, Reddy, et al., 1995).

Data integrity involves the recording of insertions, deletions and modifications of items.

The quality dimensions of external quality are different from the previous ones, are presented in (Pierkot, 2010) and displayed as follow:

- Intrinsic quality: determination of credibility, precision, objectivity and reputation that one can allocate to data.
- Contextual quality: verify if the data are suitable (relevance, added value) and sufficient (completeness, data volume) for the expected use.
- Representational quality: for the notions of interoperability and understanding of data

The last criterion is about the accessibility and the security of data. The use of metadata for the description of the user, its work and the material the user have to work is a perspective for improving the external quality.

2.1.6.3 Assessment of the quality

To assess the quality of a database, a method in four steps is proposed by (Huh et al., 1990). This data tracking method provides a measurement of the quality level of the process, a better control of the process due to the expertise about the database and an opportunity for improvement by identifying errors and inconsistencies. The goal is to identify the place where the error occurs in order to prevent future errors from occurring in the same way. Indeed, only the incoming data is assessed. The assessment of data already inside the database is made through audits of data (that can estimate error rates). The four steps are the sampling, the tracking, the identification of errors and quality control.

The sampling is done randomly in order to reduce the total amount of data to inspect. The tracking consists of giving a unique identification number to a field, so when the value of this field changes it can remain tracked. The identification of errors mostly

consists of changes in fields, which are a good indicator. The quality control consists of the verification of statistics by a comparison with objectives. Some process modification can be implied by the analysis of those statistics (Huh et al., 1990).

According to (R. Y. Wang, Reddy, et al., 1995), an assessment model of data quality should take into account when sources are original or intermediate. The authenticity and believability of data can be improved by certifications and inspections. The quality indicators must clarify data semantics when different databases which have the same values within do not share the same semantics. A better interpretation of *null* values is also possible, in the same scope.

It is sometimes difficult to assess the quality of digital data (Gervais, 2003). Unless physical data, digital data do not decay in a visible way, the use of remote computers prevent the users from giving oral warning about the quality of transmitted data. This difficulty is the source of errors, as people could choose to use an inappropriate set of data for a given purpose without knowing if the set is actually relevant to this use. It is a big issue for the quality of the work done on those sets of data, as the eventual quality of work is closely linked with the quality of original data.

The problem of the ideal set of data in the comparison made to assess internal quality is the proper definition of an ideal set. Depending on the field of work, the norms differ and can even be inconsistent within a field. The method of data specification can be defined by ISO norms for instance (such as ISO 8000 on data quality, ISO 19138 on data quality measures in geographic information, ISO 19157 on data quality in geographic information, ISO 21707 on data quality in intelligent transport systems, ISO 25012 on data quality models in software engineering or ISO 25024 on measurement of data quality in systems and software engineering), which tend to standardise such comparisons and internal quality assessments.

In order to improve this assessment, some tracks can be followed (Certu, 2010). The idea of a simplification of rules and norms can be put forward, with the risk of a weakened control. A major problem is the lack of data specifications directly from the sources, because of lack of time, of competence, of experience, of knowledge of customs. In this case, the solution would be to inform, train and help people in charge of those specifications by organising trainings, writing guide books, provide technical assistance and raise awareness among them.

So the question is also to determine if a threshold of minimum quality requirements should be put in place for the diffusion and the use of data, potentially constrained by law. Those threshold requirements could only be applied if an appropriate certification body is created alongside the rules.

The data producers should understand that the quality of the data they produce is linked to the actions built on the analysis of this data, and that erroneous data can lead to serious repercussions, involving up to the life of people trusting this data (Certu, 2010). The users also have a responsibility in a suitable use of data, and in the integration of the notion of uncertainty of the data they use. In order to do so, the awareness of the users should be raised on these problems.

What is the value of a decision based on data of which the quality is not known or

misunderstood by the users? As this is the cornerstone of the fitness for use concept, it is important to help the decision-maker to assess the external quality of data (Vasseur et al., 2005).

The notion of external quality, as previously stated in section 2.1.6.1, comes from the area of industrial production, and is defined in the world of geographical data quality since the 1980's as the ability of a set of intrinsic characteristics to fulfil requirements.

Few progress was made since that time and the assessment of the quality remains in the hands of the final user, who will judge on an intuitive way, based on the experience of the final user and on available information on the datasets, which are the *metadata*, which are a common means used for the assessment of the degree of fitness for use. However, notions of uncertainty visualisation become more and more important, being standard-based (on ontologies) or risk-based (on decision trees).

The fitness for use is an unclear, changing and complex concept. It evolves as the needs of the user do evolve, depending on the changing situation, and as the best quality is reached when difference between the actual condition of the data and the need to fulfil is minimal. Some characteristic are unclear, and depend on the people and the situation. For instance, up to what extent can data be considered as old? The usefulness of data is a concept which is difficult to define, as it varies from one user to another one, and a comparison would require a common frame (Vasseur et al., 2005).

Standards, such as ISO, help in the assessment of external quality from a qualitative as well as from a quantitative point of view. However, as those standards come from talks and agreements between institutions (often specialised), they offer a partial and possibly biased perception of reality.

2.1.6.4 Improvement of the quality

The quality of data is linked to the problems caused by heterogeneity in data representation, which lead to data misinterpretation. As the semantics for data is heterogeneous, they cause quality problems to this data.

When the same information is displayed in several forms in several databases, data quality indicators can decrease when those databases are merged because the heterogeneity of the semantics implies a non-matching merging, even though the data representing the same attribute have the same absolute value.

According to (Madnick and Zhu, 2006), the heterogeneities can be representational (*i.e.* the representation differs in different sources, e.g. the representation of the date, the different currencies, the metric or imperial scale), temporal representational (*i.e.* a representation that varies through time, e.g. when a country changes its currency), ontological (*i.e.* when two concepts slightly different are defined by the same term), temporal ontological (*i.e.* the meaning of a term, that can change over time), aggregational ontological (*i.e.* what does a term semantic implicitly embraces, so how far should the extent of this term go).

As the big data problematic becomes prominent in the society of information, it is

important to assess the quality of semantics in order to improve the general data quality.

2.1.6.5 Problems with poor data quality

The poor quality of the data can be a factor of risk worsening for some activities, and lead to disasters. As the decision one takes is based on available information, if data is of poor quality, so are likely to be the decisions based on this data.

In industrial databases, it is estimated in (Fisher and Kingma, 2001) that error rates of 30% are common, and can go up to 75%. In a certain environment, data quality is linked to the fitness of use, which is relative, whereas most of the characteristics are absolute. The format presented to the user and the relevance of this data has consequences on the value of the fitness of use. Moreover, (Agumya and Hunter, 1998) underline the strong link existing between the acceptable risk, the fitness for use and the risk response.

Some variables can influence the use of information by decision-makers: information overload, their experience level and time constraints. Information overload happens when the amount of information is too important for the time available to respond. When there is not enough time for processing the incoming data, the global quality decreases. The variables affected are the completeness (problems of filtering), accuracy (for erroneous responses given) and timeliness (outdated data can be entered in the base).

The experience level of the decision-maker has implications, as an experienced one would compensate the problems on intuition based on his prior experience. They are also more aware of the differences of quality in information they receive and deal with it more easily. However, they tend to rely too much on their feelings on the data, and they tend to take easily intuitive-based decisions, whereas the novices take more care of new information, and base their argumentation on more factual elements.

Time constraints often happen when the perceived granted time for a particular task is shorter than the time usually required. Decision-makers tend to be more selective, use only a subset of data or simplify the rules they use to follow in normal conditions.

When people have unsuitable data, they tend to reduce the uncertainty of information, reduce the harshness of loss in case of occurrence of an adverse impact, reduce the degree of utilisation of this data, higher the acceptable risk by taking further risk response measures (Agumya and Hunter, 1998).

In this section the concepts of information and data was discussed, leading to the definition and assessment methods of data quality dimensions. The use of those dimensions can be done in a study of data for various purposes. One of those purposes is the definition of normal or nominal behaviour for data, and thus the discovery of data that might not fit the normal, nominal or expected behaviour. Those events are called anomalies and their definition and their detection is the purpose of the section 2.2.

2.2 Anomalous events and anomaly detection

The anomaly detection is an important part of every data-related study. However, prior to any study, as the assessment of an anomalous thing is a relative assessment, a normality must be established and a distance (which is not required to be a metric) must be chosen for distance computation and thresholding criteria must be put in place for an actual discrimination of anomalies. This section presents the preliminary steps, some anomaly detection methods, as well as the purposes and limits of anomaly detection.

2.2.1 Definition of an anomaly

In general, an anomaly is defined as a deviation from a norm, and by extension as a measure of this deviation. It can be a oddity, a curiosity, an abnormal or anomalous thing, or an exception to the rule (Roy and Davenport, 2009). From an external operator, an anomaly will be a result which does not fulfil the frame of the results as expected by the operator, and considered as normal by this operator.

2.2.2 An introduction to anomaly detection

The goals of methods such as data mining, machine learning or statistical analysis are to drag all information within that are not explicitly delivered but which can nonetheless be found with a deep analysis, enabling the discovery of knowledge. More peculiar problems such as prediction from data, generalisation or synthesis of data can then be arisen. Anomaly detection raises slightly different questions, and consists in a study leading to knowledge discovery as well as to classification, class description or relations dependency description. Then, on a dataset, the purpose is to ascertain which pieces of information do not belong to the norm and which ones show appeal for a further deeper study.

Anomaly detection is used in a great number and diversity of contexts, from the detection of unusual images from motionless video surveillance images to the identification of defects in materials, including data cleaning. In the case of AIS messages, we are interested in this last application, however in most cases, the method remains the same, with the same elementary steps (Davidson, 2001) which are:

- The identification of the 'normality' characteristic by computation and the determination of data classical behaviour signature
- The determination of measures for the computation of the distance from the classical behaviour
- The determination of thresholding criteria, enabling to decide the normality, the abnormality, the degree of normality, the degree of abnormality of a datum, with the computation of the distance to the norm computed with the chosen measure.

For each of those steps, there is a multitude of possibilities, more or less suitable for data analysis according to the application area to which data belong.

The fact to find out the characteristics of data, the signature of the data, consists in the discovery of its model, which constitutes its normality. Methods for the determination of what is legitimate from what it is not widely varies according to data type and application area. Similarly, criteria for the determination of whether or not a datum belongs to the norm is peculiar to the application domain. In some cases, data in which only one variable differs from the norm will be considered as anomalous whereas in other cases, a given difference to the norm, even of all variables, is tolerated and the given piece of information will not be considered as anomalous. However, it is necessary to note that the measures used for the determination of the distance from the norm (and thus the normality or anomalous characteristic of the datum) widely differ according to the application domain and the type of data, and it is necessary to ever relate to this application domain for all kinds of comparisons. Then, some exclusively numeric data will only undergo some statistical methods or Minkowski-like distance types, whereas others will need to use, given their non fully numeric condition, some techniques of character strings distance measures, or on some numeric pieces of information that do not stand for a physical quantity. A semantic metric would then be used.

2.2.3 A preliminary step to anomaly detection

The purpose of those steps is to have available an understanding of the situation, or some pieces of information on the situation that would enable to have the more complete and the more continuous possible view (at once in temporal continuity and in density). Those steps are information acquisition and information fusion.

Anomaly detection largely lies on information gathering, as well as on intrinsic quality and amount of data. A part of anomaly detection work can be done at this level, with the finding of extreme values or non consistent data.

As different sources can disagree with each other, fusion is a challenge for correlation and association of data coming from different sources, taking into consideration their respective levels of confidence. Large discrepancies between sources can be considered as an anomaly.

Moreover, the nature of input data is various, and is generally a collection of several instances (referred as record, object, point, vector, event, pattern, case, sample, entity or observation), each instance being represented by a set of attributes (referred as features, dimensions or variables). The attributes themselves can be of different kind, binary, textual, continuous, numeric representing a physical quantity, numeric representing a choice in a given list or categoritical.

Several anomalies are distinguishable: the point anomalies, where an individual instance is considered as being anomalous with respect to the rest of data; the contextual anomalies, where an instance is not anomalous in a general assessment but which becomes anomalous when the context is cleared; the collective anomalies, where the data considered separately are not anomalous by themselves, but their occurrence together makes an anomalous collection (Chandola et al., 2009).

2.2.4 Several methods of anomaly detection

As seen before, pattern discovery is crucial in anomaly assessment, as a pattern is by definition built of recurring elements the repetition of which is predictable (Martineau and Roy, 2011). The terms of anomaly, nonstandard, outlier or unusual will be used for all piece of information out of the frame, that does not belong or seem not to belong to one of the clusters formed by the pattern analysis. Such a pattern can be a succession of events as a sequence, a cluster or a statistical distribution. If this pattern evolves over time, it follows a dynamic model, otherwise it is said static. Several main kind of methods are distinguishable, among which statistical methods, neural networks and machine learning.

Statistical methods are simple to implement but have the disadvantage to see their application restricted to peculiar problems. For instance the processing of the speed of vessels is simple because extreme values are likely to be anomalies. Those techniques tend to have a high rate of false positives due to the difficulty in the choice of a correct threshold between normal and anomalous values. If anomalies are *de facto* uniformly distributed in the sample, statistical methods are ineffective. A discrimination is done between the parametric methods, unsupervised and where anomalies follow a law of distribution and the non-parametric methods, used for automatic anomaly detection where no hypothesis is done on anomalies repartition, and where additional resources are needed.

Neural networks are particularly well adapted to hidden patterns, and are able, in the data, to find out classes with complex boundaries. A stage of leaning is necessary before the right operating of the neural network as a classifier. However, data must be processed several times by the system before a convergence towards a solution occurs. Moreover, their operating is often arcane (of black box type), and very sensitive to the learning stage (Martineau and Roy, 2011).

The principles of machine learning are to discover complex structures and take decisions based on data in an automatic way. Those methods are numerous and include decision trees, genetic algorithms, Bayesian networks, neural networks or clustering, amongst others.

2.2.5 The importance of the context in the hazard assessment

During the determination of the normal or abnormal nature of a datum, it is useful to take into consideration the environment (Martineau and Roy, 2011). Indeed, a situation can look anomalous whereas external information can explain such an abnormality. In the same way, a datum looking normal can become anomalous with the study and use of external pieces of information. Those additional pieces of information are of paramount importance for the contextualisation of data, and their understanding, paired up with their use, can increase the total degree of understanding of the environment. However this study, often quite complex, must generally be done or supervised by a human operator.

It is nevertheless necessary to note that an anomaly does not constitute a danger in all cases, and that anomaly detection is only one of the tools in hazard detection. The definition of what is a hazard is not unique, but some behaviours in the maritime domain such as terrorism, piracy, trade of illicit goods (such as drugs or weapons), areas violations,

pollution, illegal military manoeuvres or illegal fishing manoeuvres can fill this definition. In order to process the hazards in precedence order, a machine can help an operator to classify those hazards, by assigning to them levels of hazard (such as harmless, minor, weak, potentially hazardous in the long term, potentially hazardous in the short term, hazardous or highly hazardous). The importance of the designation of vessels of interest shall not be ignored, because the machine enables the operator to concentrate his work on a limited number of suspicious vessels or which might become a target due to their cargo. It is then a preventive detection of potential risks.

It is important that the machine displays information to the human operator in such a way that he or she can understand it easily, quickly and unambiguously. The generated warnings shall be concise and clear in order to bring the awareness of the operator on the situation as high as possible.

2.2.6 The purposes of anomaly detection

Operator's productivity shall be maximised as the maritime traffic ever rises, and the number of operators in charge of surveillance decreases. Thus, the fact to use the computation power of computers can enable a fast processing of the entirety of available data in order to smooth down the workload and provide to the reasoning capabilities of the human brain only the tasks that are non doable or non desirable to be done by the machine. The machine is then exploited for its brute force computing capabilities and the human operator for a subtle analysis of peculiar situations.

As the total amount of data is far too important to be handled by a human operator, only the relevant data shall be displayed to him or her, in order to offer him or her the best possible conditions for his or her choices to be right and justifiable, leaning on facts rather than on intuition (Martineau and Roy, 2011). Moreover, with respect to the humans beings, the computers are not subject to tiredness, and their capabilities do not vary over time.

As it is desirable to detect potentially problematical situations as early as possible, an alert shall be triggered from the moment where the situation, contextualised with available environmental data, can lead to a hazard in a plausible way. Similarly, all possibilities of hazard detection according to a sequence of events shall be taken into consideration as soon as the first steps of the sequence have already taken place.

2.2.7 The limits of anomaly detection

In the case of AIS messages, the environment of study which is the maritime environment is very complex, with a great amount of elements consisting of a great amount of agents, of which the capabilities are restricted. For instance, vessel tracking is an essential task for the understanding of maritime environment, and is relatively well developed. This tracking is in general based on the fusion of data from several sensors such as imaging devices, AIS and radar signals, but the coverage area of each of those devices is limited and varies (masks, weather) and thus limits the global knowledge of the situation. However

the perception of some elements that can be hazardous is limited (cargo, identities of mariners, identities of passengers for instance) which implies a limit of anomaly detection, because an hypothetically perfect analysis would require a full knowledge of the numerous components enabling to base the anomaly detection on a perfectly known interpretative framework.

As a conclusion to this section, we can say that once data has been labelled as more or less likely to be either normal or anomalous, the processing of data is not over, as the determination of patterns requires knowledge formalisation methods in order to be more efficient. Those methods allow data to be fitted into boxes so that patterns of anomalous data belonging to the same boxes could be highlighted in a more obvious way. The knowledge formalisation methods, which can in some cases run the processes by themselves, are presented in section 2.3.

2.3 Knowledge formalisation methods

In this section, two main knowledge formalisation methods are presented and distinguished: typologies and ontologies. Typologies divide domains of which data is about in subdomains in a tree-based pattern. There is no restriction of the number of layers (of granularity) but this method remains basic as it only offers data labelling. Ontologies, although they look alike, are not typologies as they are based on the concept of concepts and relations between the concepts, so classes and links between those classes, the links representing a given relation. As their structure is far more formalised than typologies, ontologies enable inference engine and the discovery of rules within data.

2.3.1 Typologies

The typologies are a family of methodological approaches for the definition or the study of a field, made in order to facilitate the analysis, the classification and the study of complex realities. The types contained in the typology constitute the elements which divide the main type into families that are generally mutually exclusive and collectively exhaustive.

Typologies can apply to domain as various as anthropology, theology, linguistics, archaeology, psychology or statistics. As long as there is a need for defining types from a greater phenomenon, typologies are useful. Such a classification of people or things is done on the basis of commonalities or by certain differences or particular features classified objects might have.

The use of typologies is useful in the sense of definition of families. By classifying objects according to their characteristics, it is possible to gather objects having similar characteristics in order to apply to them similar treatments. In addition, the fact to seperate the objects according to their characteristics enables, when a new object comes,

the fact for this object to be classified with respect to those elements, and to assign this object other functional characteristics derived from its belonging to a given type.

In each field of study, typologists define the main characteristics of the fields, *i.e.* the elements which will serve as a basis for types discrimination, the types being defined as being a "*holistic, schematized structure arising from a cluster of properties that exhibit preferred connexions among them*" (Shibatani and Bynon, 1999). The connexions in question having to be defined by typologists (according to their school of thought), leading to the drawing of the structure.

2.3.2 Ontologies

In this section, ontologies are introduced with first some definitions, their role and their typologies. Then their construction is evoked, with the various characteristics of ontologies to take into consideration. The used piece of software and the application of ontologies to our domain is then assessed.

2.3.2.1 Definitions

Ontologies arose from the thought that knowledge representation was important and that information shall no longer be considered only through the prism of data. Thus ontologies are today considered as an essential paradigm in the frame of semantic interoperability.

We are interested in the ontologies as a tool for artificial intelligence, so as to formalise knowledge integration within computer systems and lead to an automatic semantic handling of information, far away from the philosophical area to which ontologies traditionally belong to.

The generally admitted definition is the one of (Studer et al., 1998), which defines an ontology as "*a formal and explicit specification of a shared conceptualization*". The formalisation needs a standardisation to be manoeuvrable by a machine, the explication needs a declarative definition of the concepts and the constraints, the conceptualisation embraces the non-ambiguity of the terms and the abstractive side of the ontology, while the sharing part engenders the fostering of a consensual knowledge.

In a simplified way, ontologies can be considered as constituted of five elements: the concepts (representation of an actual object, of a notion or of an idea), the relations (possible interactions between concepts), the functions (connections in which an element is defined with respect to others elements), the instances (represent the subjects that constitute a tangible instance of the concept to which they belong to) and the axioms (statement true by definition on the subject).

2.3.2.2 The role of ontologies

In the case of information systems, ontologies have a function of unifying frame and knowledge repository. (Hepp, 2007) highlighted three fundamental points which gather

the interest for ontologies: communication (between humans, between machines and between humans and machines), computer-based inference (for representation and handling of pieces of information as well as for the analysis of the inputs, structures, algorithms and outputs of a system) and knowledge reuse (in the frame of an ontological structuration of an area).

Ontologies can be used at several levels as they are a medium of knowledge dissemination for all the components of a system. (Guarino, 1998) tallies seven of them, going from the analysis of the system (beforehand) to the processing of queries (afterwards), and going through maintenance or interoperability. In short, the role of an ontology is to specify a common language and a knowledge corpus about a given area.

2.3.2.3 Typology of ontologies

Ontologies types are numerous and list them is not much of interest. However the two typologies hereafter presented enable us to have a good overview of the different possible representations of ontologies, which are the discrimination according to the level of formalisation and the discrimination according to the subject of conceptualisation.

As for the level of formalisation, four types can be discriminated: informal ontologies that are expressed in natural language and easily understandable by the users, semi-informal ontologies with a linguistic semantic more structured and limited, semi-formal ontologies with an artificial language and formal ontologies which have a formal language and semantics.

A typology according to the level of conceptualisation can be defined by seven categories that match with the four levels initially proposed by (Guarino, 1998), plus the three additional ones proposed by (Gómez-Pérez, 1999). They are the high level ontologies (for the more generic concepts), the task ontologies (for a specific activity aside from all domain), domain ontologies (that describe the vocabulary peculiar to a given domain) and applicative ontologies (for the modelling of the concepts of a given domain in the frame of a given activity). In addition to them, the three categories proposed by (Gómez-Pérez, 1999) are the knowledge representation ontologies (that describe the generic concepts for the knowledge formalisation), meta-ontologies (with a lower level of abstraction with respect to high-level ontologies, allowing their reuse in several domains) and task-domain ontologies (for a peculiar task in a peculiar domain).

2.3.2.4 Representation languages

Under the impetus of the W3C (World Wide Web Consortium), standardised languages arose and heralded the semantic web. However from the 1990's some ontological languages were created, such as Ontolingua, Cycl, LOOM or Flogic. Some new Web-linked languages emerged since the rise in importance of the Web, up to put ontologies as one of the bases of the development of the semantic Web, foreshadowed as the future (or one of the futures) of the Web. In the late 90's, the Resource Description Framework (RDF) is the first standardised language created in the purpose of being a basis of the semantic Web (Berners-Lee, 1998). The principle is to use diagrams with subjects, predicates

and objects, with interconnections between those entities. An unified language exists although several syntaxes are coexisting, and a diagram-based representation was also created. However since the language is simple, its expressivity is not high enough to describe complex situations. That is why the W3C decided on the creation of a more expressive language: the Web Ontology Language (OWL).

The OWL is based on basic primitives describes by the RDF language, and brings all the needed semantics for the knowledge description (for instance for class comparison with mechanism such as equivalence concepts or symmetry). Three sub-languages of OWL with increasing expressivity are available: OWL Lite (which is RDF with the concepts of equivalence and simple constraints that can be specified by the user), OWL DL (addition of concepts such as disjunction or upgrading of some others such as cardinality, DL standing for description logics) and OWL Full (the most advanced version, kept for applications where a high-level of expressivity is primordial, at the risk of no longer secure the completeness of computations.

A rule-based language for the Web, the Semantic Rule Web Language (SRWL) uses OWL predicates so as to add rules that can be built or be produced by an engine.

2.3.2.5 Reasoning based on ontologies

Reasoning based on ontologies is done through an inference engine. It is a piece of software which has the purpose to verify the consistency and integrity of the ontology, to query the ontology or to deduce new pieces of information and new rules on the basis of a study of the knowledge base. Four inference engines (Fact++, KAON2, Pellet and RacerPro) implement the Description logic Implementation Group (DIG) protocol, which enables to get rid of the peculiarities of the different engines thanks to an unified communication interface based on HyperText Transfer Protocol (HTTP) queries.

2.3.3 Description logics

A knowledge-based system is done in order to solve a given problem by reasoning on a applicative domain, using various methods. The knowledge of the applicative domain is represented by entities which have a syntax-based description to which is associated a semantic meaning. In this frame, description logics have been built on predicate logics and semantic networks (Amedeo Napoli, 1997).

In the description logics formalism, a concept allows the representation of several individuals, whereas a role stands for a bilinear relationship between individuals. A concept stands for a generic entity of an applicative model, and an individual represents an instance of the concept, a peculiar entity.

Concepts and roles have a structured description, to which is associated a semantic in order to handle those concepts and roles. There are two levels where knowledge is taken into consideration: the terminological level for the representation and the handling of concepts and roles, and the factual level for the description and handling of individuals. Subsumption relationships allow the organisation of concepts and roles according to their

generality level and hierarchy of concepts (Amedeo Napoli, 1997). A whole A subsumpts a whole B if A is more general than B, so if all individuals in B are also present in A. Description logics play an important role in the description of topological relations (Roussey et al., 2013).

The syntax has several layers of complexity, as presented here, and is noted according to prefixed notation (known as German syntax). The first layer of complexity stands for the simplest concepts, and gathers the constructors representing the union (name: AND, symbol : $\cup$), the negation (name: NOT, symbol : $\neg$), the universal quantifier (name: ALL, symbol: $\forall$), the existential quantifier (name: SOME, symbol: $\exists$), the universe (name: TOP, symbol: Ω), the empty whole (name: BOTTOM, symbol: $\emptyset$).

The second layer of complexity will gather constructors such as the True statement (name: TRUE, symbol: $\top$), the False statement (name: FALSE, symbol: $\bot$), the intersection (name: INTER, symbol: $\cap$), the cardinality in the roles, the disjunction of concepts. The third layer is necessary for the predicate logics application: it is the union of elementary assertions, that can be represented by a pipe.

Other symbols exist, such as the equality or numerical identity ($=$), the inequality or numerical restriction ($\leq$ or $\geq$), the role transitivity, the fact to belong ($\in$), the role complement or the role composition ($\circ$) (Lefrançois, 2016).

Those concepts, roles and constructors gathered in a syntax enable the deductibility of systems by providing assertions that are understandable by machines and make unambiguous statement on the outcome of data treatments.

The combination of anomaly detection and knowledge formalisation methods provide labelled and assessed, their combination facilitate the use of knowledge discovery methods, presented in section 2.4.

2.4 Knowledge discovery

Knowledge discovery methods consist in the extraction of pieces of information from raw or partially refined data. In this section, data mining deals with high amounts of data, distances and similarities are presented and the determination of alert grades is proposed as a tangible implementation of knowledge discovery in the way people is led to behave.

2.4.1 Data mining

2.4.1.1 Overview

The machine learning methods can be of several kinds: deductive (mathematical modelling of the world which models, the description of which is computed) and inductive (use of past information). Inductive methods are twofold: top-down ones which base themselves on human experience and bottom-up ones which base themselves on the analysis of data (in databases or not).

The methods of data analysis are diverse (Idiri, 2013): statistic-based, visual, by clustering (of events or of groups of events, such as trajectories), and diverse as well are the modelling types: by inference rules, using ontologies, using Bayesian classifier.

Associations are used in traditional data mining and exploratory (monothematic) and decisional (multithematic) methods are use in spatial data mining. Trajectory clustering, with anomaly detection methods such as distance computation, angular analysis, periodic pattern detection (Idiri, 2013) is used in moving objects data mining. The number of parameters to take into consideration for the computation is large, and can vary largely if the world is open or if there is a constraining network.

2.4.1.2 Machine learning methods

As stated in (M. Chen et al., 2014), "*Traditional data analysis means to use proper statistical methods to analyse massive data, to concentrate, extract, and refine useful data hidden in a batch of chaotic datasets, and to identify the inherent law of the subject matter, so as to maximize the value of data*". The analysis can be done real-time or offline. The real-time one needs the adaptation to constantly changing, rapidly analysed data, with short to very-short delayed analyses. The next paragraph presents some methods (M. Chen et al., 2014) that can be used.

Cluster analyses are statistical methods in which objects are grouped and classified according to some features. The categories in which are divided the objects are the clusters such as the objects which are in the same cluster will display high homogeneity while objects in separate clusters will display heterogeneity. It is an unsupervised method without training data. Factor analysis is the fact to group several closely related features into one, in order to reduce the number of variables to take into consideration. Correlation analysis is an analytical method in which the dependence relations and the correlations, in which fluctuations of similar shape are recorded through several objects. Regression analysis is a mathematical tool for the revelation of correlations between one given variable and several other variables. A/B testing, or bucket testing, is a method in which comparisons between groups are done by applying different analyses to the same sample. Statistical analysis, as stated before, is also used, based on statistical theory, with phenomena such as randomness or uncertainty modelled, done for summarisation of datasets (in descriptive statistical analysis) or give clues for a subject in which random variations occur, and lead to a decision (in inferential statistical analysis). Last, data mining algorithms are a process for the extraction of information that can be potentially useful but which is hidden or unknown. Some of them are k-means, Apriori, Naive Bayes, amongst others. They are used for all important problem solving cases, such as clustering, classification, statistical learning, association analysis, linking making or regression.

2.4.1.3 The curse of dimensionality

Nowadays, highly dimensional data is widespread, and in data pre-processing, feature selection is one of the most important steps (Kumar and Minz, 2014). It consists in the fact to detect the relevant features and to remove the irrelevant, noisy or redundant ones. The principle is in general to find the subset of features that presents the best

commitment with the number of features and the coverage they offer. The computation time highly relies on the number of dimensions, and it can go exponential with them, that is why dimension reduction is often needed in order to avoid what is called the curse of dimensionality, which leads to the impossibility to carry out the analysis.

The general procedure for such a selection has four steps which are subset generation, subset evaluation, a stopping criterion for subset generation and evaluation loop and a result validation. In order to assess their relevance, relevancy criteria must be put in place, with an evaluation of degree of relevancy and thresholding for the selection.

Six methods are proposed by (Kumar and Minz, 2014) such as relevance to the target, strong relevance to the samples, weak relevance to the samples, relevance as a complexity measure, incremental usefulness and entropy relevance.

For feature selection, a general procedure is defined, with the search organisation being described as being either sequential, exponential or random; the successor generation is done with five main operators: forward, backward, compound, random and weighting. The evaluation of the subset can be done using different criteria: distances, divergence, uncertainty, probability of error, dependency or consistency measures can be used.

A selection of algorithms is proposed in (Kumar and Minz, 2014) taking into consideration the search strategies (exponential, sequential or random), the data mining tasks (classification or clustering) and the evaluation criteria (distance, information, dependency and consistency).

2.4.2 Distances and similarities

This section displays some useful distances and similarities. What distinguishes distance from similarity is that distance is a value quantifying the value between two points in a given metric while similarity is a value of how much data look alike (same values, same evolution, same ordering, amongst others).

2.4.2.1 Distances

As stated previously, the anomaly is defined as a distance to normality, and the computation of this distance needs the use of some metrics adjusted to the study frame. This section, inspired by the work of (Etienne, 2011), proposes an overview of some available metrics.

2.4.2.1.1 Minkowski distances Minkowski distances are particularly well fitted for the computation of quantitative data distances. Those distances are linked to a norm, which is an integer superior or equal to 1. Thus the distance in the p-norm between two vectors of data (the elements of which are the variables representing the quantities to compare, *i.e.* position or speed) is computed as the p^{th} root of the sum of the norms put to the power p of absolutes values of the differences of the values. The obtained result can enable the creation of a similarity between the two vectors of data. The most used norms

are three: norm 1 for Manhattan distance, norm 2 for Euclidian distance and norm ∞ for Chebyshev distance.

Let $p \in \mathbb{N}^*$ be the norm, let $n \in \mathbb{N}^*$ be the coordinates vector dimension, let $i \in [\![1\ ;\ n]\!]$, let A and B be two points, let $x_A \in \mathbb{R}^n$ be the vector of coordinates of point A, let $x_B \in \mathbb{R}^n$ be the vector of coordinates of point B, let d_{mk} be the Minkowski distance, let d_M, d_E et d_T be the Manhattan, Euclidian and Chebyshev distances,

$$d_{mk}(A,B) = \left(\sum_{i=1}^{n}(|x_{A_i} - x_{B_i}|^p)\right)^{1/p}$$

$$d_M(A,B) = \sum_{i=1}^{n}|x_{A_i} - x_{B_i}|$$

$$d_E(A,B) = \sqrt{\sum_{i=1}^{n}(|x_{A_i} - x_{B_i}|^2)}$$

$$d_T(A,B) = \max_i(|x_{A_i} - x_{B_i}|)$$

Manhattan distance is induced by norm 1, it consists of the simple sum of the absolute values of attribute values differences. Euclidian distance corresponds to norm 2, and matches to the widest common and mainstream definition of the term distance in the reasoning in 1, 2 and 3 dimensions. At the limit, in $+\infty$, Chebychev distance is the Max of absolute values of the differences of attribute values.

The AIS transmits positioning data in the geodetic reference frame WGS84. In this case, we have two possibilities: compute the distance directly from latitudes and longitudes or use the cartesian coordinates and compute a Minkowski distance (Euclidian in general) in the plane.

Let A and B be two points, let (φ_A, λ_A) and (φ_B, λ_B) be the latitudes and longitudes of A and B in rad, let $R \in \mathbb{R}$ be the radius of the Earth, in meters, a, b, $d_{ortho} \in \mathbb{R}^3$ then $\forall(\varphi_A, \lambda_A, \varphi_B, \lambda_B) \in [0; 2\pi[^4$, the distance d_{ortho} of the minor arc of great circle (orthodromy) linking A and B can be computed as:

$$d_{ortho}(A,B) = R \cdot b$$

$$a = \sin^2\left(\tfrac{\varphi_B - \varphi_A}{2} + \cos(\varphi_A)\cdot\cos(\varphi_B)\cdot\sin^2\left(\tfrac{\lambda_B - \lambda_A}{2}\right)\right)$$

$$b = 2 \cdot atan2(\sqrt{a}, \sqrt{1-a})$$

2.4.2.1.2 The Mean Distance The mean distance is about two lines, or two trajectories. The actual trajectory and the standard trajectories for instance, can be compared this way. Its computation is not unique but a widespread version consists in the fact to consider one of the lines as a reference, draw segments between the extreme points of the lines and divide the area of the surface between the two lines by the length of the reference line. The result is expressed in units of length and represents the mean distance of the second line with respect to the reference line. A graphical representation of the mean distance is displayed in Figure 2.1.

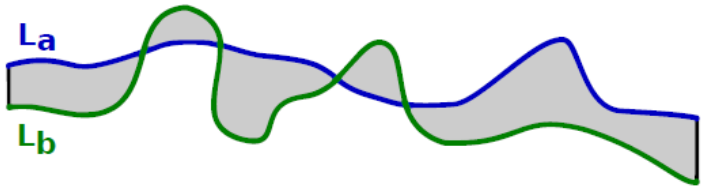

Figure 2.1: Mean distance computation by area method, from (Etienne, 2011)

The applicability of this distance is nevertheless limited to spatiotemporal trajectories and to trajectories for which the footprint are similar (in order to have a distance that makes sense).

2.4.2.1.3 Hausdorff Distance Hausdorff distance is the maximum distance between two lines, as defined by the following formula:

Let L_A and L_B be two lines, let p_A and p_B be two points such as $p_A \in L_A$ and $p_B \in L_B$ let $d(p_A, p_B)$ be the distance between the two points, whatever the norm used, let $d_H \in \mathbb{R}$ be the Hausdorff distance, computed as:

$$d_H(L_A, L_B) = \max\left(\max_{p_A \in L_A}\left(\min_{p_B \in L_B}\left(d(p_A, p_B)\right)\right), \max_{p_B \in L_B}\left(\min_{p_A \in L_A}\left(d(p_A, p_B)\right)\right)\right)$$

We can define its determination as follow: let L_1 and L_2 be two lines. Amongst all points of L_1, which one is the farmost from any of L_2 points? Let name it p_1. Amongst all L_2 points, which one is the closest to p_1? Let name it p_2. Let D_1 be the distance between p_1 and p_2. We can determine D_2 by reversing the respective roles of L_1 and L_2. Hausdorff distance will then be $Max(L_1, L_2)$, as presented in Figure 2.2.

In order that Hausdorff distance makes sense in a spatiotemporal analysis of trajectories, and as it is shown in Figure 2.2, it is necessary that compared lines have quite similar footprints and quite similar shapes. Indeed, this distance is a bad indicator for very twisting and turning lines, close spatially , due to the fact that the notion of homologous points in the trajectories are not taken into consideration.

2.4.2.1.4 Fréchet Distance Fréchet distance is a distance corresponding to the maximal distance between two spatiotemporal lines. It is defined as follow:

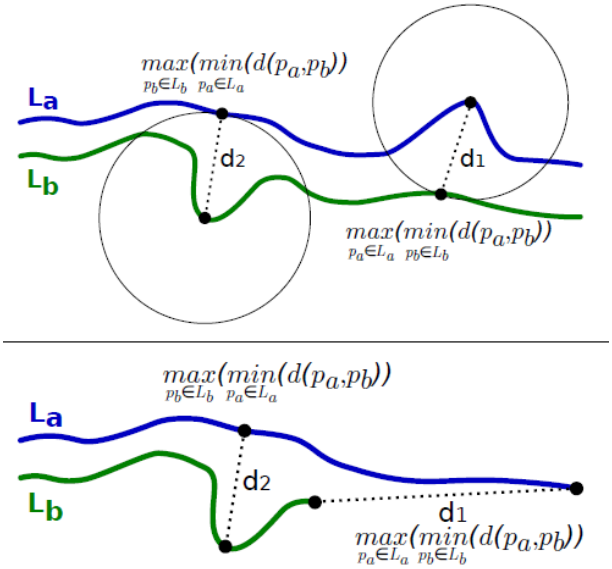

Figure 2.2: Hausdorff distance calculation sketch. Up: with similar footprints. Down: With different footprints. From (Etienne, 2011)

Let S be a metric space, let $d(a, b)$ be the distance between two points a and $b \in S^2$, whatever the norm used, considering a line as a row of points being equivalent to a C^0 function of S, let $a, a', b, b' \in \mathbb{R}^4$ be as $(a < a'), (b < b')$, let the line L_A be depicted by the continuous function $f : [a, a'] \mapsto S$, let the line L_B be depicted by the continuous function $g : [b, b'] \mapsto S$, let $d_F(f, g)$ be the Fréchet distance, the expression of which between two lines L_A and L_B is as:

$$d_F(f,g) = \inf_{\substack{\alpha:[0,1]\mapsto[a,a'] \\ \beta:[0,1]\mapsto[b,b']}} \left(\max_{t\in[0,1]} \left(d(f(\alpha(t)), g(\beta(t))) \right) \right)$$

An illustration of this distance can be done with the analogy of a master going for a walk with his dog. The two lines are then defined as being the ends of a lead of length l. The Fréchet distance L is then defined as being the lowest value of l allowing the movements to occur. The computation of this distance suffers from the representation of continuous spatiotemporal trajectories, making its computational complexity quite important, as $\mathcal{O}(N_a \cdot N_b \cdot log^2(N_a \cdot N_b))$, N_a and N_b being the number of segments of the two lines, which restricts the computations. Some similar distances exist, such as the discrete Fréchet distance, hereafter presented, or the mean discrete and partial discrete Fréchet distances.

The discrete Fréchet distance is an approximation of the Fréchet distance enabling to reduce the computational complexity to $\mathcal{O}(N_a \cdot N_b)$. The trajectories are discretised under the form of M and N points, respectively. Thus each point of a trajectory is paired to a point, the closer, of the other trajectory (homologous points). It is then formed $R = Max(M, N)$ couples of which the Max is the discrete Fréchet distance.

2.4.2.1.5 Edit Distance This distance is used in the case of character strings, and the value of the edit distance between two character strings is the number of elementary operations necessary in order to change one string into the other one. There are different types of edit distances, giving more or less weight to the different possible operations which are the insertion, the removal and the substitution.

The Levenshtein distance is one of the most famous, giving the same weight of 1 to all three operations. The distance between two sequences of length i and j is computed according to an iterative formula and has a computational complexity of $\mathcal{O}(i \cdot j)$.

Let A and B be two character strings, let $i, j \in \mathbb{N}^2$ be the respective lengths of A and B, let $d_L(A, B)$ be the Levenshtein distance, computed as:

$$d_L(A_{1...i}, B_{1...j}) = \left\{ \begin{array}{cc} j & \text{if } i = 0 \\ i & \text{if } j = 0 \\ d_L(A_{1...i-1}, B_{1...j-1}) & \text{if } i, j > 0 \text{ et } i = j \\ 1 + \min \left(\begin{array}{c} d_L(A_{1...i-1}, B_{1...j-1}) \\ d_L(A_{1...i-1}, B_{1...j}) \\ d_L(A_{1...i}, B_{1...j-1}) \end{array} \right) & \text{else} \end{array} \right\}$$

2.4.2.1.6 The longest common subsequence This distance measure compares two successions of elements and counts the longest succession of common elements. It can be computed on textual elements as well as on numeric elements provided that a thresholding is done on the latter in order to be able to consider slightly different elements as being equals in this computation.

2.4.2.2 Measures of similarity and dissimilarity

(Goshtasby, 2012) sums up some similarity and dissimilarity measures that could be used in our study.

A similarity measure must produce a higher value if the dependencies between the values in the series increase. A metric similarity must satisfy the following properties: limited range, reflexivity, symmetry and triangle inequality.

A dissimilarity measure must produce a higher value as the corresponding values in the series are less dependent. A metric dissimilarity must satisfy the following properties: non-negativity, reflexivity, symmetry and triangle inequality.

A similarity or dissimilarity measure can be effective without a metric, although it is desirable. There is a large number of similarity or dissimilarity measures, each having its advantages and its drawbacks.

2.4.2.2.1 Similarity measures The Pearson correlation coefficient allows the comparison between two sequences of numbers. Its range goes from -1 (which represent a

perfect negative correlation) to +1 (which represents a perfect positive correlation).

$$r = \frac{\sum_{i=1}^{n}(x_i-\bar{x})\cdot(y_i-\bar{y})}{\left(\sum_{i=1}^{n}(x_i-\bar{x})^2\right)^{1/2}\cdot\left(\sum_{i=1}^{n}(y_i-\bar{y})^2\right)^{1/2}}$$

The Tanimoto measure is a measure between two vectors X and Y and is defined as follow, where the numerator represents the inner product of the vectors and the denominator represents the inner product plus the square Euclidian distance between the vectors. X^Tdenotes the transpose vector of X.

$$S_T = \frac{X^TY}{\|X-Y\|^2+X^TY}$$

The stochastic sign change is done in case one of the two vectors contains noisy information, if they are similar, their differences tend to change sign often. The larger the number of sign changes, the higher the matching between series will be.

The deterministic sign change is a similarity measure which is similar to stochastic sign change except that this time the noise is voluntarily added in one of the two series. The amplitude of the noise must be chosen based on the results or on the standard deviation of the series.

The Spearman's ρ represents a rank correlation: the values within the vectors are ordered (according to an ordering law), ties for discrete values are broken. Then the Pearson correlation formula is used replacing the values by their ranks in order to obtain Spearman rank correlation. Compared to the Pearson correlation coefficient, the Spearman's ρ is less sensitive to outliers. Assuming that $R(x)$ represents the rank of the value x, once all values are ordered, the formula is:

$$\rho = 1 - \frac{6\cdot\sum_{i=1}^{n}(R(x_i)-R(y_i))^2}{n\cdot(n^2-1)}$$

The Kendall's τ is another measure of similarity. In the two series that are compared, a large number of pairs can be done. The sign of the corresponding pairs in the two series are either the same or different. If the sign is the same, the pair is said to be concordant, if the sign is different the pair is said to be discordant. Kendall's τ is then defined as follow, with representing the number of concordant and discordant pairs, respectively.

$$\tau = \frac{2\cdot(N_c-N_d)}{n\cdot(n-1)}$$

The mutual information is another form of similarity measure, linked to the entropy. As there are different kinds of entropy, there are different kinds of mutual information, such as Shannon's, Rényi's and Tsallis'. The value, assuming that $p(x,y)$ is the joint probability distribution function of x and y and where $p(x)$ is the marginal probability distribution function of x, is:

$$I(X;Y) = \sum_{y\in Y}\sum_{x\in X} p(x,y)\cdot log\left(\frac{p(x,y)}{p(x)\cdot p(y)}\right)$$

2.4.2.2.2 Dissimilarity measures The Manhattan, Euclidian and Chebychev norm seen above are dissimilarity norms. In the case of Manhattan and Euclidian cases, instead of taking the sum of the absolute value of the differences, it is possible to take the median of the absolute value of differences, for the two measures called median of absolute differences and median of square differences (Goshtasby, 2012).

$$MAD = med_{i=1}^{n}|x_i - y_i| \; MSD = med_{i=1}^{n}(x_i - y_i)^2$$

The rank distance is defined as the Manhattan norm of rank ordered (according to a ordering law) values of both vectors, and ties are broken. Rank distance ranges from 0 to 1, and the distance will be as small as the dissimilarity between the values is low. It is computed as follow:

$$D_r = \frac{1}{n} \cdot \sum_{i=1}^{n} |R(x_i) - R(y_i)|$$

The exclusive information is a dissimilarity measure linked to the concept of entropy, and goes up as the mutual information goes down.

2.4.3 Modelling and determination of risk levels

This section presents the various ways in which it is possible to set risk levels and alerts, with first the definition of an alert, and then the way alert levels are produced.

2.4.3.1 The alert

An alert is a warning given to someone in order to be on the lookout, it is a notion supplied by a source entity notifying to the target entity a piece of information that could be of interest and bearing the fact to be on the lookout with respect to an event of which the occurrence is considered. Source entities can range from a single individual to an *ad hoc* structure, e.g. a piece of software, a computer program automatically displaying alerts when given conditions are gathered; and target entities can as well range from a single individual to the whole population, passing through intermediate elements such as a group of individuals selected according to relevant features with respect to the domain in question (feature criteria can be geographical, sociological, political, ethnic, amongst others).

The alert aims at the establishment of means allowing the wanted response to a peculiar warning to be organised. Yet, in order to adjust the proportions of the means to the actual situation, alert levels can be set up, as levels enable a gradation of the risk and an adjusted response.

2.4.3.2 Production of alert levels

The production of the standards leading to alert levels is important in the establishment of a graduation, and some elements must be taken into consideration during this establishment. Those elements are the Why, the How, the Sources, the Determining of the right level of action and the element to consider for the announcements.

2.4.3.2.1 The Why The Why is about the purpose and the targets. It is necessary to ask oneself what is the purpose of the establishment of alert levels, and build those alert levels with these objectives in mind. Similarly, the establishment of alert grades must take into account the recipients, and their implementation will vary with respect to the target audience (for professionals or mainstream for instance). The grades of alert must be clearly understood by the targeted audience, with unambiguous alert grade labels, and the description of actions to do, if necessary, must be precise and concise. Pieces of information for the attention of targeted people must then reach those people undamaged, with clear actions to do in order to reduce the risk of feared event occurrence.

2.4.3.2.2 The How The How must underline the importance of the graduation, and the granularity of the graduation. If indeed some cases will need a great amount of alert levels, some others will only need few of them. In general, the production of alert levels needs on the one hand events which will lead to the triggering of an alert level and on the other hand measures for risk mitigation. Thus, the number of levels must be chosen in line with several parameters: the evaluation of how much parts (or levels) can the events be divided into can be done, with the purpose of proposing a number of levels enabling the coverage of all the spectrum of gravity of this event and at the same time displaying a significant difference between those levels, such as the doubts that an operator could have according to the right level for any on-going action would be reduced at most; and it is necessary that the measures needed are different enough so that the existence of several levels is legitimate.

2.4.3.2.3 The Sources The sources of the events leading to the production of alert levels are numerous, and their diversity must be taken into account during the process of this production. Three main categories are distinguishable: hazards, threats and activities. Threats are events in which the will to harm is declared, typically the terrorism lies within this category. The activities are the events for which the action taken can have harmful impacts such as street demonstrations, meetings in stadia, area occupations. Hazards are events for which risk is pending but which do not result from any human action, such as earthquakes, tidal waves or storms. The causes of those events being diverse, the response provided in the alert levels must be adapted to the considered case. This adaptation needs the a priori knowledge of the target audience which will actually use those alert levels.

2.4.3.2.4 The Determining of the right level of action The determining of the right level of action is a key element linking the causes leading to the application of a given alert level and the actions taken to mitigate the risk. In particular, it is important

that the actions are in line with the events they are supposed to mitigate. To fulfil this point, it is important to avoid the phenomena of under-protection and over-protection. Over-protection is the fact to use actions that are too important for the situation, and this must be avoided for financial reasons, because of the inefficiency and the uselessness of the taken measures and the possible obstacles to normal operations that those measures can bring. However, over-protection must not be confused with precautionary principle, as the precautionary principle applies in a predefined frame. On the contrary, under-protection consists in the deployment of insufficient measures to mitigate the risk of a given alert level. This can impact directly the security and safety of normal operations and an distorted vision of the reality by the target audience. A case of under-protection can be a proof that a problem lies in the mechanisms leading to a rise of the alert level. The cost of the decision must also be taken into consideration, assessed and if possible roughly set in advance, so that the operator is aware of the cost of the choice he or she makes.

2.4.3.2.5 The elements to take into account for the announcements The elements to take into account for the announcements encompass all the characteristics the knowledge of which is useful for an efficient communication. For the audience, it must particularly target people for whom the knowledge of the information is primordial, and secondarily people for whom the knowledge of the information can be of interest. It must avoid the communication of pieces of information to people for whom those pieces of information would be useless and as much as possible giving priority to people for whom it is of some interest. The way the message is formulated is important in alert levels messages as the target audience is possibly to be in an urgent situation, with no time for processing information. Thus it must be short, concise, clear, with no room for ambiguity. Last, the definition of communication means is important as it is the conveyor on which the pieces of information are transmitted. This conveyor must take the environment and the target audience into consideration, must transmit the pieces of information without degradation and its reliability must be, if not maximum, at least known.

Conclusion

In this second chapter, we saw the origins of information concepts and the various data quality dimensions that are used, and in particular integrity, noticed as especially important in anomaly detection cases. Anomalies were defined and anomaly detection steps displayed as well as the methods, purposes and limits of anomaly detection. The knowledge formalisation methods presented the typologies, ontologies and description logics and the knowledge discovery methods highlighted data mining and distances for metrics determination, necessary for thresholding anomaly detection cases. The modelling and the determination of risk levels was presented, as detected anomalies can be assessed from the point of view of risks associated with those anomalies.

This second chapter consisted of a presentation of information systems in general, as well as means to study, assess and classify them. The next chapter will present a peculiar information system, the AIS, which is the one we are interested in for our system assessment and risk analysis.

Chapter 3

The Automatic Identification System

Chapitre 3 : Le Système d'identification Automatique

Mis en place par l'Organisation maritime internationale dans la version de 2002 de la convention pour la sauvegarde de la vie humaine en mer, le système d'identification automatique (AIS) concerne de façon obligatoire tous les navires de plus de 300 tonneaux engagés dans des voyages internationaux, tous les navires de charge de plus de 500 tonneaux ainsi que tous les navires à passagers. Cependant tous les navires peuvent être équipés d'un émetteur-récepteur AIS, qui sera dit de classe B dans le cas d'une transmission non obligatoire, alors qu'il est dit de classe A dans le cadre d'une transmission obligatoire.

La transmission de l'AIS s'effectue par messages radio dans la bande des très hautes fréquences (VHF) dédiées aux communications maritimes : deux fréquences sont mondialement dédiées à la transmission des messages du système, il s'agit de 161,975MHz et 162,025MHz. L'émission des messages est effectuée au sein de créneaux temporels définis de 26,67ms, chaque message occupant entre un et cinq de ces créneaux. Pour chacune des fréquences, il y a 2250 créneaux par minute, et afin d'avoir un agencement ordonné des messages, des protocoles ont été mis en place. Le plus utilisé de ces protocoles est l'accès multiple par répartition dans le temps auto-géré (SOTDMA), fonctionnant sur le principe de la réservation du prochain créneau de transmission dans le message précédent, permettant un arrangement local des transmissions, le même créneau ne pouvant alors pas être réservé par une autre station ayant été mise au courant de cette réservation. Ce système permet ainsi la limitation des conflits d'émission.

Les messages AIS ont une fréquence de transmission qui leur est propre, et qui varie en fonction du type de communication et de la vitesse du navire, les messages de report de position étant envoyés avec un intervalle allant de 2s à 3min. Cette fréquence de transmission élevée implique un fort volume de données qui est estimé à 5 millions de messages par jour, envoyés par 200 000 navires. Le trafic peut être observé en ligne sur des sites spécialisés, permettant d'avoir à tout moment une image du trafic maritime mondial.

L'AIS a été conçu pour transmettre des messages de divers types, chacun portant une

information qui lui est propre. A cet égard, 27 types de messages différents ont été définis, chacun ayant sa disposition de champs de donnée, et ses propres champs de donnée variant en fonction du type d'information transmise. Le message numéro 1, qui est le message de report de position à créneau réservé, représente à lui seul plus de la moitié de tous les messages AIS envoyés. Les grandes familles de messages sont les messages standard de positionnement ou d'informations statiques sur les navires, les messages d'aide à la navigation, les messages temporels, les messages de sécurité, les messages d'informations binaires, entre autres.

Cependant le système souffre de faiblesses, soit internes dues au système lui-même, soit externes dues au détournement ou à la mauvaise utilisation du système. Les faiblesses intrinsèques regroupent les données manquantes (les navires disparaissent parfois des cartes du fait de la couverture côtière limitée) et la collision de messages, ces collisions étant dues aux problématiques liées au protocole lui-même, au chevauchement des messages, aux collisions de messages (notamment quand des envois simultanés ont lieu) et aux problématiques de réception aérienne, où les récepteurs peuvent couvrir plusieurs zones auto-gérées et donc s'exposer à de multiples collisions.

Les vulnérabilités externes concernent les erreurs constatées au sein des messages (champs mal renseignés, par exemple le champ destination), les falsifications du système (comprenant l'usurpation d'identité, le masquage de destination, les disparitions volontaires) ou les piratages du système (couvrant plusieurs activités telles que la création de navire fantôme, le forçage de fréquence, saturation du canal de transmission l'émission d'une fausse aide à la navigation ou d'un faux bulletin météorologique).

Malgré ces faiblesses, l'AIS est largement utilisé car il permet d'accéder à une quantité massive de données de navigation maritime, et les applications couvrent la connaissance de la situation maritime, la détection d'anomalies, l'analyse de trajectoires, la découverte de connaissances, la prédiction de comportement de navire ou encore la fusion de données maritimes.

Introduction

This chapter presents the Automatic Identification System in all its aspects that are interesting for our study. In a nutshell, it is an information system for vessels transmitting information about the position, the kinematics, the physical characteristics of the vessel, but also identity information and information related to the safety of navigation. Originally dedicated to maritime collision avoidance, it later began to be used for monitoring and surveillance purposes. Today, besides its initial use of collision avoidance, it is used by the mariners to be aware of their environment, by coastal authorities to know the traffic off their coast, by countries to be aware of the location of their pavilion vessels, by companies to monitor their fleet and by researchers as a useful tool for the comprehension of maritime traffic and its various consequences. However, this system is weekly secured is not perfect as falsifications have been demonstrated.

First, the genesis of the system is presented, then its physical and technical main characteristics are shown. As a message-based system, the messages themselves, numerous

(27 different messages have been designed), take an important role and they are presented in the third section. The issues about the vulnerability of the system such as errors, falsification and spoofing cases are presented in the fourth section of the chapter, before the last fifth section which is a state-of-the-art in the various uses of AIS on maritime situational awareness (in such domains as anomaly detection or trajectory analysis) as well as the uses of AIS by researchers in a handful of applicative areas.

3.1 Genesis

The Automatic Identification System (AIS) was put in place by the Safety Of Life At Sea (SOLAS) convention, in its 2002 version (IMO, 2004). This convention, initiated in 1914 by the sinking of the *RMS Titanic* two years beforehand, has the purpose of defining the minimal requirements to which every vessel from signatory countries should comply with. The SOLAS convention deals with a lot of subjects, ranging from the construction of vessels to the way radio-communications shall be done.

More precisely, the SOLAS convention is widely considered as the mother of all international instruments for the security of vessels. After the first version of 1914, other versions were issued in 1929 (second version), 1948 (third version), 1960 (fourth version). The last version, in force as of 2017, is the fifth one, and was adopted on the 1^{st} of November 1974, coming into effect as of the 25^{th} of May 1980. It includes the tacit acceptance procedure, which provides the fact that any amendment enters into force at a given date provided that before this date no objections to the amendment are received from a specified number of countries.

The main purpose of the SOLAS convention is to specify the minimal requirements for ship building, ship equipment and ship exploitation, in respect with their security. It is incumbent upon the signatory states to look after the respect of the prescriptions of the convention by the vessels under its flag. In addition, if a foreign vessel raises significantly enough suspicion about the compliance with the convention, a state can examine a vessel in one of its harbours.

The main topic of the SOLAS convention are about the construction, the structure, the compartmentalisation, the stability, the machinery, the prevention, detection and extinguishment of fires, the rescue plan, the radio communications, the security and safety of navigation, the cargo transportation, the transportation of hazardous merchandise and special provisions for nuclear vessels and high speed crafts.

As seen in the previous paragraph, one of those subjects is the security and safety of maritime navigation, and the AIS system was created in this scope, in order to provide real-time spatiotemporal positioning of a vessel to the other vessels and to shore stations located in its radio range of action (so no further the radio horizon).

Some ships from the signatory countries are concerned by this regulation. Indeed, the SOLAS convention, in its fifth chapter, nineteenth rule, paragraph 2.4, states the use of the Automatic Identification System (IMO, 2004)

2.4 *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 (AIS) as follow*

2.4.1 *ships constructed on or after 1 July 2002*

2.4.2 *ships engaged on international voyages constructed before 1 July 2002*

2.4.2.1 *in the case of passenger ships, not later than 1 July 2003*

2.4.2.2 *in the case of tankers, not later than the first survey for safety equipment on or after 1 July 2003*

2.4.2.3 *in the case of ships, other than passenger ships and tankers, of 50.000 gross tonnage and upwards, not later than 1 July 2004*

2.4.2.4 *in the case of ships, other than passenger ships and tankers, of 300 gross tonnage and upwards but less than 50,000 gross tonnage, not later than the first safety equipment survey after 1 July 2004 or by 31 December 2004, whichever occurs earlier*

2.4.3 *ships not engaged on international voyages constructed before 1 July 2002, not later than 1 July 2008*

2.4.4 *the Administration may exempt ships from the application of the requirements of this paragraph when such ships will be taken permanently out of service within two years after the implementation data specified in subparagraphs 2.4.2 and 2.4.3*

2.4.5 *AIS shall*

2.4.5.1 *provide automatically to appropriately equipped shore stations, other ships and aircraft information, including the ship's identity, type, position, course, speed, navigational status and other safety-related information*

2.4.5.2 *receive automatically such information from similarly fitted ships*

2.4.5.3 *monitor and track ships*

2.4.5.4 *exchange data with shore-based facilities*

2.4.6 *the requirements of paragraph 2.4.5 shall not be applied to cases where international agreements, rules or standards provide for the protection of navigational information*

2.4.7 *AIS shall be operated taking into account the guidelines adopted by the Organization. Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information.*

3.2 The characteristics of the system

The characteristics of AIS system covers various domains, as the system has intrinsic physical characteristics with respect to transmission, protocol use or the range of transmission but also global characteristics such as data volume, stations location or means to display

information. In this section, the transmission mode of the system is first presented, then the broadcasting characteristics are displayed with a focus on protocols, local policies and range of transmission. Another subsection deals with data collection in the vessels, in coastal stations and via dedicated satellites, before display in local ECDIS on-board ships or on dedicated Internet websites. The last part presents the message-based systems that are somewhat similar to the AIS which are the LRIT and the ADS-B.

3.2.1 Transmission mode

The transmission of AIS is done in the Very High Frequency (VHF) bandwidth (which ranges from 30 to 400 MHz), and more precisely in the dedicated Marine VHF bandwidth (consisting in four distinct bandwidth which have a total range of 2.225 MHz), as VHF band is split in sub-bands which are used for specific and various applications, such as search and rescue, private or military applications, radio-astronomy, amongst others. Two worldwide dedicated wavelengths are used to transmit AIS data: 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 can be distinguished: class A transponders, class B transponders, multi-channel receivers and radio scanner receivers. The devices are technically not transponders, but transceivers, as a transponder is a radio or radar transceiver that transmits some signal in response to receiving a predetermined signal while transceiver is a combined radio transmitter and receiver. Class A transceivers transmit with 12.5 W power and have priority over class B, which are limited to 2 W (K. Schwehr, 2011).

One of those subjects is the security and safety of maritime navigation, and the AIS system was created in this scope, in order to provide real-time spatiotemporal positioning of a vessel to the other vessels and to shore stations located in its radio range of action (so no further the radio horizon).

Class A transponders equip all the ships that are legally required to use the system by the SOLAS convention. They can receive and transmit simultaneously on both channels, and have full capability and options for the users. Class B transponders equip some of the ships that are not legally required to use the system but which owners wish to transmit their information and receive information from the others. As their capabilities and options are reduced, their price is lower. Those transponders can receive and transmit on both channels simultaneously. Multi-channel receivers and radio scanner receivers cannot transmit information but they can receive, simultaneously on both channels or only on one channel at a time respectively. Those receivers are used by ships wishing to improve their situational awareness at sea.

The AIS transponders must be linked to a GNSS antenna for positioning reports, and can be linked to an ECDIS for the visualisation of surrounding traffic and improvement of maritime situation awareness.

Today, two types of transmission are available: terrestrial (*i.e.* direct reception from emitting device) and by satellite (*i.e.* the broadcast signal is received by a dedicated spacecraft). However, at first, the system was only terrestrial, with transmission occurring from one vessel to another, or between a shore station and a vessel, in a range of distance

which is limited by the curvature of the Earth (circa 40 nautical miles in optimal conditions (ESA, 2012)). The development of satellites enabled to receive messages even far from the coast line, as it uploads and stores the received messages then download information as soon a coast line and a shore station is reached. There are specially designed high end receive only units, in towers, aircraft, unmanned aerial vehicles, autonomous surface vehicles, satellites (K. Schwehr, 2011). Transmissions between the stations are shown in Figure 3.1[1].

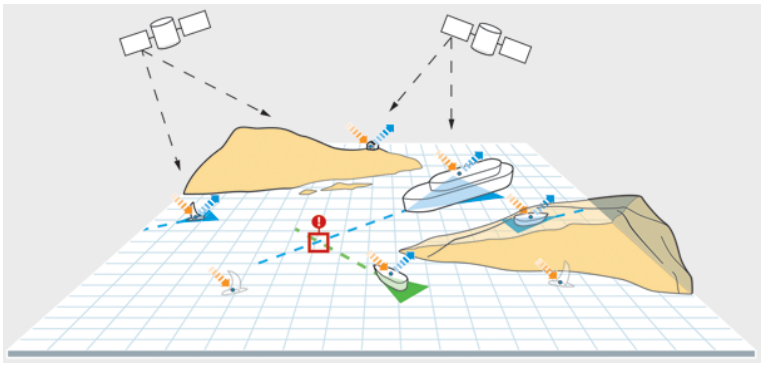

Figure 3.1: Transmissions between AIS stations

The development of Internet gave an even more important step forward in the knowledge of maritime situation as websites display AIS information from all over the world. So 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.

3.2.2 Broadcasting characteristics

3.2.2.1 Protocols

The emission is made during time slots, with a length of 26.67 ms, each message being sent uses between one and five of those time slots of 256 bits each, but messages of 4 and 5 slots are discouraged due to VHF noise that reduces the probability of correctly receive long messages (K. Schwehr, 2011). Amongst the 256 bits of the first slot, the first 88 are reserved for header, remaining 168 usable bits. Space for actual information transmission is small, as for a 3-slot message, it remains 21 to 83 bytes of actual information, which is smaller than the space available for a SMS or a 140-characters Twitter message (K. Schwehr, 2011).

For one frequency, there are 2250 of those slots in a minute of time. In order to have a scheduled, organised and ordered sending of the messages, several protocols were put in place. The frame starts or ends coinciding with the UTC time provided by the GNSS, and exact slot time synchronisation is secured using PPS (Pulse Per Second) signal and UTC generated in the internal GPS receiver (H. Lee et al., 2007). According to (Chang, 2010), reported slots and free slots obey the Poisson theory.

[1] from www.allaboutais.com

The most used of those protocols is the SOTDMA, which stands for Self Organised Time Division Multiple Access. This protocol enables to manage operations in an automatic way, and conceived for sea communication networks. The stations (vessels or shore stations) manage their own time slots reservations for the subsequent messages, and they can modify their own reservations in case of conflict (for instance a meeting with a new station). The principles of the protocol is presented in Figure 3.2[2]. This protocol is used by class A transponders. This protocol leads to the creation of self-organised areas, with the purpose of avoiding message collision, as presented in Figure 3.3.

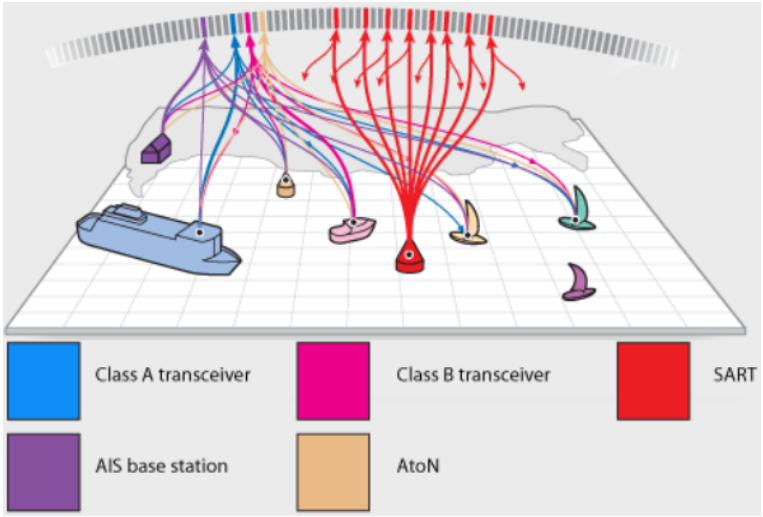

Figure 3.2: Slot Reservation Sketch

Two frequencies are dedicated to AIS at the global level: 161.975 MHz and 162.025 MHz. In the VHF Marine band, the channel number assignments are 87 and 88 (ITU, 2012), the two frequencies (2087, 87B) and (2088, 88B) (K. Schwehr, 2011), of which the bandwidth are 25 kHz each. Hence, in total, 4500 slots are available per minute. The transmission bit rate is about 9.6 kbit per second (Chang, 2010). As for the modulation, a Gaussian Minimum Shift Keying (GMSK) modulation is used, with a modulation index $h = \frac{1}{2}$ and a product $B \times T = 0.3$ or 0.5, where B is the -3 dB cut-off frequency of the Gaussian filter and T the bit duration (Berder et al., 2005). No interleaving nor Forward Error Correction (FEC) is used (Clazzer, Munari, et al., 2014). In addition, the brevity of ship transmissions cause inter channel interference (ICI) and decrease the rate of successful transmission. This issue will be developed in section 3.4.1.2.

As stated before, the slot use obeys to Poisson distribution, and (Chang, 2010) proposes the formulas for computation of the number of reports (time of study divided by the report interval of the user), the total number of reports, the number of slots for success report, the number of release slots (with the given release probability of slots in SOTDMA), the number of free slots, the number of collision, which leads to the computation of the constant λ of Poisson distribution, itself useful for the computation of collision ratio, successful transmission ratio and utilisation ratio of a channel.

Other protocols are also used for specific uses, for instance RATDMA (Random Access Time Division Multiple Access), FATDMA (Fixed Access Time Division Multiple Access), PATDMA (Pre Announced Time Division Multiple Access), ITDMA (Incremental Time

[2]from www.allaboutais.com

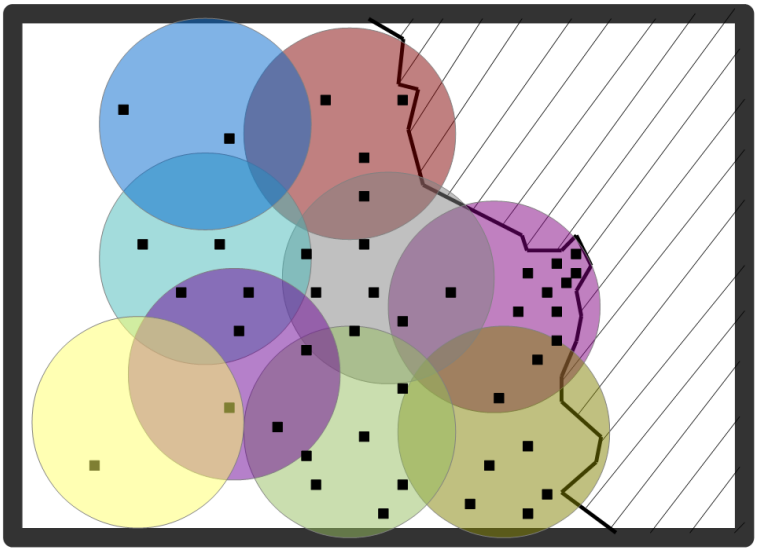

Figure 3.3: Self Organised Areas

Division Multiple Access) and CSTDMA (Carrier Sense Time Division Multiple Access), but there are far less numerous than SOTDMA messages. There are two types of class B transceivers, the "SO" transceivers (standing for Self-Organised) using the SOTDMA standard and the "CS" transceivers (standing for Carrier Sense) using the CSTDMA, designed for the class B transceivers that does not make time slots reservation but which finds free time slots and broadcast its message in them. The table 3.1 presents all protocols in force and their use.

Protocol	Use
SOTDMA	All class A and some class B, with reservations in the slot map
CSTDMA	Some class B, scanning for available space in the slot map
FATDMA	AIS Base stations and AIS AtoN
RATDMA	AtoN for which slot reservation is not done by Base station
PATDMA	SARTs
ITDMA	All AIS devices, to pre announce their AIS data

Table 3.1: Protocols in AIS

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. For class A transceivers, the reporting rates are given in the table 3.2.

Static or Voyage related	6 min, amended data, on request	
Safety	as required	
Long Range	30 min	
↓ Dynamic ↓	not changing course	changing course
At anchor or moored, < 3 kn	3 min	3 min
At anchor or moored, > 3 kn	10 s	10 s
0 to 14 kn	10 s	$3\frac{1}{3}$ s
14 to 23 kn	6 s	2 s
Over 23 kn	2 s	2 s

Table 3.2: Reporting frequencies for class A transceivers

Equipments other than class A transceivers also have reporting rates, which are given in table 3.3.

Class B "SO" shipborne mobile equipment < 2 kn	3 min
Class B "SO" shipborne mobile equipment in 2-14 kn	30 s
Class B "SO" shipborne mobile equipment in 14-23 kn	15 s
Class B "SO" shipborne mobile equipment > 23 kn	5 s
Class B "CS" shipborne mobile equipment < 2 kn	3 min
Class B "CS" shipborne mobile equipment > 2 kn	30 s
Search and rescue aircraft (airborne mobile equipment)	10 s
Aids to navigation	3 min
AIS base station	10 s

Table 3.3: Reporting frequencies for equipments other than class A transceivers

In addition, some particular cases will imply other intervals, for instance SAR reporting interval can be reduced to 2 seconds in the SAR operation area, the messages 24A and 24B have to be transmitted every 6 minutes, in addition to position report messages, and the transmission of the message 24B must follow the transmission of a 24A message within 1 minute.

However, all information above is in force when the AIS is using the autonomous mode. When the assign mode is used, the reporting interval set by the message number 23 must be used, which can range from 2 seconds to 10 minutes. In addition, the same message number 23 can command a transceiver to stop transmitting information for a given time, which can range from 1 to 15 minutes.

3.2.2.2 Range of transmission

The typical range of a class A AIS transceiver can be calculated in km with the formula $R = 4.131 \cdot (\sqrt{h_t} + \sqrt{h_r})$, h_t and h_r being the heights of the transmitter and receiver antenna respectively, expressed in meters above the sea level.

Three main phenomena affect tangibly AIS transmission: diffraction over the sea around the curvature of the earth (extend the range of transmission), multipath effects due to the mounting of the emitter antenna, the structure of the ship, the wind conditions, the mounting of the receiving antenna and configuration, and ducting due to the varying refractivity of the air (extend the range of transmission) (Mazzarella, Vespe, Tarchi, et al., 2016).

Other phenomena such as tropospheric scatter and ionospheric layers scattering have not a considerable effect on the transmission range. Usually, in normal conditions, the transmission range is about 40 NM (ESA, 2012) but the effects such as ducting effect presented above can extend this propagation up to 100 NM (Natale et al., 2015).

The relation between the transmitter power and the receiver power is summarised in the following equation: $P_r = \frac{P_t G_t G_r}{L} \cdot (\frac{\lambda}{4\pi d})^2$, with P_r power of the receiver, P_t power of the transmitter, G_t antenna gain in transmission, G_r antenna gain in reception, λ the wavelength, $4\pi d$ the Free Space path Loss and L a term without unit taking into account

receiver losses, transmitter losses and the fading effects due to shadowing, multipath and atmospheric propagation loss (Mazzarella, Vespe, Tarchi, et al., 2016).

Being used with a lesser power, the transmission of AIS Class B transceivers is limited to 5 to 10 nautical miles (Serry and Lévêque, 2015).

3.2.2.3 Local policies

Some local policies can apply for the use of AIS, as several states take internal measures for law enforcement. For instance, in the EU it is compulsory to carry a AIS device for all vessels of length above 15 m since May 2014 (Natale et al., 2015), following the obligation for all fishing vessels of length above 15 m, back in 2009 (Lindstrom, 2014).

Mexico made class B transceiver use mandatory on all vessels of length above 7 m, India made AIS mandatory for all vessels of length above 20 m since 2009. In Singapore, all power-driven vessels must be fitted out with AIS since January 2012 and in the USA, all commercial self-propelled vessel of length above 65 feet, all towing vessels of length above 26 feet and of power above 600 horsepower, all vessels with a capacity above 50 passengers for hire, all high speed passenger vessels of capacity above 12 passengers for hire, certain dredges and floating plants, as well as vessels carrying certain dangerous cargoes have to be fitted out with AIS (Lindstrom, 2014). Canadian fishing vessels are completely exempted (McCauley et al., 2016) from carrying AIS by their government. In the Bay of Brest, fishing vessels are obliged to carry AIS, regardless of their size (Télégramme, 2011).

3.2.3 Data collection

3.2.3.1 Data volume

As there is no official bureau for AIS-fitted vessel, it is not possible to know how many vessels are fitted out with the system, and how many messages are transmitted, however some estimates are given in literature, displaying some variations in the figures. (Windward, 2014) estimates the number of AIS-fitted vessels at 200,000 as of 2014, and in the European Union waters, 5 million messages are sent every day, by circa 17,000 unique vessels (EMSA, 2015). At any time, the website *marinetraffic.com* tracks more than 80,000 vessels, the data being collected by a network of over 1,800 coastal stations, in 140 countries (Zissis, 2016). (Natale et al., 2015) estimates that in a month, at a global scale, 200,000 unique messages are received, and 130,000 vessels of all categories are sending those messages. (Jukka-Pekka Jalkanen et al., 2014) notices an increase in the number of messages, from 172 million in 2006 to 261 million in 2009. In the European Union waters, there are circa 10,000 unique vessels per day and about 100,000,000 messages per year (Iphar, Aldo Napoli, and Ray, 2016) and at the global level, as stated by (ESA, 2012), "*on a good day, approximately 400,000 ship position reports are received from more than 22,000 different ship identification numbers (Maritime Mobile Service Identity, or MMSI). In a summary made in Oct. 2011, the total number of position reports received exceeded 110 million messages from more than 82,000 different MMSI numbers*".

3.2.3.2 Coastal stations

AIS transceivers are located both on vessels and on coastal stations, and all transceivers are sending a message that all transceivers within the line of sight can receive, provided that there is no slot collision. Mobile stations and shore-based stations send different kind of messages, but receive all messages sent by all transceivers, independently from their origin.

Local data collection in vessels enables the information display system to give a reliable image of the traffic in the surroundings of the vessel, improving the maritime domain awareness. Some additional pieces of information about dangers at sea are also provided in order to enhance the security of navigation. However, the amount of data which is storable in the buffer is limited and data is erased so new data can be stored and displayed.

Local data collection in coastal stations enables the coastal country to have a clear view of the traffic off its coasts, to know vessels that have a destination in one of its ports or if the vessel just passes by. This information can be useful to many people, such as MRCCs, coastal police or ship owners. On-shore stations also have the possibility to store an important amount of messages, so that the history of one vessel can be tracked, and it is possible to know if the vessel is a new one in the area or if it is a current vessel in the neighbourhood.

The communications between the coastal stations, in convergence with the rise of the Internet and the development of Satellite AIS technology, led to the creation of data repository, to which coastal stations can send their messages in order to give a global overview of the marine traffic, as faithful as possible. The satellite AIS technology will be further described in section 3.2.3.3.

3.2.3.3 Satellite AIS

Satellite AIS (S-AIS) is a satellite-based system in which *ad hoc* satellites receive messages sent by vessels. The message number 27 was designed for this particular purpose of ship to satellite communication. The AIS was not designed for the reception of messages for space, and interference problems could arise if vessels are near-by (Faber et al., 2012). In addition, protocols like SOTDMA will tend to avoid message collision within an organised area in the neighbourhood of the vessel, and as the field of view of a satellite is important, multiple organised areas will enter its scope, which is likely to increase message collision cases. At 650 km of altitude, the field of view is 5000 km in diameter (Plass, Poehlmann, et al., 2015).

The possibility of reception of AIS messages from space was first presented in 2003, in the 4^{th} IAA Symposium on Small Satellites for Earth Observation, by the Norwegian Defence Research Establishment (FFI). This possibility is due to the miniaturisation of space technology (Wahl et al., 2005). The messages can be received by a standard receiver up to 1000 km in altitude (Høye et al., 2008) applying the Friis transmission equation and a decrease of -1dB / 100 km (Eriksen et al., 2006), where the swath worth 3630 NM (in the European waters it could worth up to 6200 vessels simultaneously). There

is a demand for such global data for several reasons such as surveillance, anti-piracy or environmental protection for instance (Plass, Poehlmann, et al., 2015). It is necessary to have a space segment: the satellite itself, with the antenna and the storage device, a ground segment, which are ground stations for the download of information and the user segment, with online display of data (Vu Trong et al., 2011).

The feasibility of such satellite-based reception of AIS needs to focus on several aspects (Eriksen et al., 2006): the signal power in space, the detection probability in space, the scenarios for coverage in Europe (the busiest location) and the consideration for space-based subjects. For the coverage of Europe, a 1900 NM span would be needed, which is far larger than the 800 NM possible span without excessive loss, as seen in the message collision section (section 3.4.1.2). For information loading of 10,000 vessels, a 2 Mb memory would be needed on-board, and assuming a downlink of 10 minutes to a ground station, the downlink rate must be at least 34 Kbps (Eriksen et al., 2006). A single satellite is not sufficient then, and a constellation must be used.

The AIS satellites are located on the Low Earth Orbit (LEO) (Natale et al., 2015), which are 600-800 km orbits (Vu Trong et al., 2011). The fist AIS satellite was TacSat-2, with a weight of 370kg, done by the US Air Force laboratory. Some followed, such as PathFinder2 of LuxSpace (8 kg) in 2009 and AISSAT-1 of the Norwegian FFI (7 kg) in 2010, amongst others (Vu Trong et al., 2011). In the mission presented in (Vu Trong et al., 2011), the downlink rate if 38.4 Kbps and the revisit time is about 12 hours, but this time can be reduced by the increase of the number of satellites, and can be reduced by the large spatial line of sight of the antenna (as it is omnidirectional). However, in some cases, a directional antenna can be used in order to avoid message collision and increase the message reception rate (Høye et al., 2008).

The study proposed in (Cervera, Ginesi, and Eckstein, 2011) and (Cervera and Ginesi, 2008) shows that the use of a deployable antenna (Helix) with 6 turns improve the chances to decode messages because of the power variation it introduces on the link budget. The target is to have a ship report every 3 hours. This target is reachable using 5-10 LEO (Low Earth Orbiter) satellites, at 600 km of altitude, with carefully chosen orbital constellation, which can lead to a probability of ship detection of 90%. The size of the constellation (5 to 10) will depend on the traffic prediction uncertainties. Satellites are getting ever smaller, with for instance the Norwegian micro-satellite NSAT-1, of dimensions 55x55x70cm, fitted with a X-band radar, or the very small feasible AIS satellite of type CubeSat, which dimensions are 10x10x10cm (Wahl et al., 2005).

The use of satellite AIS is various, but can be particularly useful in come cases such as the estimation of gas emissions in arctic regions (Winther et al., 2014), data fusion with other sources of data (SAR, terrestrial AIS, radar, amongst others) or the detection and classification of fishing patterns, as presented in (Souza et al., 2016).

3.2.3.4 Dedicated websites

AIS data being collected and gathered worldwide, and shared on the Internet it was then possible to display it on dedicated websites. Some of them have a free access for visualisation and some basic features, and a paying access for charged features, other need

registration for data visualisation, and other are fully charged. The purpose of this section is neither to present the characteristics of each website nor to display an exhaustive list of them, but amongst the websites, some of the most widely used are *marinetraffic.com*, *shipfinder.co*, *fleetmon.com*, *vesselfinder.com*, *aishub.net* or *globalfishingwatch.org*.

3.2.4 Similar systems

The AIS is not the only maritime positioning system, albeit being the one sending the greater amount of data due to the high rate of transmission. In this part we introduce the LRIT system, similar to AIS, on board ships and the ADS-B system, based on the same kind of position report messages, but for the airplanes. AIS and ADS-B undergo similar problems, thus the comparison of the system makes sense.

3.2.4.1 The LRIT

The Long-Range Identification and Tracking system is a satellite-based system for position reporting, set up under the auspices of IMO, with purposes in maritime safety, marine environment protection and maritime search and rescue (EMSA, 2013). In force since July 2009, it is a mandatory system for all passenger ships, high speed crafts and cargo vessels which have a gross tonnage above 300, provided that they are engaged in international voyages. Mobile offshore drilling units must also carry LRIT. However, vessels fitted out with AIS which operate exclusively within the Sea Area A1 (of the IMO SOLAS GMDSS Sea Areas) as described in (IMO, 1995) (between 20 and 35NM from the coast) are exempted from using LRIT (Faber et al., 2012).

The information transmitted is the identity of the vessel, its position and the date and time of position. The advantages of LRIT are a global coverage and a large number of concerned vessel as the decision to set up this system was taken at the IMO level. Some drawbacks of the system are the fact that very few information is transmitted: there is no speed for instance, nor heading, and the frequency is low, as the vessels have to transmit at least once every six hours. Moreover, data is not gathered at one central point and data is confidential as only SOLAS contracting governments are allowed to request information on a limited amount of vessels (Faber et al., 2012) (EMSA, 2013), which are:

- The vessels operating under their flag
- The vessels operating within 1,000 NM off their coast
- The vessels that declare their intention to enter a port which is under their jurisdiction

The European Union set up the EU CDC (European Union Cooperative Data Centre), one of the biggest data centres in all LRIT network, with over 8,500 vessels tracked and 200,000 position report per week, for a coverage of approximatively 25% of the world equipped fleet (EMSA, 2013). LRIT system can be used in data fusion with AIS, as shown in section 3.5.1.6, but it can also be the only reliable maritime positioning source,

as the AIS can lawfully be switched off in peculiar hazardous cases. For instance, the study done by (Vespe et al., 2015) presents the decline of the piracy attacks off the Somalian coast, as the LRIT system is not shut down in case of hazardous areas (due to the confidentiality of data).

3.2.4.2 The ADS-B

The ADS-B, which stands for Automatic Dependent Surveillance-Broadcast, is an airplane-based location system. The broadcast is made of a plain text, unencrypted (Finke et al., 2013), with no authentication (Faragher et al., 2014), error-code protected (Costin and Francillon, 2012) and under the form of messages. There is one message sent per second, containing position, velocity, identification, air traffic control information and management information (Costin and Francillon, 2012). The current ADS-B implementation is based on single-hop unidirectional broadcast link, with any kind of energy constraint not taken into consideration. The ADS-B protocol is intended to be widely deployed for air traffic management by 2020 (Costin and Francillon, 2012), and as a positioning device, GPS will be used (so some GPS-related attacks are conceivable), with some requirements such as integrity checks on GPS signals, so most attacks will be withstood, and the fact that aircraft data such as position, identity and velocity is broadcast via unencrypted raises serious security concerns.

ADS-B signals are received by ground stations and website display the world air traffic. If this is at first intended for hobbyists and aviation enthusiasts, such an information display could be used for malicious purposes (Finke et al., 2013). This is due to the lack of authentication (for protection against injections from unauthorised actors), to the lack of message encryption (for protection against eavesdropping), to the lack of challenge-response mechanisms (for protection against replay attacks) and to the lack of ephemeral identifiers (for protection against privacy tracking attacks).

Attacks can come from different sources and take several forms (Costin and Francillon, 2012). The attacker can be external (most probable) or insider, ground-based (probable) or airborne, and the goals can be various : pranksters (least offensive), abusive users (diverse motivations, up to pilots with abusive access use), criminals (for money and/or terror), military/intelligence (state-level motivations: spying, sabotage...). The various threats at stake are the jamming, the denial of service, the eavesdropping, the spoofing, the impersonation, the message injection, the message replay and the message manipulation. The attacks on ADS-B system include: ghost aircraft injection, ghost aircraft flooding, virtual trajectory modification, false alarm, ground station flooding, aircraft disappearance and aircraft spoofing, whose feasibility has been studied by (Schäfer et al., 2013).

Encryption of the signal is proposed as a way to reduce the threats on the system. Three kinds of encryption methods (Finke et al., 2013) are assessed for ADS-B signals: asymmetric encryption, symmetric encryption and format preserving encryption. (S.-H. Lee et al., 2014), (Strohmeier et al., 2015) and (Faragher et al., 2014) propose ADS-B protection measures.

3.3 The messages

AIS messages have been designed to carry messages of various types, each one carrying a given type of information. In this respect, 27 different messages have been designed, each one having its own layout of data fields nature according to the type of information it is supposed to carry. This section presents on the one hand the various types of messages and on the other hand their content, with a focus on the two most important messages and on vessel identifiers.

3.3.1 Messages of various types

There are 27 different kind of messages as of 2017, but this number could evolve in the future and 64 different messages are possible according to the specifications. Out of those messages, some categorisation is possible. The study of (Tunaley, 2013) proposes a separation in six categories of messages, namely standard, aid to navigation, timing, safety, binary and other. A summary of the categories of messages is proposed in Figure 3.4.

Category	Message	Description
Standard	1	Scheduled position report (class A)
	2	Assigned position report (class A)
	3	Special position report (class A)
	5	Static report (class A)
	9	SAR aircraft position report
	18	Position report (class B)
	19	Extended position report (class B)
	24	Static report (classB)
	27	Long range position report
AToN	21	AToN report
Timing	4	Base station report
	10	UTC inquiry
	11	UTC response
Safety	12	Addressed text message
	13	Acknowledgment
	14	Broadcast text message
Binary	6	Addressed binary
	7	Binary acknowledgment
	8	Broadcast binary
	17	GNSS update
	25	Short binary (no acknowledgement)
	26	Binary with communications state
Other	15	Interrogation for specific messages
	16	Assignment mode command
	20	Data link management
	22	Channel management
	23	Group assignment command

Figure 3.4: Summary of all AIS messages by category, from (Tunaley, 2013)

The first category, the most important one, is the Standard category, which gathers the messages that are position reports (or static information reports). The static information reports are the message 5 for class A transceivers and message 24 for class B transceivers, and contain all static and voyage-related information for a vessel. All other messages from this category display the position (latitude and longitude), as well as other dynamic information such as the speed over ground. Position report messages for class A vessels are 1, 2 and 3, for class B transceivers are 18 and 19, the message number 9 is intended for search and rescue operations aircrafts and the message number 27 has been specifically designed for satellite communication. In the case of class A transceivers, the message

number 1 corresponds to the autonomous position report, done at a rate fixed by the intervals defined in section 3.2.2.1, whereas the message number 2 stands for position reports done at intervals which are assigned by a competent authority, this assignment being done via a message 16 or a message 23. Similarly, the message number 3 is a special position report sent as a response to a command done via message 15.

In the second category, aid to navigation, there is only one message, which is the number 21. In this message, the aids to navigation characteristics are displayed, their nature, their unique identifier, their type, their location (latitude and longitude) and their status.

The third category is timing, and gathers all messages in relation with time and timing of the messages. The message 4 is the base station report, sent by every single base station in a periodical way, including the UTC time to the nearest second. In addition, it includes communication status, indicating how the system is synchronised with external stations. The messages 10 and 11 are respectively UTC inquiry and UTC response. Message 11 is similar in shape to message 4, but message 4 is not sent as a response to an inquiry. Those messages can be sent to and from all stations. In addition to those three timing messages, some timing information is included in standard messages such as messages 1, 2, 3, 18 and 19, which is the UTC second. Also, satellite AIS reports include a time stamp for each message, dated with the satellite clock.

The safety related messages form the fourth category, with the messages 12, 13 and 14. The number 12 is an addressed text message in which the main part of the message is dedicated to a safety related text, in addition to the identifiers of the sender and of the addressee. The message number 13 constitutes the acknowledgement of the reception of a message 12, although up to four senders can be acknowledged at once. Message 14 is a safety related message similar to message 12, the difference being that there is neither addressee nor required acknowledgement.

The six types of binary messages form the fifth category. Message 6 is an addressed binary message containing a binary message and the identifiers of the sender and the addressee, in an analogous way to message 12. Acknowledgement message for message 6 is message 7, which in a similar fashion to message 13 can acknowledge up to four senders. Similarly to message 14, a corresponding broadcast message similar to message 6 that does not need neither addressee nor acknowledgement exists: it is message 8. Message 17 contains the GNSS update data, which is transmitted by a base station, in which the position of the DGNSS (Differential GNSS) reference is included. Message 25 is intended for short (one slot) infrequent transmissions, at either the addressed or the broadcast format. Last, message 26 is designed for scheduled binary data transmissions, with structured or unstructured data.

The last category gathers all the remaining messages, which are message 15 (interrogation for specific messages), message 16 (assignment mode command), message 20 (data link management), message 22 (channel management) and message 23 (group assignment command).

Figure 3.5 presents the number of messages (and thus the relative prevalence of messages) from a study conducted by (Tunaley, 2013) with one month of data.

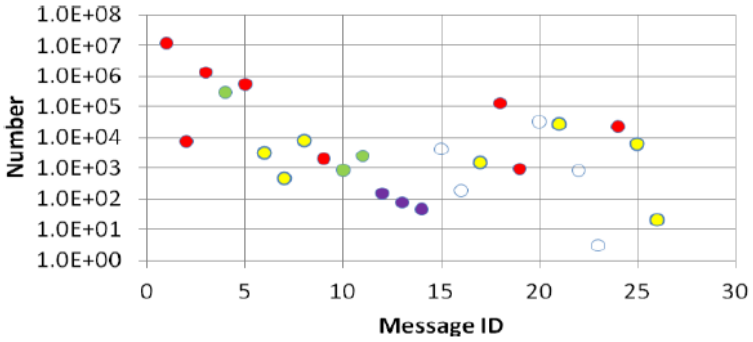

Figure 3.5: Number of messages according to message type, from (Tunaley, 2013) study

3.3.2 The content of the messages

The data inside AIS messages can basically be divided into three main categories: static, dynamic and voyage-related (Lundkvist et al., 2008). Static data are data fields which are not intended to change, or at least to seldom change, such as MMSI number, IMO number, call sign, name of the vessel, length and beam, the type of ship or the position of the position fixing device. Dynamic data are the pieces of information contained in the data fields which are expected to change over time, displaying a physical motion, such as the latitude, longitude, course over ground, speed over ground, rate of turn or true heading. Voyage-related data are pieces of information that are expected to change often, at each new voyage, such as the draught, the number of person on-board, the destination, the estimated time of arrival or the hazardous nature of the cargo.

3.3.2.1 The main messages

In the AIS system, all messages matter, although all are not used at the same rate, and the understanding of the system as a whole needs the knowledge and the understanding of every single message out of the list of messages presented in section 3.3.1. However, due to their prevalence and their particularly important role in AIS display information they provide, the messages 1 and 5 are presented in this part. They are the most used messages for each of their functions, which are dynamic data reporting and static data reporting. Those messages are the main information provider for digital chart displaying on-board vessels and for Internet AIS data hubs presented in section 3.2.3.4.

The Table 3.4 displays the layout of message 1, with the fields, the number of bits allocated to each field and a comment on this field. It must be noticed that the messages 2 and 3 display the exact same layout as message 1, and that the layout of message 18 is very similar to this one. Apart from the identification field, location data is provided by the “longitude” and “latitude” fields, with a precision on localisation provided by the “position accuracy” field. Some dynamic data are provided by the “speed over ground”, “rate of turn”, “course over ground” and “true heading” data fields. Some additional data are also provided such as navigational data in “navigational status” and “special manoeuvre indicator” data fields. There is also a weak time stamp provided by the “time stamp” data field.

Field	Bits	Description
Message ID	6	Message number. Here = 1
Repeat Indicator	2	How many times the message was repeated
User ID	30	MMSI Number
Navigational Status	4	Current status (anchored, fishing, ...)
Rate of Turn	8	Convertible in $deg.min^{-1}$
Speed Over Ground	10	In $\frac{1}{10}$ kn
Position Accuracy	1	Over or Under 10 m
Longitude	28	In $\frac{1}{10000} arcmin$
Latitude	27	In $\frac{1}{10000} arcmin$
Course Over Ground	12	In $\frac{1}{10} deg$
True Heading	9	In degrees
Time Stamp	6	UTC Second
Special Manoeuvre Indicator	2	If engaged in special manoeuvre
Spare	3	Not Used = 0
RAIM-flag	1	Use of Receiver Autonomous Integrity Monitoring
Communication State	19	Planning of next transmission

Table 3.4: Layout of AIS Message number 1

The Table 3.5 displays the layout of message 5 with the fields, the number of bits allocated to each field and a comment on this field. It must be noticed that the message number 19 displays a layout which is quite similar to this one. Apart from the identification field used in every single AIS message, some other identification fields are present in this message, such as "IMO number" and "name". Other fields show information about the physical characteristics of the vessel such as "overall dimensions / reference for position" and "maximum present static draught" data fields, or about the vessel itself such as "type of ship and cargo type" and "type of electronic position fixing device" data fields, or about the current voyage such as "estimated time of arrival" and "destination" data fields.

Field	Bits	Description
Message ID	6	Message number. Here = 5
Repeat Indicator	2	How many times the message was repeated
User ID	30	MMSI Number
AIS version indicator	2	Compliance with ITU recommendations
IMO Number	30	As seen in section 3.3.2.3.2
Call Sign	42	In 7 6-bits ASCII characters
Name	120	In 20 6-bits ASCII characters
Type of ship and cargo type	8	As defined by the specifications
Overall dimension / reference for position	30	Dimension of the ship and position of reference point
Type of electronic position fixing device	4	GPS, GLONASS, Loran-C, ...
ETA	20	Estimated Time of Arrival in next port of call
Maximum Present Static Draught	8	In $\frac{1}{10} m$
Destination	120	In 20 6-bits ASCII characters
DTE	1	Data terminal equipment ready
Spare	1	Not Used = 0

Table 3.5: Layout of AIS Message number 5

3.3.2.2 Theoretical and practical range of values

The theoretical range of values of each field is the total number of possible values for this specific field. As we know the number of bits dedicated to each field, it is easy to compute it: for a field taking n bits, we have 2^n possible value, resulting in a range going from 0 to $2^n - 1$. The empty field can also be taken into account as a possible data (or lack

thereof), adding a 2^nth value.

However, in a certain amount of fields, the definition range of the field does not cover the entire range of the field. For instance the "Type of electronic position fixing device" field has a theoretical range of value of 16, however the values 9 to 14 are not used, so in this case the practical range of values is smaller than the theoretical one, as the practical range of value represents the values allowed by the specifications of the system, including default values.

Let Ω_{x_i} be the theoretical range of value of the i^{th} field of message number x, let R_{x_i} be the practical range of value of the i^{th} field of message number x, then $\forall i, x \in \mathbb{N}^2, R_{x_i} \subseteq \Omega_{x_i}$

3.3.2.3 The vessel identifiers

3.3.2.3.1 The Maritime Mobile Service Identity The MMSI (Maritime Mobile Service Identity) is a number which stands as identifier as it uniquely identifies a ship or a coastal station. It consists in a number of nine digits and is standardised by ITU in (ITU, 2015). Within the MMSI number is the Maritime Identification Digits (MID), which are identifiers of three digits, which denote the country (or administrative region) responsible for the ship station. The assignment of the nine digits number varies according to the type of station.

When the station is a vessel, the MMSI number is under the form "MIDXXXXXX", "MID" are the first three digits which stand for the MID number, and the six remaining "X" are figures from 0 to 9.

When the station is a coastal station, the MMSI number is under the form "00MIDXXXX", where the third, fourth and fifth digits stand for the MID number, and "X" is any figure from 0 to 9. The sixth digit can be optionally used to differentiate between certain specific uses, with "1" used in case of coast radio station, "2" used is case of harbour radio station, "3" used in case of pilot stations and "4" used in case of AIS repeater station.

When the station is an aircraft, the MMSI number is under the form "111MIDXXX" where the fourth, fifth and sixth digits stand for the MID number, and "X" is any figure from 0 to 9. The seventh digit can be optionally used to differentiate certain specific uses, with "1" used in case of fixed-wing aircraft, or "5" used in case of helicopters.

When the station is an AIS aid to navigation, the MMSI number is under the form "99MIDXXXX", where the third, fourth and fifth digits stand for the MID number, and "X" is any figure from 0 to 9. The sixth digit can be optionally used to differentiate between certain specific uses, with "1" used in case of physical AIS aid to navigation or "6" used in case of virtual AIS aid to navigation.

In the special case of crafts associated with parent ships, their MMSI is under the form "98MIDXXXX", where the third, fourth and fifth digits stand for the MID number, and "X" is any figure from 0 to 9.

In addition to those casual cases, special cases are also addressed, with MMSI assignments methods for special purposes. A VHF transceiver with digital selective calling

(DSC) and GNSS, which participates in the marine mobile service, will have a MMSI number under the form "8MIDXXXXX". Other devices use a free-form number identity without reference country, such as AIS-SART (Automatic identification system-search and rescue transmitter), man overboard (MOB) device or EPIRB (Emergency Position Indicator Radio Beacon), which MMSI number are under the forms "970XXYYYY", "972XXYYYY" and "974XXYYYY" respectively, where the fourth and fifth digits ("XX") stands for a manufacturer identifier number from "01" to "99" and the four last digits ("YYYY") is the sequence number from "0000" to "9999". The various cases of MMSI format are presented in figure 3.6.

MMSI Format	Application
MIDXXXXXX	Normal ship MMSI
0MIDXXXXX	Group of ships
00MIDXXXX	Coastal station
00MID1XXX	Coastal radio station
00MID2XXX	Harbour radio station
00MID3XXX	Pilot stations, etc.
00999XXXX	All coastal stations
111MIDXXX	SAR aircraft
111MID000	Entire group of SAR aircraft
99MIDXXXX	AToN
99MID1XXX	Physical AToN
99MID6XXX	Virtual AToN
98MIDXXXX	Craft associated with parent ship
8MIDXXXXX	Handheld VHF tranceiver
970XXXXXX	SAR transponder
972XXXXXX	Man overboard device
974XXYYYY	EPIRB-AIS

Figure 3.6: MMSI formats allowed, from (Tunaley, 2013)

Administrations are in charge of managing their own list of vessels (under its or their MIDs), by implementing effective procedures for registration and identity assignments, by providing regular updates of assigned MMSI numbers to the Radiocommunication Bureau, by ensuring that the moves to and from another administration are made properly, by assigning a non-used number in case of arrival and by reassigning the former number in case of departure. In addition, if 80% of the allocated MID resource is exhausted, it is possible for this administration to request the allocation of an additional MID to the Radiocommunication Bureau.

3.3.2.3.2 The IMO number The IMO number field that is present in the message 5 in an international number put in place in 1987 by the International Maritime Organisation in the resolution A.600(15) (IMO, 1987), the prerogatives of it were enhanced in 2014 by the resolution A.1078(28) (IMO, 2013). Those resolutions put in place a ship identification number scheme, with the purpose of enhancement of maritime safety, pollution prevention and the facilitation of the prevention of maritime fraud. Administrations can apply this system on a voluntary basis for both new and existing ships engaged in international voyages under their flag. It is also possible to give IMO numbers for vessels engaged in domestic voyages only.

According to (IMO, 2013), "*The scheme applies to seagoing ships of 100 gross tonnage and above*", with the exception of some vessels, such as "*ships without mechanical means of propulsion, pleasure yachts, ships engaged on special service*", such as floating

radio stations, search and rescue vessels, lightships, "*hopper barges, hydrofoils, hovercraft, floating docks and structures classified in a similar manner, ships of war and troop ships, and wooden ships in general*".

The IMO number consists of the "IMO" letters followed by 7 digits ranging from 0 to 9. The number is allocated by IHS Maritime, on the behalf of IMO. This number is shown on ship certificates and is never reassigned to another ship.

3.4 The issues of the system vulnerability

As stated before, the system is weakly protected and several falsification cases have been demonstrated. In this section the various issues of the system are presented, in the first place the intrinsic weaknesses of AIS such as the missing data, the message collision (cases of overlapping, particularly in the airborne reception). Then the errors, falsification and spoofing cases of AIS are presented and explained.

3.4.1 The system has intrinsic weaknesses

3.4.1.1 Missing data

The system in itself can fail in transmitting information. Some transponders fail to reach all the requirements set by the International Telecommunications Union, and some ships display large blank areas. This missing data, as shown in (Lecornu et al., 2013), weakens the exploitation of AIS data by decreasing the reliability, but does not prevent it (as a meaningful statistical study is needed in order to judge the quality of data). The AIS has some critical shortfalls in additions to problems such as limited bandwidth and range: limited retransmit capabilities for a few messages and no retransmit capabilities for the majority (McGillivary et al., 2009). There is no way to detect dropped packets (typically observed by embedding sequence number in packets), there is no mechanism to verify the identity of the sender, so a large portion of the message may be problematic. Moreover, the several systems put in place in order to handle the different messages, with priority purposes and management of conflicts. Those systems are not perfect, and when they get overloaded, they cannot handle all the messages and lose some of them. This phenomenon, known as message collision, is presented in the section 3.4.1.2.

3.4.1.2 Message collision

3.4.1.2.1 Collision Cases are due to the Protocol itself All AIS signals are not received by the receivers, as there is a loss percentage. 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 (Last, Hering-Bertram, et al., 2015), even if the traffic is far less important that the one that the SOTDMA protocol could handle, however, this protocol is not perfect and some messages collide and some time slots are lost. But the biggest reason for message loss is the shadowing due to

obstacles (Last, Hering-Bertram, et al., 2015). The obstacles can be on board the vessel (masks, even if the IMO guidelines for installation clearly states the fact that the antenna shall be free of masks), or other vessels hiding more distant ones.

The SOTDMA protocol creates organised areas in which message transmission is optimised, in order to reduce as much as possible the fact that two vessel use the same slot to sent their message. However, this is not always possible as vessels are moving, and a vessel can move from one organised area to another one between two message transmissions, the slot reservation of the former area remaining unused and the slot used in the new area being possibly already reserved by another vessel. In addition, the reception of messages by airplanes and satellites is done with a large spatial span, leading to the reception of messages coming from several organised areas. The cases of slot collision are frequent (H. Lee et al., 2007), as this section displays.

3.4.1.2.2 Message Overlapping When two messages are overlapping, both messages are lost. This can happen when two messages are sent during the same time slot from two organised areas, as explained before, or sent during two adjacent time slots and overlapping due to the path difference of the signals. The AIS has a 12 bits delay (Eriksen et al., 2006), which is 202 NM at the speed of light. From 600 km altitude, 202 NM in difference is worth 394 NM ground range or a swath width of circa 800 NM. In order to respect this 800 NM maximal value, the field of view angle for the satellite must not be over 96° (Eriksen et al., 2006).

3.4.1.2.3 Collision ratio and vessel perspective From the point of view of a vessel, two situations can be distinguished: outside-group slot collision and inside-group slot collision (Liping and Shexiang, 2012). Outside-group slot collision occurs when two vessels afar enough from each other send messages at the same time and one vessel in the middle gets the two messages at the same time and inside-group slot collision occurs in high-density traffic areas, when the system still reserves a spot knowing it has already been reserved.

Several quantities can be computed: the collision ratio of the free slots, the number of collision slots, the system collision ratio, the successfully transmission ratio, the number of successfully transmission slots, the number of successfully transmission in the system and eventually the utilisation ratio of one channel. A simulation of collision ratio and utilisation ratio (also successful transmission ratio) was conducted by (Chang, 2010) with the reports numbers, and up to 2000 messages per minute, collision ratio remain under 1%. Utilisation ratio has a peak around 4000 messages per minute (75%). In addition, In the ocean, far from VTS, the utilisation ratio does not exceed 20% (within 1000 reports), with a successful transmission ratio over 98.5% and a collision ratio under 0.2%.

(Last, Hering-Bertram, et al., 2015) estimated that for a channel load of 20%, 5% of messages were lost, for a channel load of 60%, 15% of the messages were lost and 25% of the messages were lost with a channel load of 90%.

3.4.1.2.4 The case of airliners The possibility to equip airliners that are already in operation with AIS reception system is presented in (Plass, Poehlmann, et al., 2015)

and (Plass and Hermenier, 2014). The equipment of airliners is proposed as satellites are very remote and have high collision rate due to large coverage area, moreover, satellite uplink reception has to handle any influence on the signal done by a Faraday rotation due to the propagation through the ionosphere. In addition, the maritime traffic and the aircraft traffic are stunningly similar worldwide, as the main routes are the same. It is evaluated by (Plass and Hermenier, 2014) that 62.5% of the worldwide fleet is covered by at least one airliner on the first computation. The authors assume that up to 85.9% of vessels could be covered if current data is taken (as their study is based on 2007 data), elevation angle being taken at 10° (but 5° is also a realistic value). The aircrafts could then become another source of AIS data for the World, as the use of airliners from a big alliance could cover most of the marine traffic and provide several contacts per day for every vessel (Plass, Poehlmann, et al., 2015).

In a study led by (Plass, Poehlmann, et al., 2015), an aircraft measurement campaign took place in 2013, over Germany and a part of the Northern Sea. 46 minutes of data were recorded at an altitude between 8,500 and 10,000 meters (flight levels 280 and 330). At the altitude of 10,000 m (frequent cruise altitude), the radius of coverage of an airliner is 56 km (Plass and Hermenier, 2014). A lot of packets were received, but only 29% were error-free due to multiple collisions. The detection rates were 3823 packets per minute for 1000 valid packets per minute. It was demonstrated that when a packet from nearby collides with a packet from far away (which can be 10-20 dB weaker), the first one survives. In heavy traffic, the use of directional antenna could be useful to limit message collision (Høye et al., 2008).

3.4.1.2.5 The Satellite Reception The impact of capture effect and multi-user detection on the satellite reception of AIS messages is assessed in (Clazzer and Munari, 2015). The purpose is to enhance the "destructive collision channel model" which states that all packets involved in a collision are lost and packets not involved in a collision are received. The enhancement uses physical layers that represent the propagation of the waves. In addition to the basic model, two additional, namely the capture model and the successive interference cancellation model, where vessel-satellite distance and Rayleigh fading (linking the received power and the transmitted power, the received power being in $\frac{1}{R^2}$ (Liping and Shexiang, 2012)) are both taken into consideration.

As some parts of the message are known (some bits never vary), it is possible to know *a priori* parts of messages. A receiver aware of those characteristics of the system can increase, according to (Hassanin et al., 2015), the amount of received messages by 10% with respect to coherent AIS receiver and by 80% with respect to conventional receivers. This could be useful in the case in which heavy collision is observed, such as satellite reception. As for satellite reception, (Clazzer, Munari, et al., 2014) demonstrate that SOTDMA can be seen as a slotted random access protocol at the satellite. This simplifies in a noteworthy way the analysis of the protocol performance, as an optimisation on the rate of transmission of AIS packets generation can be done to have a better success rate and then maximise the vessel tracking frequency.

3.4.2 The system broadcast errors

A part of the information contained in AIS messages are entered manually by the crew, both at the initialisation of the system for permanent data (such as the name of the vessel for instance) and at every new journey for journey-related data (such as the destination for instance), some of the pieces of information can be erroneous. A study of such erroneous data can be found in (Harati-Mokhtari et al., 2007). They can be done by underestimating the importance of a correct fulfilment of the system or by ignorance and, as being errors, are not intentional.

Each human-filled field is subject to errors, as well in static data such as identification number of the ship, type of the vessel, name of the vessel, the physical characteristics (length, beam, draft) that in dynamic data such as the position (latitude, longitude), the navigation status, the estimated time of arrival or the destination. According to the study of (Harati-Mokhtari et al., 2007), both static and dynamic data are subject to errors.

Thus, the MMSI number is false is an estimated 2% of the cases (Harati-Mokhtari et al., 2007). Four numbers appeared in a regular way: "0", "1", "999999999" and "1193046", the latter being guessed as being the initialisation number of some kind of transponder. Also, the type of the vessel is often unclear. As 6% do not define a type at all, 3% define their vessel simply as "vessel". The problem of definition is larger, as it lies on the perception of the person entering information: a case of three ferries, perfectly identical vessels, was shown, were the three given types were "High Speed Craft", "Passenger" and "Cargo" (Harati-Mokhtari et al., 2007). 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.

The position is also subject to problems, as it was noticed that circa 1% of ships had a latitude value (in absolute value) superior to 90° or a longitude value (in absolute value) superior to 180°. Physical characteristics of vessels also suffer from several lacks of consistency (Harati-Mokhtari et al., 2007).

On the website *marinetraffic.com* where a part of the international traffic is displayed, some cases of erroneous destination fields are shown. Six examples of such problematic data are: "ATLANTIC OCEAN", where the destination is too vague, "HOME", where the destination is perhaps true but not precise, "FOS SUR MER", where the vessel clearly seems to come from this French city, and not go to it, "CH 16 FOR DESTINATION", where the pilot asks for a communication in the maritime channel number 16, "TBA", where the destination seems not to be known yet and "ANYWHERE BUT HERE", where the pilot seems to joke without having bad intentions. Globally, only 41% of the ships report their destinations (Hadzagic and Anne-Laure Jousselme, 2016). The most common errors in the next port of call data field are, according to (Bošnjak et al., 2012), a number instead of the port of destination, a name of country and not a name of port, an unknown abbreviation, the word "unavailable", the word "unidentified", a *null* space or a black space.

Moreover, the system in itself can fail in transmitting information. Some transponders fail to reach all the requirements set by the ITU, and some ships display large blank areas. This missing data, as shown in (Lecornu et al., 2013), weaken the exploitation of AIS data

by decreasing the reliability, but do not prevent it (as a meaningful statistical study is needed in order to judge the quality of data).

3.4.3 The system presents data falsification

Intentional falsification of the AIS signal is done by the crews on board the ships 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 (Windward, 2014). It corresponds to the fact to navigate with a MMSI number which is not the real one, allocated and internationally recognised, but with the one of another vessel that actually exists somewhere else. Hundreds of ships are disguised this way. As the MMSI number changes, there is no way to assess a priori whether the vessel one is looking at is the right one. As stated in (gCaptain, 2012) and (The Maritime Executive, 2012b), Iran used to falsify the MMSI number of some ships in order to trade with Syria, then under embargo. The Iranian ship *Millionnaire* took the identity of the Syrian ship *Lady Rasha*. At some time, there were two declared *Lady Rasha*, one in the Mediterranean Sea and one in the Indian Ocean.

Destination masking is also sometimes a falsification (Windward, 2014). 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 are also a kind of falsification, as ships turn off their AIS transceiver in order to hide some of their activities, such as fishing in an unauthorised area, or trade illegal goods (Katsilieris et al., 2013) with other ships or on coasts.

The problems met with AIS are numerous, and most of them are the consequence of the non-secured nature of the transmission. According to (Lloyd's List, 2013), the fixes that would be needed to have a reliable AIS system are at the protocol level. Five main issues are developed by (Windward, 2014): the identity fraud, the concealing of destination, the fact to voluntarily stop the broadcast, the GNSS manipulation and the spoofing of the system.

Identity fraud is the fact to use a false or stolen identifying mark of a vessel. An estimated 1% of the vessels assessed by (Windward, 2014) used a false IMO number. The impact is then that anyone interested in AIS data has no assurance that the name displayed corresponds to the selected vessel of interest. Cases have been demonstrated, such as Iranian vessels trading with Syria under Tanzanian flags (before their deregistration), their previous flag, Tuvalu, having deregistered them beforehand (gCaptain, 2012) (The Maritime Executive, 2012b).

Concealing the destination occurs more than half of the time, when vessels do not report their next port of call (41% rate (Windward, 2014)). The impact is the creation of information gap (as it is not possible to know when the vessel will arrive) and possibly an intentional mislead, a skew of the view of the state of the traffic.

The fact to "go dark" is the fact to turn off the AIS transmission, as over a quarter of the vessel turn off their system at least 10% of the time (once the active shut downs

and lack of satellite coverage taken into consideration). As the large vessels (over 250 m in length) are more likely to turn off their transmission, this is suggesting that they have greater will to conceal some of their activities. The impact is that it undermines the ability to track vessels, and it is challenging for financial and security stakeholders.

As there is no validation of GNSS location, the coordinates can be changed. From mid-2013 to mid-2014, a 59% increase in GPS manipulation has been observed (Windward, 2014). The impact is the difficulty it brings to know the actual location of a vessel.

The spoofing case impacts the maritime situational picture in a harmful way, and more particularly in conflictual areas.

3.4.4 The system undergoes spoofing

The spoofing of messages is done by an external actor by the creation *ex nihilo* of false messages and their broadcast on the AIS frequencies (Balduzzi, Pasta, et al., 2014). Those spoofing activities are done in order to mislead both the outer world and the crews at sea, by the creation of ghost vessels, of false closest point of approach trigger, a false emergency message or even a false cape (in the case of a spoofed vessel).

In the scope of spoofing capabilities, several threats can be taken into consideration: ship spoofing, aid to navigation spoofing, collision spoofing, AIS-SART spoofing, weather forecasting, AIS hijacking and availability disruption threats (Balduzzi, Pasta, et al., 2014). Cases presented in this section have been implemented in a proposed software and self-built transmitter, with built AIS frames (Balduzzi, Pasta, et al., 2014), in an experiment conducted far from any significant body of water (Balduzzi, Wilhoit, et al., 2014).

Ship spoofing consists in the crafting of a valid non-existent ship, with the assignation to the fictions ship of static information. A wide range of malicious scenarios can be imagined, such as spoofing a vessel into the jurisdiction water of an enemy, making a nuclear carrying vessel sailing in the waters of a nuclear-free nation, amongst others. An attacker would also be able to counterfeit information to blame someone else about an event, for instance a voluntary oil spill in the open sea.

Aid to navigation spoofing consists in the crafting of false data to lure a targeted ship into a manoeuvre that could be wrong and possibly hazardous. For instance it would be the fact to place buoys at the entrance of a harbour, or to place buoy to instruct a vessel to navigate in low waters.

Collision spoofing is the fact to create a ghost vessel which would cross the trajectory of the targeted vessel and trigger a CPA (Closest Point of Approach) alert, which could lead the vessel off-course, possibly running aground or into a rock.

AIS-SART spoofing consists in the generation of a false distress beacon for man over-board at given coordinates in order to lure and possibly force the target vessel into an attacker-controlled area, as by law a vessel is required to join an ongoing rescue operation upon the reception of such message.

Weather forecasting can be involved in the case of spoofing of binary messages, which convey messages such as weather and in this threat false weather forecast can be done and sent to the vessels.

AIS hijacking consists in the alteration of information of existing AIS stations, with eavesdropping on the communication and replacement of some AIS data. The recipient receives a message which is not the one sent, as the attacker overrides the original transmission by broadcasting the fake signal with a higher power.

Availability disruption threats are three of a kind: slot starvation, frequency hopping and timing attacks. Slot starvation consists in impersonating the maritime authority to reserve all the spots, thus all stations within coverage have no slot available for reservation and emission. Frequency hopping in the fact to instruct the AIS transceivers to change their transmission frequency, as it is possible by protocol specification for given areas in the World. In timing attacks, the malicious user instruct transceivers to delay their transmission, by doing it repetitively, it prevents the system from functioning normally; and on the contrary, the attacker can command transceivers to send updates at a very high rate, thus overloading the channel.

3.4.4.1 Implications

The implication of a false, falsified or spoofed AIS are, first, on the subject of the safety of maritime navigation, as it weakens the view one can have of the marine traffic, of its surroundings for a vessel, off its coasts for a country or of its fleet for a company. But there is also an implication for finance as it brings a distorted view of the flows of goods, a flawed understanding of supply and demand, and an impact on trading models (Windward, 2014).

For security and law enforcement, the main implications are the fact to trust no one, as AIS data cannot be fully trusted as it is manipulated. The use of AIS for maritime control requires the ability to assess AIS data; the existence of ghost ships, potentially elevating political tensions in case of malicious vessel appearance; the erasing of footprints, by the removal of tracking data of the activities of the vessel; and the fact to undermine watch lists as, by concealing their activities and their identities, vessel avoid the watch lists held by ports and authorities, dramatically decreasing their effectiveness.

3.5 Overview on the uses of AIS data

AIS is widely used for drafting a picture of the maritime situation at a given time. Due to the large number of vessels carrying it, it offers a wide and somewhat truthful view of the state of the marine traffic. Some of the main applicative domains for the use of AIS messages which are maritime domain awareness, anomaly detection, trajectory analysis, knowledge discovery, vessel prediction and data fusion are presented in this section. An overview of all several other minor applicative models is also proposed at the end of this section.

3.5.1 On maritime situational awareness

3.5.1.1 On maritime domain awareness

Maritime Domain Awareness (MDA) is the detection, classification, identification and monitoring of vessel data (Lessing et al., 2006). From an operational point of view, the Commandant of the United States Coast Guard defines it as such: Maritime Domain Awareness, "*in its simplest terms, is to identify and intercept threats well before they reach our shores. Realisation of this goal depends on timely information-sharing, protecting our vital maritime infrastructure, partnering with others at home and abroad, building on current international cooperative security efforts, and preparing to respond quickly to future events. Enhancing our awareness – of our vulnerabilities, threats, and targets-of-interest on the water – is perhaps the most critical element of our Maritime Homeland Security Strategy. We want total transparency of people, cargo, and vessels that use our maritime system... We need to know which vessels are in operation, their history, the names of the crews and the passengers, as well as the nature of the ship's cargo, especially for those vessels that are inbound to U.S. ports. Global MDA is critical to distinguish the law-abiding sailor and ship from the anomalous threat. Achieving MDA allows interventions to prevent a security incident from happening ... allows us to mitigate risk. To gain MDA means having the right sensors and tracking systems, the right intelligence architecture, and the ability to globally fuse and share information in a timely way. We are putting the policy, procedures and systems together that will help us get there.*" (Tetreault, 2005).

The needs are to check that the passage in the territorial waters is harmless, so in order to fulfil those needs control bodies are used, to which analysis tools must be provided for a spatio-temporal monitoring of sea activities. The concerns of the administrations in charge of the maritime domain awareness are numerous (Gaspar et al., 2016): prevention of accidents, particularly on ships which carry hazardous material or pollution cargo ; detection of oil spills and generation of alerts for agencies in charge of oil spill operations ; support anti-piracy operations; monitor the maritime borders ; monitor the fisheries, and detect illegal, unregulated and unreported fishing ; the detection of illegal trafficking and smuggling ; the support of authorities in S&R (Search and Rescue) operations. Thus the stakes are maritime security: port security, container tracking, effective S&R, and maritime safety: struggle against trafficking, piracy, smuggling, illegal immigration, illegal pollution or antiterrorism (Morel et al., 2009) (Maggi et al., 2013).

In order to do so, it is necessary to use heterogeneous sources of information, to permanently discovery new knowledge on maritime routes and vessel behaviours. Systems must enable a permanent watchfulness of the maritime traffic, and adapt to new customs of transgressors (Morel et al., 2009). AIS is part of the usable sources, but other self-reporting systems exists in the maritime domain and outside: VMS, VOS, AMVER, LRIT, ADS-B, EPLRS, VTS, civilian or military such as the VRMTC used by the Portuguese Navy operations centre (Serafim, 2016), coordinated by Italian Navy and NATO military systems. The use of those systems arise the problem of privacy and trust as privacy of people shall be preserved and trust between authorities and self-reporting entities is of paramount importance for information quality and quantity (Hammond et al., 2006). The key characteristics to understand and assess information coming from self-reporting

sources are the entity which has to pay the equipment, the fact that it is voluntary or legal, the fact that self benefits are obvious for the mariners, if they are expectations on privacy, the easiness to intercept the communications and the online availability of information, this is why for a proper use, those self-reporting systems must, as a public policy, be of legitimate purpose, be proportional, be fair, lawful and equal, and be transparent (Hammond et al., 2006).

The Maritime Situational Picture is basically the maps of the locations of the ships in a given area of interest, at a given time. A proper Maritime Situational Awareness requires the ongoing maintenance of the Maritime Situational Picture (Mazzarella, Arguedas, et al., 2015). In this scope, the goals of AIS for Maritime Domain Awareness are the coverage, the network, the interoperability and the data management (Tetreault, 2005). To fulfil those goals, the system must be made usable for Maritime Domain Awareness by the validation of data, correlation, data fusion and the storage of AIS data in an usable way for future analysis. The policy issues around AIS are numerous, for the management of binary information (that must not affect current and future AIS equipment on-board ship by causing mariners to stop their use of the system), the data sharing policies, the use of AIS for other purpose than its original ones (that could cause people to be reluctant in its use), the frequency allocation and the use of other frequencies in some parts of the world (which prevents the satellite system from receiving all data), and the enforcement of carriage (Tetreault, 2005).

3.5.1.2 On anomaly detection

Detecting and classifying abnormal behaviours is a key task of maritime situational awareness, for several reasons such as the extraction of relevant contextual information and the proper monitoring of both self-reporting systems (such as AIS) and non-cooperative systems (such as satellite imagery or coastal radar). The operator must get information with a quality which is good enough to make a decision but also to understand the underlying meaning of the data handled, through evaluation criteria. Those criteria are numerous, but the main ones are uncertainty, imprecision and trueness (Anne-Laure Jousselme and Pallotta, 2015), the uncertainty being the degree of confidence assigned to a specific value (when one is known to be true), and can be caused by lack of knowledge (epistemic uncertainty) or random variability of the process (aleatory uncertainty); imprecision being the inability of the source to provide a single value or to discriminate between several values; and the trueness being the criterion linking a piece of information to the truth (or reference), also referred as the closeness of agreement between the expectation and the measurement.

The size of data matters, as the cost to extract relevant information increases with the data volume. Data acquisition costs also exist, and the right amount of data needed to enable the detection of anomalies within the desired confidence bracket shall be determined. In the maritime environment, data often is surface data, whereas it is not necessarily the case as aircraft, submarines or unmanned underwater vehicles can provide data as well.

The different kind of anomalies that can be met are the kinematic (anomaly shown in the motion of the vessel) and static (anomaly shown in the properties of the vessel) (Horn et al., 2016). They can be further divided in subgroups, such as manoeuvring

issues (involving the velocity vector of a vessel), location issues, interaction issues (illicit or unusual interaction between vessels, or between a vessel and an infrastructure) for kinematic anomalies.

The detection of anomalies can then embrace the cases of vessel stopping, vessel loitering, the entrance in an exclusion zone, the crossing of an exclusion zone, or a rendezvous detection, amongst others.

For outlier detection, several models are possible in the maritime domain: statistical, distance-based, density-based, rules-based or model-based (Koufakou et al., 2011) and the rule-based one is particularly popular in the maritime domain (Holst et al., 2016). But today, one major drawback of anomaly detection is that it is necessary to filter this data prior its entrance into the database, which is not an easy task for a website like *marinetraffic.com*, with approximatively a 5 GB increase rate per day, and over one million events triggered. There is therefore a need for the information system to process itself, so that it can increase its autonomy, and do low-level repetitive tasks. The anticipation, the detection, the identification and the protection of the system are important, and the rise of the Internet of Things and the Big Data techniques will make it possible (Zissis, 2016).

Several methods are used and have been implemented for anomaly detection of maritime traffic using AIS data, such as clustering and classification (Zissis, 2016), Bayesian networks (Hadzagic and Anne-Laure Jousselme, 2016), hidden Markov Models (Zouaoui-Elloumi, 2012) (Yaghoubi Shahir et al., 2014), unsupervised route extraction (Pallotta et al., 2013c), rare events detection (Riveiro, Falkman, et al., 2009), taxonomies (Pinto, 2016), outlier detection based on frequent itemsets (Koufakou et al., 2011), low-likelihood behaviour (A. Alessandrini et al., 2016), route pattern comparison (Liu and X. Chen, 2013). Those methods are implemented for specific cases of anomaly detection, including (Gaspar et al., 2016) entrance in a specific area (in general or by a vessel displaying given characteristics (Serafim, 2016)), exit of a specific area, encounter of two vessels at sea (Holst et al., 2016), huge change in estimated time of arrival, case of off-track location with respect to declared destination, underreporting or overreporting of positions, significant change of speed, significant change of heading (and the movement patterns in general (Holst et al., 2016)), significant change of destination, anchored vessels in harbour, and grounding hazard (Holst et al., 2016). Other cases can include (Pinto, 2016) unusual and unexplained high speed, slow speed and turn, unusual course region, loitering, presence of a vessel outside historical routes or traffic lanes, high-seas or littoral proximity rendezvous and recurrent proximity with other vessels.

Last, some methods are peculiar to use cases, such as the inter-detection time, which follows a log-logistic distribution (Horn et al., 2016), so a measure can be set up to check the reality of this distribution, and the characteristics for instance of migrant vessels (following the major crisis of the rise of illegal immigration in Europe) at sea via correlation methods. In (Langford et al., 2016) this case is studies, and in their dataset, three vessels were known to have smuggled migrants, so their track data is analysed. The correlation, positive or negative, between variables for both migrant vessels and all vessels in the database is performed (5804 unique), the variables are the kurtosis of SOG, the latitude range, the longitude range, the skewness of SOG, the standard deviation of SOG, the mean of SOG and the 0^{th}, 25^{th}, 50^{th}, 75^{th} and 100^{th} centiles of SOG quantile breaks. The

migrant vessel behaviour is then characterised, so it is possible to detect further migrant vessels at sea.

3.5.1.3 On trajectory analysis

The analysis of trajectories are a main feature of AIS data. A trajectory being a spatio-temporal track of a moving object and trajectories a travel from a begin to an end which can be decomposed. (Yan et al., 2008) define a trajectory as "*a record of the evolution of the position (perceived as a point) of an object that is moving in space during a given time interval in order to achieve a given goal*". The AIS, in this scope, provides data at a high reporting rate enabling the analysis of trajectories, provided that a sufficient amount of messages is received by the receivers.

A semantic trajectory can be described in a sequence of stops and moves (Parent et al., 2013), and in this scope significant stops must be separated from non-significant ones. In addition, a geographic component of the trajectory is necessary to understand well the trajectories, that is why (Yan et al., 2008) state that a semantic trajectory modelling requires three modules: geometric features, geographic features and application domain knowledge. Some AIS trajectories are incomplete (Lecornu et al., 2013), and this is a problem for trajectory analysis, which is necessary for understanding of maritime situation. Data can be missing for various reasons: technical problems, navigation in areas of lacking coverage or voluntary interruption of signal transmission. Semantic trajectories have application in many fields (Ilarri et al., 2015) as various as traffic management, ambient assisted living or urban dynamics analysis.

For reliability assessment of data suspected from being incomplete, on the one hand, for each pair of message, the time elapsed between the messages can be compared to the expected time between two messages (which depends on the speed of the vessel). On the other hand, the position of the second point can be calculated with respect to the position, the speed and the heading of the first point in order to assess whether or not the segment is reliable. In order to do so, (Lecornu et al., 2013) proposed a method in which a statistical distribution of positions was put in place and a risk value assigned to the points of the trajectories, leading to the determination of the lack of reliability of such a segment using Shannon's amount of information for the determination of the occurrence of events.

Spatial aggregation of trajectories based on AIS data is discussed in (Andrienko et al., 2016b) and (Andrienko et al., 2016a), as discrete data is not always usable for analysis purposes, as well as incomplete data. Two approaches are then usable when it comes to spatial aggregation of trajectories: discrete and continuous. Continuous approach preserves spatial pattern as they avoid distortion due to discretisation of space, and discrete approach gives accurate numeric measures of movements. A way to summarise the vessels movements is the trajectory box plot, as presented in (Etienne, Devogele, Buckin, et al., 2016).

As for trajectory analysis, the sinuosity of the trajectory *i.e.* the fact not to be straight is computed and high sinuosity tracks are isolated. In (Andrienko et al., 2016b), 326 out of 334 sinuosity detected concern vessel that are also involved in a near-location event. It

is a signature of collision avoidance manoeuvre, and it can avoid a miscategorised data, as some anomalous behaviour can be explained this way. Statistical analysis can be done in the cases where vessels follow the same itinerary (Etienne, Devogele, and Bouju, 2010).

The application of traffic route extraction algorithms is performed in (Pallotta et al., 2013b) in the bay of Brest, France, which can enhance the situational awareness in a given area (of interest) because it can predict future position, probable destination, even with no prior knowledge of situation, or prior knowledge of the area of interest.

One of the descriptive ways of frequent behaviours in terms of space and time (area visited during the movement evolution and the duration of those movements, respectively) is trajectory pattern discovery (Giannotti et al., 2007). Based on the notion of frequent sequential patterns (timestamped set of items) where the elements are ordered by their timestamps, its purpose is the discovery and construction of regions of interest by detection of popular points.

3.5.1.4 On knowledge discovery

Knowledge discovery from AIS messages covers areas such as data mining techniques, mining of association rules, multilevel data generalisation, summarisation and characterisation, data classification, clustering analysis and pattern-based similarity research (M.-S. Chen et al., 1996) with the purpose of finding a new piece of information about maritime traffic.

The analysis of mobility track is an important point of knowledge discovery. Today, those tracks are everywhere in our environment, and this presence is going to increase in the near future. Applications for travel time optimisation, car-sharing or dating websites, or adjustment methods for insurances companies for instance. The first step of the analysis of mobility tracks is to transform the spatio-temporal sequence of events into a sequence of events associated with points of interest (POI) with spatial or temporal descriptors: which POI visited, how much time, at which time (of the day, of the week, of the year, with which weather) and pieces of information on the POI itself. Then the second step is the pattern generation, with the only one of the most relevant ones with respect to a quality measure (Belfodil et al., 2016).

From AIS data, it is possible to extrapolate an automatic production of hierarchical graph-based representation of shipping lanes, by separating the traffic between segments (tracklets) and turning points (breakpoints) (Fernandez Arguedas et al., 2014a). The maritime network is then constructed as follow: from AIS raw data, entry in an area of interest, exit of an area of interest and location near a point of interest (port, off-shore platform) are detected, leading to route extraction, breakpoint detection (based on course over ground data, and more particularly course over ground circular standard deviation, where behavioural changes are shown by peaks (Fernandez Arguedas et al., 2014b)) and maritime lane association for the construction of the geographical maritime network. The parameters for a route are the time, the route ID, the number of vessel associated to that route at that time, the MMSI list of vessel associated with that route, the vessel type, the direction (way in, way out) and the points, defining the spatio-temporal evolution. Detection and discovery of such highlighting of frequent lines and breakpoints have been

performed by (Fernandez Arguedas et al., 2014a) in the Dover Strait and by (Fernandez Arguedas et al., 2014b) during the journey between Dover Strait and Gibraltar Strait.

A method, called Ornstein-Uhlenbeck, based on a stochastic process, is a prediction methods for vessels, the parameters of which being estimated by historical patterns. This method, used in (Pallotta, Horn, et al., 2014) and (Braca and d'Afflisio, 2017), enables the prediction of the trajectory of a vessel that follows a route by several hours and point out vessels of interest that are not following the predicted route. In addition, Shannon entropy can be used to assess route complexity (Pallotta et al., 2013a) after a learning of maritime routes. The patterns extracted from such studies are useful for traffic knowledge of human operators, as they put the bases of anomaly detection, vessel behavioural models, density maps, prediction, and a source of information for data fusion (Pallotta et al., 2013c).

3.5.1.5 On vessel prediction

The best way to track a vessel and predict its future position is to rely on the way it moves. Different methods for vessel prediction can be used, such as point-based, acceleration-based, heading-based, vector-based or cog-based (based on the course over ground). *Ad hoc* systems (Redoutey et al., 2008) compute predicted positions with at least two actual updated positions, and then when a new piece of information is provided, it can be compared to the predicted position. If the difference is larger than a given threshold, new updated positions are used for a new prediction.

The point-based prediction can be used when the ship does not move a lot, *i.e.* when anchored or moored. The vector-based approach can be used when the vessel has a long-time linear and constant speed. At the beginning of such a phase, cog-based should be more efficient, then heading-based before the eventual vector-based. When the vessel accelerates or decelerates, acceleration-based predictions shall be used. A combination of such methods (Redoutey et al., 2008) should decrease the calculation time of tracking algorithms.

Other methods for the prediction of the position of a vessel include genetic algorithms (Vanneschi et al., 2015), track prediction algorithms using Malahanobis distance (Mazzarella, Arguedas, et al., 2015) or probability-based methods (Last, Bahlke, et al., 2014) (L. Millefiori et al., 2016) such as the evaluation of latitude, longitude, course over ground, speed over ground and rate of turn data at a given time t, using the values of those fields previously received.

3.5.1.6 On data fusion

The purposes of data fusion are to ingest data from different sources, to track vessels from certain areas in both real-time and offline cases, to provide a maritime situational picture and to associate cooperative reporting systems with non-cooperatively detected vessel (Mazzarella, Alfredo Alessandrini, et al., 2013). None of the sensors such as AIS or radar can provide sufficient data on a regular basis for the establishment of a accurate and reliable picture of the maritime traffic at each moment. Radar is less accurate than AIS, and is subject to weather conditions, while AIS is fully dependant on its cooperative

nature (Siegert et al., 2016). The fusion of data can improve the quality of information.

Numerous methods to deal with multiple data of the same type exist, however few exist to deal with multiple data of different types. The multi-type multi-source data fusion is complicated and computationally expensive. Single-type multi-source data fusion techniques are Neural Network learning, Bayesian learning, Kalman filtering and Dempster-Shafer evidential reasoning. Only few of those techniques can be applied to multi-type data fusion but some variants can be applied. Neural networks can be extended to neuro-fuzzy and genetic algorithms, and Bayesian learning can be extended for the correlation of heterogeneous data (Corporation, 2015). In their study, (Siegert et al., 2016) designed a interacting multiple model multi-sensor Probabilistic Data Association with unscented Kalman filtering.

Figure 3.7 displays a table of the main observation-based and self-reporting positioning systems available for maritime situational awareness, from which data fusion can be performed (from (Alfredo Alessandrini et al., 2014)).

		Spatial coverage	Vessels coverage	Probability of Detection (P_d) & False Alarm (P_{FA})	Refresh rate / Tracking capabilities	Data latency
Self-reporting systems	Terrestrial-AIS	VHF propagation, nominally line-of-sight	Only SOLAS Regulation V/19-2 vessels	All vessels covered and in range are detected. P_{FA} limited by spoofing	Always adequate by design	Virtually no latency
	Satellite-AIS	Virtually Global	Only SOLAS Regulation V/19-2 vessels	P_d can depend on ship. De-collision algorithms needed in busy areas. P_{FA} limited by spoofing	Depending on # satellites in constellation	Depending on the latitude/visibility of the ground station
	LRIT	Virtually Global	Only SOLAS Regulation V/19-1 vessels	All vessels covered are detected. P_{FA} limited by spoofing	Every 6 hours. Can be polled any time	Network-related (sat communications)
	VMS	Virtually Global	Fishing vessels in excess of 12m (in EU)	All vessels covered are detected. P_{FA} limited by spoofing	Up to hourly rate. Can be polled any time	Network-related (sat communications)
Observation positioning sensors	Coastal/-Mobile radar	Nominally 20NM from the coast	All in range, depends on P_d	Depends on sea state, Radar Cross Section, frequency and polarisation	Continuously scanning radar	Virtually no latency
	EO SAR	Virtually Global	Depends on P_d	Depends on sea state, RCS, frequency and polarisation	Latitude dependent, reduced by sun-synchronous orbits	Depending on the latitude/visibility of the ground station
	EO-Optical	Virtually Global	Depends on P_d	Depends on sea state, target size and cloud cover	Latitude dependent, usually reduced by sun-synchronous orbits	Depending on the latitude/visibility of the ground station
	RPA/Airborne radar systems	Limited by operational costs	All in range, depends on P_d	Depends on sea state, RCS, frequency and polarisation	Continuously scanning radar if aircraft is present	Virtually no latency

Figure 3.7: Main operational observation-based and self-reporting positioning systems for maritime situational awareness, from (Alfredo Alessandrini et al., 2014)

Data fusion enables target identification: in the Halifax harbour, AIS reports are used to direct a camera towards a ship to take a picture of it, via the Automated Ship Image Acquisition (St-Hilaire, 2010). AIS data fusion with terrestrial radar (Katsilieris et al., 2013) (Morel et al., 2009) (Habtemariam et al., 2015) and Synthetic Aperture Radars (Mazzarella, Vespe, and Santamaria, 2015) (Corporation, 2015) (Mazzarella, Alfredo Alessandrini, et al., 2013) (Brusch et al., 2011) (Oo et al., 2010) are the most commonly met.

Data fusion with AIS and SAR data is widely used as it can provide a better picture of maritime traffic and detect vessels which are not reporting their position via AIS. On the other side, it is possible to identify vessels detected via satellite imagery (Mazzarella, Vespe, and Santamaria, 2015). It depends on the resolution of SAR Beacons, but it is often possible not only to detect an object, but also to estimate some parameters such as its length, width or heading (Voinov et al., 2016) (Brusch et al., 2011), with a further

crossing of information with AIS. Specialised satellites such as TerraSAR-X (Brusch et al., 2011) and RADARSAT-2 (Corporation, 2015) by the Canadian Space Agency are used. A track reconstruction can also be performed with both data sources (Voinov et al., 2016), the intermediate points being estimated by the use of the dead reckoning method.

3.5.2 On various applicative models

AIS data is widely used for various applicative models of the maritime network and the maritime navigation. AIS, given its high frequency and carriage obligation for a large number of vessels, provide a reliable picture of the maritime navigation, at least for the vessels obliged to carry the system. In addition, AIS provide a wide range of data, which can be used in a wide range of applications.

In general, it must be noticed that most of the studies take the AIS data "as if" and do not question their genuineness. Some studies, such as (Qu et al., 2011) or (Weng et al., 2012) even create missing data from neighbouring data, in accordance with their need for particular data at a given time.

The **collision risk** is the main application of this section, as some waterways are busy, such as Rotterdam (30,000 sea-going ships and 135,000 inland vessels per year) or Shenzhen, near Hong Kong, with 500,000 ships per year. In the downstream Yangtze, up to 5,000 ships are transiting daily. The collision occurrences would climb proportionally with the number of ships without traffic management and traffic services (Mou et al., 2010). In European waters, some recent disasters such as *Erika* (December 1999), *Ievoli Sun* (October 2000), *Prestige* (November 2002), *Tricolor* (December 2002) occurred, underlining the necessity of collision risk reduction. The traffic lane situation is assessed by (Su et al., 2012), (Qu et al., 2011) and (Fangliang Xiao et al., 2015), as one of the elements of safe navigation is the ship domain, defined in (Qu et al., 2011) as "*the surrounding effective waters which the navigator of a ship want to keep clear of other ships and fixed objects*", from a quotation of Goodwin. Various geometries have been proposed for such domains (Fujii and Goodwin for instance), including binary ship domains (safe/dangerous) or fuzzy ship domains (very safe, safe, less safe, dangerous, very dangerous). Regulations, such as COLREGS, are a major point of collision risk prevention (Stitt, 2004), (Y. Wang et al., 2013). Collision reasons are various and presented in (Montewka et al., 2010), (Tsou and Hsueh, 2010), (Zhang et al., 2015), (Goerlandt and Kujala, 2011), (Montewka et al., 2010) and (Shu et al., 2013). Probability computations on various domains of vessel collision has been studied in (Gilberg et al., 2016), (Silveira et al., 2013), (Montewka et al., 2010), (Perkovic et al., 2012), (Kao et al., 2007), (Qu et al., 2011) and (Weng et al., 2012).

All other listed applicative models include **emergency response**: the way AIS helps us to understand the response to an emergency, spots the issues raised by this response and proposes improvement to emergency response plans (K. D. Schwehr and McGillivary, 2007) (K. Schwehr, 2011), **fisheries**: in order to analyse the pressure on fishing grounds, and the fishing patterns of vessels, in order to understand the fishing habits and the way various kinds of fishing activities are conducted (Hu et al., 2016) (Mazzarella, Vespe, Damalas, et al., 2014) (Natale et al., 2015) (Souza et al., 2016), **planning**: the use of AIS as a monitoring tool (Stoddard et al., 2016) (Vodas et al., 2013) (Huntington et al., 2015) (McCauley et al., 2016) (Serry and Lévêque, 2015) (Shelmerdine, 2015) (Faber et al.,

2012) (Shucksmith et al., 2014), **traffic modelling**: the use of traffic lane, the behaviour of the vessels at the entrance of ports, or in rivers (J. Chen et al., 2015) (Numano et al., 2003) (Zheng et al., 2008) (Oo et al., 2010) (Gucma, 2008) (Naus et al., 2007) (Fanglinag Xiao et al., 2012) (Aarsæther and Moan, 2007) (Aarsæther and Moan, 2010) (Kotovirta et al., 2009) (L. M. Millefiori, Zissis, et al., 2016) (L. M. Millefiori, Cazzanti, et al., 2016), **vessel emissions**: gas released by maritime navigation, including greenhouse gases and pollutants (Miola and Ciuffo, 2011) (Ng et al., 2013) (Yau et al., 2012) (Song, 2014) (J.-P. Jalkanen, Brink, et al., 2009) (Diesch et al., 2013) (L. Goldsworthy and B. Goldsworthy, 2015) (J.-P. Jalkanen, Johansson, et al., 2012) (Jukka-Pekka Jalkanen et al., 2014) (Winther et al., 2014) (Perez et al., 2009), **vessel noise**: noise exposure of human operations at sea on animal life (Hatch et al., 2008) (Erbe, MacGillivray, et al., 2012) (Merchant, Witt, et al., 2012) (Bassett et al., 2012) (Erbe, Duncan, et al., 2012) (Erbe, Williams, et al., 2014) (McKenna et al., 2012) (Merchant, Pirotta, et al., 2014), **animal collision**: collisions between vessels and animals, particularly marine mammals (McGillivary et al., 2009) (Wiley et al., 2011) (Allen, 2014) and **sea surface currents**: study of the near-surface oceanic currents (Guichoux et al., 2016).

Conclusion

This chapter has shown the diversity of AIS messages, their technical characteristics and the way information is carried through them. Messages have to follow very strict layouts, which makes AIS a system of organised data. Such analysis of the system, understanding of its inner mechanisms and applicative domains is necessary for the methodology for AIS messages assessments presented in the next chapter.

Chapter 4

A methodology for AIS messages assessment

Chapitre 4 : Une méthode pour l'évaluation des messages AIS

Du fait des vulnérabilités présentes au sein du système AIS, et du fait que la présence de ces vulnérabilités sont à même d'augmenter les risques de la navigation maritime, ce chapitre propose une méthode pour évaluer ces risques, basée sur la notion d'intégrité des messages AIS. Dans cette méthode, un examen minutieux du système lui-même a permis l'établissement de 935 items uniques d'évaluation de l'intégrité du système, prenant en compte la structure complexe de l'AIS. A cette fin, une nomenclature a été mise en place afin de pouvoir distinguer de façon unique et non ambiguë n'importe quel champ de n'importe quel type de message.

Ces items d'évaluation sont autant de points élémentaires dans lesquels les données AIS pourraient ne pas être en conformité avec ce qui est attendu du point de vue des spécifications techniques ou démontrer une faille d'intégrité du système en présentant un couple ou un ensemble de données incohérent. Quatre ordres d'évaluations ont été établis : un premier ordre où un champ d'un message est pris individuellement et traité au regard des spécifications du système, un second ordre ou différents champs d'un même message sont comparés entre eux, un troisième ordre où un même champ ou différents champs issus de messages différents mais du même type (par exemple une succession de message 1) sont comparés et un quatrième ordre où différents champs de messages de type différents sont comparés. Des grandes familles d'items peuvent être établies, ces familles sont les problématiques de conformité, les données de champs incohérentes, les problématiques d'évolution de valeur d'un champ, d'une trajectoire, les valeurs inhabituelles, une communication trop importante ou trop lointaine, un changement inattendu de valeur d'un champ, les problématiques liées au positionnement ou à la position même du navire, ou encore une réponse incohérente. Pour chaque message, chacun des items est évalué de façon binaire, et une valeur Vrai ou Faux leur est attribuée en suivant la logique des prédicats, permettant une évaluation rigoureuse de chacun des items.

L'utilisation des seules données AIS serait suffisante dans le cadre d'un système isolé. Hors les navires évoluent dans un environnement qui doit être pris en considération dans le cadre d'une étude basée sur l'intégrité du système AIS et devant aboutir à une évaluation des risques associés. Ainsi, toute source de données dans laquelle un élément peut-être comparé à une ou plusieurs données issues de l'AIS peut servir pour cette évaluation complémentaire. Le système AIS couvrant un large panel d'informations, de multiples sources de données peuvent être utilisées, et trois familles principales ont été distinguées : les sources de données environnementales (donnant des informations à propos de l'environnement dans lequel le navire évolue, telles que les données météorologiques), les sources de données orientées navires (avec les registres de pêche par exemple) et les sources de données orientées navigation (avec les géométries des zones d'intérêt par exemple, telles que les zones de mouillage ou les dispositifs de séparation du trafic).

Afin de permettre une compréhension de la situation d'un message par rapport à son analyse d'intégrité, un système de fanions a été mis en place, un fanion étant un élément en langage naturel décrivant une situation donnée liée à l'état du message, conséquence directe des analyses qui ont été effectuées suite à la réception du message. Un fanion est booléen et prend la forme d'une valeur Vrai ou Faux représentant le statut de l'élément de langage correspondant. Quatre types de fanions ont été définis : les fanions liés aux items d'évaluation de l'intégrité et les fanions liés aux données contextuelles, auxquels sont ajoutés des fanions directement liés à la situation et à l'état du navire, fanions issus de l'AIS mais ne constituant pas une problématique d'intégrité qui sont les fanions liés aux indicateurs de situation maritime et les fanions liés au type du navire en question.

Introduction

As AIS messages present vulnerabilities such as falsifications in their structure and data, and that those vulnerabilities can lead to the creation or the increase of maritime risks, the necessity of a treatment of data arises. In this chapter is proposed a method for assessing such risks, based on the notion of integrity of AIS messages. In the proposed method, a thorough examination of AIS messages enables the identification of integrity items (over 900) which are elements in AIS complex structure in which AIS data may disagree, which would be the indicator of an integrity problem. A system of flags, on the one hand based on items and on the other hand based on additional non-AIS data, has been developed, with the purpose of highlighting humanly understandable issues about the system, in the frame of specified scenarios. The flags are raised when a combination of integrity assessment item results are gathered, and the conjunction of some given flags will trigger some scenarios and associated maritime risks, the final purpose being to deliver in near-real-time added-value pieces of information to maritime authorities and rescue centres, based on a risk level assessment.

A raw frame of AIS can be treated by the data side or by the signal side. This section and this study concentrates on the data side, *i.e.* using AIS data once parsed into data fields. The signal side, which consists of the study of the signal characteristics from a physical point of view, has been performed by other actors of the DéAIS project (Alincourt et al., 2016) (Collin et al., 2017).

The method is made of three parts, the first two consisting each of a section of this chapter and the last one being presented in chapter 6, as illustrated in Figure 4.1. The first part is about the integrity assessment of AIS messages, the second one concerns the falsification scenarios and the way situational flags are raised, and the third one is about the way to the risk assessment based on the flags previously computed and the maritime environment.

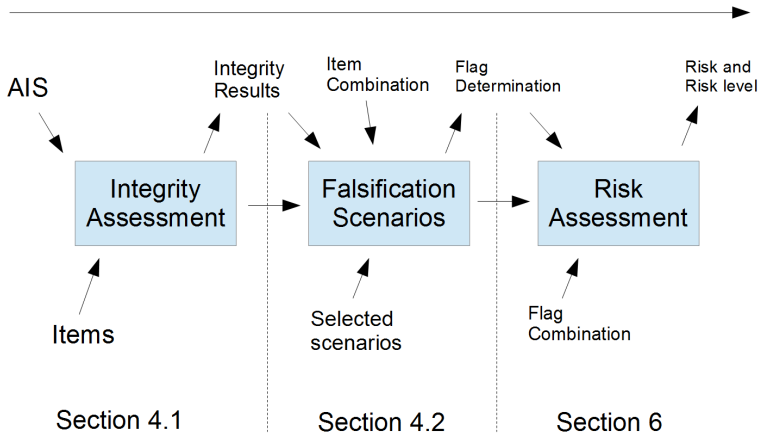

Figure 4.1: Methodology Workflow

The section 4.1 treats how all data fields have been discriminated via a nomenclature, to create over 900 different integrity items (themselves uniquely described by a nomenclature), and how the items work using predicate logic so that it is possible to assign them a value True (if an integrity problem is demonstrated) or False (if no integrity problem is shown).

Then, section 4.2 presents the available data for the scenario assessment, and more particularly the various non-AIS databases which are usable in the process, such as a polygon of the local port, or a fleet register. The various considered scenarios are then described, as well as the various flags which are raised, following the results of the integrity assessment. Those flags are of different nature, either directly coming from integrity item results, or from additional data (as the fleet register database can provide useful pieces of information on the identity of a vessel), for scenario assessment and for vessel neighbourhood assessment (trajectory of the vessel, nature of the environment, the location, the surrounding vessels and their trajectory).

4.1 Integrity assessment of messages

4.1.1 Data structure and fields nomenclature

4.1.1.1 A variety of message types

As displayed in section 3.3.2, the AIS messages are various, therefore they can be discriminated in various families, each families having similar kind of messages, which will

be able to undergo similar integrity assessment. Figure 4.2 presents several kinds of AIS messages classification.

Figure 4.2: Variety of AIS messages

The column on the left-hand side of the Figure 4.2 displays the different kind of senders for the AIS messages. Indeed, some messages are only sent by base stations (shore-based stations or other non-vessel stations), others are only sent by mobile stations, and a large number of messages can be sent by both mobile and base stations. In this scope, it is not expected for vessels having a given MMSI number (discriminating it as a vessel or as a base station, or even at a aid to navigation) to send messages which do not match its category. The same column shows the messages that are sent by class A stations (*i.e.* violet and blue ovals, not circled) and those sent by class B stations (circled ovals). It is not expected that any MMSI can match any pair of (class A, class B) messages.

The column in the centre shows the variety of AIS messages, as it was previously stated in section 3.3.2. There are several kinds of AIS messages, and all messages belonging to the same kind will have the tendency to undergo similar studies. In addition, when it comes to multi-messages assessments, any pair of similar messages will have the tendency to propose similar items, as the data fields involved in the comparison of the messages will tend to be present in both couple of messages.

The column in the right-hand side of the Figure 4.2 displays three of the main messages families: the messages in which positioning is involved, the messages in which static data is provided and the messages in which a communication between two vessels is involved.

The fact, for a message, to have a positioning data (so a latitude field and a longitude field) is that it opens all position-related assessments. Similarly, to have static data open identity-related assessments and to have communication data (so a source MMSI number and a destination MMSI number) opens all kind of analyses on the identities and locations of those vessels. In this figure, the messages in grey do not belong to any of the three kinds of messages families presented.

4.1.1.2 A variety of data types

The AIS messages are various and the data within can take several forms. The diversity of the data fields types can be demonstrated by the study of the message number 5. Table 4.1 displays the fields of the message with the parameter represented and the type of datum.

Field	Data type
Message ID	Numeric representing an identifier
Repeat Indicator	Numeric representing a quantity
User ID	Numeric representing an identifier
AIS version indicator	Numeric representing a choice
IMO Number	Numeric representing an identifier
Call Sign	Textual
Name	Textual
Type of ship and cargo type	Numeric representing a choice
Overall dimension / reference for position	Numeric representing a quantity
Type of electronic position fixing device	Numeric representing a choice
ETA	Date
Maximum Present Static Draught	Numeric representing a quantity
Destination	Textual
DTE	Binary
Spare	Binary

Table 4.1: Different data types in AIS Message 5

Six data types are then discriminated, which are: numeric representing an identifier, numeric representing a quantity, numeric representing a choice, textual, date and binary.

A numeric datum representing an identifier is a piece of information linked to a unique identification number of a kind, e.g. the "User ID" field stands for the MMSI number, a unique identification number for an AIS emitter, or the "IMO number" field stands for a number linked to the vessel given by the IMO as an unique identifier. Such fields can be taken as primary key for further studies.

A numeric datum representing a quantity is a piece of information linked to a physical quantity, in general the given value is not exact but rounded to a given precision for data representation purposes and sensors physical limitations, e.g. in the message 5, the maximum present static draught field is defined over 8 bits, with values ranging from 0 to 255, representing the corresponding physical quantity in $\frac{1}{10}$ of meters, which means the values range from 0 to 25.5 m, with a precision of 0.1 m.

A numeric datum representing a choice is a piece of information linked to the fields that display their range of possibilities over a list of choices, the selected value representing the choice of the corresponding item in the list. For instance the "Type of electronic position fixing device" field ranges from 0 to 15, with some value unused, 10 of them are actual possible choices. The field representing the type of electronic fixing device, according to

the message layout if the value if 1, it means that "GPS" is used, if the value is 2 it means the use of "GLONASS", and so on and so forth until the last possible value.

A textual datum is a textual piece of information, *i.e.* the bits are converted into ASCII characters by groups of six (six-bit character code). Fields such as "Name" or "Destination" require such information, necessary although impractical as the limitation of the number of characters (20 for "Name" and "Destination") can lead to problems in cases where the actual name or destination needs more than 20 characters to be written. In this case, abbreviations can be used but decrease the level of clearness of the field.

A date datum, represented here by the "Estimated Time of Arrival" field is a rare data type for a field in AIS messages, represents a date under a given form, in the "Estimated Time of Arrival" case being MMDDHHMM, *i.e.* the juxtaposition of month, day, hour and minute pieces of information.

A binary datum is a field defined by a single bit, therefore taking only two possible values: 0 and 1. Such a field is in general related to fields where a statement is declared as true or false, a value superior or inferior to a given threshold or a choice in a list of exactly two possible choices.

In addition to those data types that are found in normal use conditions, two additional cases must be taken into consideration: default values and empty fields. Default values exist in AIS messages, as some fields have a value which is designated in case no value is allocated to it. For instance, in the case of message number 1, the longitude value "181" is the default value, or the value "511" for the data field True Heading (Raymond, 2016). Empty fields often occurs in the data when a field has no value allocated to it, and constitute an issue of data completeness.

4.1.1.3 A unique identification number for the data fields

As stated before, each one of those 27 messages have a certain amount of fields, as defined by the International Telecommunication Union in (ITU, 2014), each field providing a value. In our study, we are interested in every single field value of every single received message, as the integrity of information in AIS and thus integrity of the system itself shall be treated from the broadest possible point of view in order to get an all-encompassing assessment. Furthermore, the complexity of the various AIS message types (as seen in section 4.1.1.1) and layout (as seen in section 4.1.1.2) forces a clear identification of each single data field.

The number of fields varies according to the message type, e.g. message 1 has 16 fields whereas message 10 has 6 and message 22 has 19. Moreover, two similar fields can be found in two different messages, and do not occupy necessarily the same position in both messages, e.g. "Course over Ground" field appears in messages number 1, 2, 3, 9, 18, 19 and 27, and is located in those messages as the eighth field for message 18, the ninth field for messages 9 and 19 and the tenth field for messages 1, 2, 3 and 27. In addition, a field in a message can have the same name as another field in another message, represent the same quantity and yet have a different inner definition, e.g. the field "Latitude" which appears in 11 messages has two different layouts: in the first one the field is 17-bit long (2 messages out of 11) and in the second one the field is 27-bit long (9 messages out of

11). Furthermore, the first three fields are common for all messages: the message ID for 6 bits, a repeat indicator for 2 bits and the MMSI number of the source station for 30 bits.

This profusion of identical or barely identical fields in several messages is another step forward for the necessity of a clear nomenclature of the fields, so that one specific field cannot be confused with another one. Therefore, the nomenclature we propose connects each field of each message to a unique three-characters string of type "**XXY**", where **XX** stands for a number between **01** and **27** corresponding to the message number and where **Y** stands for a letter, between **A** and **S** (at most), the position of which in the alphabetical order indicating the position of the field in the given corresponding message, e.g. the field nomenclature "09E" corresponds to the fifth field (as E is the fifth letter in the common English alphabetical order) of the message number 9, *i.e.* the "Speed Over Ground" field. For the application of the nomenclature to AIS messages, three different kinds of messages are exemplified in Table 4.2.

Nom.	Field
01A	Message ID
01B	Repeat Indicator
01C	User ID
01D	Navigational Status
01E	Rate of turn
01F	Speed over ground
01G	Position Accuracy
01H	Longitude
01I	Latitude
01J	Course Over Ground
01K	True Heading
01L	Time Stamp
01M	Spacial manoeuvre indicator
01N	Spare
01O	RAIM-flag
01P	Communication state

Nom.	Field
05A	Message ID
05B	Repeat Indicator
05C	User ID
05D	AIS version indicator
05E	IMO Number
05F	Call Sign
05G	Name
05H	Type of ship and cargo type
05I	Overall dimension / reference for position
05J	Type of electronic position fixing device
05K	ETA
05L	Maximum Present Static Draught
05M	Destination
05N	DTE
05O	Spare

Nom.	Field
12A	Message ID
12B	Repeat Indicator
12C	Source ID
12D	Sequence Number
12E	Destination ID
12F	Retransmit flag
12G	Spare
12H	Safety related text

Table 4.2: Nomenclatures of data fields for messages 1, 5 and 12

4.1.2 Data integrity items

4.1.2.1 A four-order integrity assessment

Considering the data within the fields of the 27 AIS messages, four ways to discriminate the inner integrity of those data can be distinguished, those four ways are displayed in Figure 4.3. The first way consists of the control of the integrity of each field of each message taken individually. The second way is at the scale of one single message, and assesses the integrity, in this very message, of all the fields with respect to one another. As there are 27 types of messages, message of the same type have the same fields and it is thus possible to compare them and assess their integrity, this makes the third way. Eventually, the fourth way is the comparison and integrity assessment of the fields of different messages. Indeed, although pieces of information can come from different messages, it is possible to assess their integrity as some fields are either the same or linked or comparable. Those four ways will then be referred as first-order, second-order, third-order and fourth-order assessments, respectively. The first-order and second-order assessments only rely on one message, and thus are invariant with the environment, whereas the third-order and fourth-order assessments rely on several messages in data history (at least one other, up to an entire time series for one vessel), and the result of those assessments can vary according to the environment (the sample size, the location of the message within the sample).

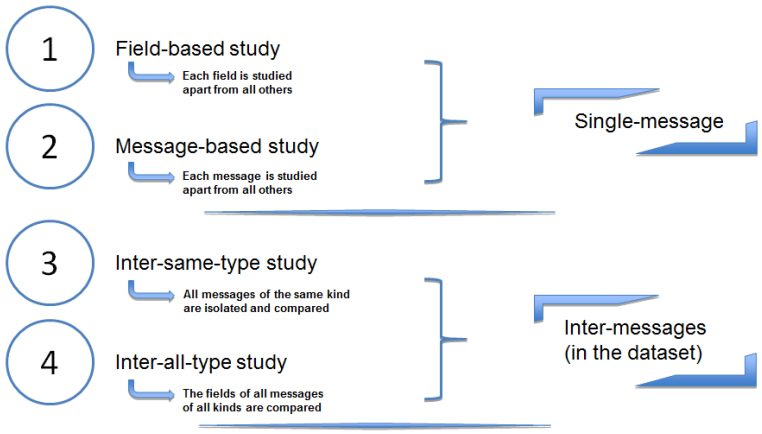

Figure 4.3: The four-order assessment

The assessment of data integrity is done through integrity items, which are simple and unambiguous statements involving one or several data fields, which are designed under their nomenclature presented in section 4.1.1.3. Each statement is about one field, several fields in the same message or several fields in several messages in which data could be in discordance with the expectations of the technical specification or in which data within the data fields could disagree, *i.e.* displaying two or more pieces of information that might not been displayed in a proper or expected functioning of the system.

4.1.2.2 Nomenclature

An *ad hoc* nomenclature has been established so that each assessment can have a clear unique identifier. There is a slight difference in the nomenclature between the first three

orders and the fourth one.

For the first, second and third order items, the unique identifier is a character string of five characters. The first two characters correspond to a number from **01** to **27**, corresponding to the message number, the third character is a letter: S, M or I. The "**S**" letter stands for "Single field" and indicates a first-order assessment, the "**M**" letter stands for "Message" and indicates a second-order assessment and the "**I**" letter stands for "Inter-message" and indicates a third-order assessment. The two last characters correspond to a number from **01** to **12** (actual limit, whereas the theoretical limit is 99), which stands for the number of the item for both its order and the message. For instance "**09M03**" corresponds to the third item of second-order assessment for message 9.

For the fourth order items, the unique identifier is a character string of seven characters. The first two characters correspond to a number from **01** to **27**, corresponding to the first message number, the two following characters correspond to another number from **01** to **27** (which shall be different from the first one) corresponding to the second message number, the fifth character is the letter "**I**", which stands for "Inter-message". The two last characters correspond to a number from **01** to **12** (actual limit, whereas the theoretical limit is 99), which stands for the number of the item for both its order and the two messages. For instance "**0105I02**" corresponds to the second item of fourth-order assessment for the case where we have the message number 1 and 5 to compare, in the case the assessed message is message 1. In the reverse case in which the assessed message is the number 5, and that the assessment is done with respect to the message number 1, the very same item would be called "**0501I02**" . This distinction is due to the fact that the frequencies of the messages are not the same, therefore the relationships between the messages are not bijective. Figure 4.4 sums up all the different kinds of nomenclatures.

Figure 4.4: The four-order nomenclature

4.1.2.3 Order one: Single-message single-field assessment

This section focuses on the cases of assessment of the first order, which are the simplest as the only involve one single data field at a time. The values within the data fields are defined by the International Telecommunications Union and a layout for each field of each message is given, displaying all necessary information to a proper understanding of an AIS message.

As the fields are allocated a given number of bits, the range of values is limited, and

is easy to compute: for a field taking n bits, we have 2^n possible values (plus the empty field), resulting in a range going from 0 to $2^n - 1$.

However, in some fields the possible range for actual data as prescribed by the specifications do not cover the entirety of the possible range. For instance the 05J field (Type of electronic position fixing device) has a theoretical range of value of 16, however the values 9 to 14 are not used, so in this case the practical range of values is smaller than the theoretical one, as the practical range of value represents the values allowed by the specifications of the system, including default values. Another example is in message 1, where field 01H (longitude) extends between hexadecimal values of 0 and 66FF300 for positive longitudes, between hexadecimal values of 9900D00 and 7FFFFFF for negative longitudes (following the rules of the two's complement for binary values), as well as the hexadecimal value of 6791AC0, standing as a default value. As seen in Section 3.3.2.2:

Let Ω_{x_i} be the theoretical range of value of the i^{th} field of message number x, let R_{x_i} be the practical range of value of the i^{th} field of message number x, then $\forall i, x \in \mathbb{N}^2, R_{x_i} \subseteq \Omega_{x_i}$

Figure 4.5 displays a list of assessment items of first-order assessments, with the nomenclature, in two kinds of messages: sent by a mobile station and sent by a fixed station.

(18S01) 18A: field value is not 18
(18S02) 18C: field value is not a number consistent with a MMSI number of a mobile station
(18S03) 18D: field value is not 0
(18S04) 18G: field value is superior to 66FF300h, inferior to 9900D00h and is not 6791AC0h
(18S05) 18H: field value is superior to 337F980h, inferior to 4C80680h and is not 3412140h
(18S06) 18I: field value is superior to E10h
(18S07) 18J: field value is superior to 359 and is not 511
(18S08) 18L: field value is not 0
(18S09) 18E: field value is 1023

Figure 4.5: Some order 1 item, from message 18

4.1.2.4 Order two: Single-message multi-field assessment

The assessments of second order are involving several data fields of the same message. Remaining at the level of one single message, all possible disagreements between data are listed. For example, in a position report message such as message number 1, 2 or 3, we expect data in fields 01D (Navigational Status) and 01F (Speed Over Ground) to be in accordance: if the 01D gives "moored" or "anchored", a 01F value equal or very close to 0 is expected. A list of second-order assessment is proposed in Figure 4.6.

(19M03) 19E field value is not consistent with 19N field value
(19M04) 19I field value is not consistent with 19J field value
(19M07) 19P field value is 4 and 19G and 19H is not a possible location for Loran-C navigation
(19M08) 19P field value is 5 and 19G and 19H is not a possible location for Chayka navigation

Figure 4.6: Some order 2 item, from message 19

4.1.2.5 Order three: Multi-message single-type assessment

The third-order assessments involve several messages, but of only one message type, and sent by the same emitting station (MMSI number). Those messages must also have been

received by the same receiving station (although this condition might be withdrawn with future developments). The scope is extended with respect to the first two orders and now takes into consideration the environment. The number of messages involved in those assessment items is variable, from only two (one message and the former one of the same kind from the vessel in question) or a time series with all known messages of this type coming from the vessel in question, in the study range or in the whole set of available data.

The main feature of those assessment is to concentrate on the evolution of a field along time, as well as the fields which are intended to change (which display a movement, speed or position) as the fields which are not intended to change (the dimensions of the vessel), or even the fields that are seldom expected to change, such as the name of the vessel. Another feature is the predictive position computation (with only two messages for instance), where the next expected position is computed from the former position, speed, course over ground and rate of turn data. Other kinds of pieces of information could also be predicted in this way, such as heading or speed. Source alignment could also be a way to provide additional information to this study.

A list of several different third-order assessment items is presented in Figure 4.7.

(02I01) 02B is not 0 and others fields are not the same
(02I02) 02C changes over time
(02I03) 02E evolution is not coherent
(02I04) 02F evolution is not coherent
(02I05) 02H and 02I field values evolution is not consistent with 02F, 02E, 02J and time
(02I06) 02K evolution is not consistent with 02E
(02I08) 02H and 02I field values are not usual values for those fields
(02I09) 02F data is not in accordance with usual 02F data for this vessel

Figure 4.7: Some order 3 item, from message 2

4.1.2.6 Order four: Multi-message multi-type assessment

The fourth order of integrity items deals with several messages of distinct type, but still coming from the same emitting station (and received by the same receiving station). It can either be a comparison between two data fields in two messages (in this case the closest message of the second kind in time is compared to the message of the first kind), or an assessment between one message of the first kind and a time series of messages of the second kind. Thus, we can concentrate on the possibility of the existence of two values in different single messages or compare a datum with a series of data from data fields from another message type. A list of fourth-order assessments is proposed in Figure 4.8

The number of items for each order and each message varies largely. A summary of the number of identified items for each message is presented in Table 4.3.

4.1.2.7 Assessment classification

Two main kinds of assessments can be discriminated: the ones that assess conformity, *i.e.* the conformity of the AIS message to the AIS specifications, and the ones that assess coherence between data fields and messages.

(0103I01) 01E and 03E evolution is not coherent
(0103I02) 01F and 03F evolution is not coherent
(0103I03) 03H and 03I field values evolution is consistent with 01F, 01E, 01J and time
(0103I04) 01H, 01I, 03H and 03I evolution is not coherent
(0103I05) 03K evolution is consistent with 01E
(0103I06) 01K evolution is consistent with 03E
(0103I07) 01J evolution is consistent with 03K evolution
(0103I09) 01F data is not in accordance with usual 03F data for this vessel
(0105I01) 01H and 01I evolution is not consistent with 05K and 05M
(0105I02) 05H is not consistent with 01H and 01I evolution
(0105I03) 05H is not consistent with 01F
(0105I04) 05H is not consistent with 01D
(0105I05) 05I is not consistent with 01E
(0105I06) 05J field value is 4 and 01H and 01I is not a possible location for Loran-C navigation
(0105I07) 05J field value is 5 and 01H and 01I is not a possible location for Chayka navigation
(0105I08) 05M data information is changed in a 01H, 01I location where such change is not usual
(0106I01) 06C and 06E vessels are too remote for their 01H and 01I field values
(0107I01) 07C and 07E vessels are too remote for their 01H and 01I field values
(0107I02) 07C and 07G vessels are too remote for their 01H and 01I field values
(0107I03) 07C and 07J vessels are too remote for their 01H and 01I field values
(0107I04) 07C and 07L vessels are too remote for their 01H and 01I field values
(0109I01) 01C and 09C are identical
(0110I01) 10C and 10E vessels are too remote for their 01H and 01I field values
(0111I01) 11K and 11L field values evolution is consistent with 01F, 01E, 01J and time
(0112I01) 12C and 12E vessels are too remote for their 01H and 01I field values

Figure 4.8: Some order 4 item, from message 1

The conformity items are all the first order items and a very small part of second order items, the one in which conformity is assessed but the value of another field is required in order to know if the value is present in the data field. It can occur in two cases: for message 24 which is in two separate transmissions, and one part of the message can be received and not the other part, so a query on an *ad hoc* data field is required to know is the expected data is present; and some message (such as 22 and 25) present two kinds of possibilities: address the message to a specific user or broadcast it to whom it may be received by, in this case, a Boolean data field must be queried to know in which case we are, and subsequently which are the nature of the relevant data fields in the message. In the first order items, the presence of a default value does not constitute a conformity issue, whereas the presence of an empty field in an item in which it is expected to have a value does.

The coherence items are all the remaining second order items, as well as all the third and fourth order items. Amongst all coherence items, eleven families of items have been discriminated. They are presented in Table 4.4, with a precision on which order their items can be found and a short description of their nature.

4.1.3 A logic-based formalism for item assessment

4.1.3.1 Item determination

Once the list of items determined, each item must be assessed following a rigorous process in order to check the coherence or the conformity of the fields within. The value associated with the item to the message assessed is assigned as Boolean, taking the value True or False, considering this value as an answer to the question:

Is the statement expressed in the item demonstrating an AIS-data integrity violation?

Message #	O1	O2	O3	O4	Total
1	10	3	9	51	73
2	10	3	9	51	73
3	10	3	9	51	73
4	11	4	5	22	42
5	8	0	8	44	60
6	4	3	2	12	21
7	6	10	5	36	57
8	2	0	1	0	3
9	7	2	5	10	24
10	5	1	2	7	15
11	11	3	6	29	49
12	4	3	2	12	21
13	6	10	5	36	57
14	2	0	1	0	3
15	11	3	3	16	33
16	5	3	3	8	19
17	6	1	4	20	31
18	9	1	5	31	46
19	12	4	10	35	61
20	3	0	1	0	4
21	7	3	7	10	27
22	12	4	4	3	23
23	13	2	2	0	17
24	2	4	7	16	29
25	2	2	2	8	14
26	3	2	2	8	15
27	7	4	6	28	45
Total	188	78	125	544	935

Table 4.3: Number of items by message and by order (O1 = Order 1, etc...)

If the item states something which occurs to end in an integrity problem, then the value associated to this item for this message is True, else it is False.

In many cases, the item essence will not be assessed, for several reasons. In this case, unless no assessment has been done, the value associated to this item is False, as the integrity of the system has not been violated. For instance, third order algorithms require a former message of the same type from the same sender, if such a message does not exist, it does not constitute an integrity violation, despite no third-order item was properly assessed. It is also the case for fourth order items with rare messages: for instance, as the reception of a message number 13 is quite rare, it is highly probable that the item "0113I01" will be seldom properly assessed, yet the value False will be assigned each time that no message 13 shows up.

4.1.3.2 Exemplification with five items in a logic-based formalism

Predicate logic formally presents the actions that will lead on the determination of the item integrity in a rigorous and unambiguous way. It relies on three main elements: the syntax, the data fields values and the expert knowledge values. A logic-based formalism based on predicate logic has been chosen for item assessment. The syntax is the whole of the elements that make the statements logical and understandable. They are:

- $\forall$, for all, the universal quantifier
- $\exists$, the existential quantifier

Families #	O1	O2	O3	O4	Description
Conformity issues	X	X			Non compliance to the specifications
Inconsistent field values		X	X	X	Inconsistencies between two or more values, from the same message or from different messages, such as speed over ground and rate of turn, or course over ground and true heading.
Data field evolution			X	X	The evolution of the value of one data field in several messages is not coherent, such as tremendous speed differences in short amount of time, or brutal change of position
Motion evolution			X	X	The motion values between several data fields are not in accordance, such as the position between two consecutive messages, given the speed over ground, the course over ground and the rate of turn
Unusual values			X	X	The value of one particular field is not in accordance with the usual values of this field for this vessel in other messages, such as a declared speed being over the usual cruising speed of this vessel
Overabundant reporting				X	The vessel sends too many messages with respect to its kinematic values and the expected transmission rate, in absence of any message 23
Overabundant communication				X	The study points out that two stations are communicating a number of times which is too important with respect to usual communication between stations
Remote communication				X	A communication between two stations for which the location data displays a distance between them which is too important for a communication to take place
Unexpected data field change		X	X	X	The value of one particular field has changed with respect to the former message of this vessel, usually a static information field for which data is not expected to evolve
Position fixing device issue		X	X	X	The vessel displays a position which is not compatible with the declared position fixing device it is using
Unexpected country location		X	X	X	The station is a base station or an aid to navigation and has position data which is not in accordance with the country displayed in the country code part of the MMSI number
Inconsistent response				X	The data field is part of a response message but the message that triggered this response is nowhere to be found, or the data field is an inquiry and the response is nowhere to be found

Table 4.4: Families of items and the order in which they are found

- !, the uniqueness indicator for existential quantifier
- $\vdash$, the implication
- $\neg$, the negation
- $\in$, the affiliation
- $\leftarrow$, the attribution
- $\top$, the True statement
- $\bot$, the False statement
- $\cup$, the union
- $\cap$, the intersection

The data field values are the values called in the frame of our item. According to section 4.1.1.2, they can take various types, and their number is function of the item itself, as it can require very few data field or several.

The expert knowledge is a set of values that have been determined for each item in which it is necessary. Some items, such as the ones assessing conformity, are straightforward, as the data value is either is accordance with the specifications or in disagreement with the specifications. However, for the determination of items in which, for instance, continuous data such as speed or location are used, for which distances are computed, a limit between the True and the False value must be set. In this perspective, expert knowledge is used.

In the remaining of this section, M_x stands for the whole of messages number x, m stands for a single message, D stands for a whole of data field values (a list of fields, set in accordance with the need), T_a is a time bracket standing for the reference time (T_a standing for $T_{assessment}$), T_c is a time bracket standing for the current assessment time (T_c standing for $T_{current}$)(*i.e.* we assess all messages received during T_c, using all messages received during T_a as our archived message database, this mechanism will be explained more in depth in section 5.1), R_m^z stands for the result of assessment item z on message m.

Example 1: Item 01S05: *01I: absolute value of the field is superior to 337F980h and is not 3412140h*

The purpose of this item is to check if the latitude value of message number 1 is within the scope of expected values, which are $[-90, 90] \cup \{91\}$ (because the extent of longitude is between -90 and 90 and the value 91 is the default value.

$$\forall m(D,t) \in M_1, D = \{id, lat\}, t \in T_c$$

$$((lat \in [-90, 90] \cup lat = 91) \vdash R_m^{01S05} \leftarrow \bot)$$

$$(\neg(lat \in [-90, 90] \cup lat = 91) \vdash R_m^{01S05} \leftarrow \top)$$

Example 2: Item 05S07: *05J: field value is between 9 and 14*

The purpose of this item is to check if fixing device value of message number 5 is within the scope of expected values, which are $[\![1\ ;\ 8]\!] \cup \{15\}$.

$$\exists K = [\![1\ ;\ 8]\!] \cup \{15\}$$

$$\forall m(D,t) \in M_5, D = \{id, fixdevicetype\}, t \in T_c$$

$$((fixdevicetype \in K) \vdash R_m^{05S07} \leftarrow \bot)$$

$$(\neg(fixdevicetype \in K) \vdash R_m^{05S07} \leftarrow \top)$$

Example 3: Item 16M01: *16C and 16E are identical*

The purpose of this item is to check if the MMSI of the source of the message is different than the MMSI of the vessel to which the message is emitted.

$$\forall m(D,t) \in M_{16}, D = \{id, sourcemmsi, destinationmmsi\}, t \in T_c$$

$$((sourcemmsi = destinationmmsi) \vdash R_m^{16M01} \leftarrow \top)$$

$$(\neg(sourcemmsi = destinationmmsi) \vdash R_m^{16M01} \leftarrow \bot)$$

Example 4: Item 01I05: *01H and 01I field values evolution is not consistent with 01F, 01E, 01J and time*

The purpose of this item is to check the position of the vessel is in accordance with the kinematic values of the messages. This item uses additional function of trajectory planning which have been named f and g in this item.

$$\exists f : [-180, 180] \times [-90, 90] \times [0, 102.2] \times [0, 4.21] \times [0, 360] \times [-180, 180] \times [-90, 90] \rightarrow \mathbb{R}^+$$

$$\exists g : [0, 102.2] \times [0, 4.21] \times \mathbb{N}^* \times \mathbb{N}^* \rightarrow \mathbb{R}^+$$

$$\forall m(D, t) \in M_1, D = \{id, lon, lat, speed, rateturn, course\}, t \in T_c$$

$$((\exists! m'(D', t') \in M_1, t' \in T_a, t' < t, D' = (id', mmsi', lon', lat'), mmsi = mmsi', \min_{\forall t' \in T_a}(t' - t)) \vdash$$

$$(\Lambda = f(lon, lat, speed, rateturn, course, lon', lat'), \Omega = g(speed, rateturn, t', t) :$$

$$(\Lambda < \Omega \vdash R_m^{01I05} \leftarrow \bot),$$

$$(\neg(\Lambda < \Omega) \vdash R_m^{01I05} \leftarrow \top)))$$

$$(\neg(\exists! m'(D', t') \in M_1, t' \in T_a, t' < t, D' = (id', mmsi', lon', lat'), mmsi = mmsi', \min_{\forall t' \in T_a}(t' - t)) \vdash R_m^{01I05} \leftarrow \bot$$

Example 5: Item 0305I06: *05J field value is 4 and 03H and 03I is not a possible location for Loran-C navigation*

The purpose of this item is to check if fixing device value of message number 5 is in accordance with the location of the vessel as displayed in message number 3. As the value of the data field 05J is 4, it is expected that Loran-C is used for position fixing. But Loran-C can only be used in given areas, that have been defined here under the variable Dom.

$$\exists Dom, x \in [\![1\ ;\ 8]\!] \cup \{15\}, x = 4, \tau \in \mathbb{N}^*$$

$$\forall m(D, t) \in M_3, D = \{id, mmsi, lon, lat\}, t \in T_c$$

$$((\exists! m'(D', t') \in M_5, t' \in T_a, t' < t, D' = (id', mmsi', fixdevicetype'), mmsi = mmsi', \min_{\forall t' \in T_a}(t' - t), t' - t < \tau) \vdash$$

$$(fixdevicetype' = x \cup \neg(\{lat, lon\} \in Dom) \vdash R_m^{0305I06} \leftarrow \top),$$

$$(\neg(fixdevicetype' = x \cup \neg(\{lat, lon\} \in Dom)) \vdash R_m^{0305I06} \leftarrow \bot)),$$

$$(\neg(\exists! m'(D', t') \in M_5, t' \in T_a, t' < t, D' = (id', mmsi', fixdevicetype'), mmsi = mmsi', \min_{\forall t' \in T_a}(t' - t), t' - t < \tau) \vdash R_m^{0305I06} \leftarrow \bot)$$

As a conclusion of this section, we can say that description logic is an useful way to describe items in a deterministic way under an unambiguous form (as it provides a Boolean result), in order to assess the integrity status that this item represents. In this scope, a substantial part of the 935 defined items have been formalised this way.

4.2 Falsification scenarios

4.2.1 Data for scenario assessment

Once computed, the Boolean result of the integrity items will be the cornerstone of scenario assessment, as it will be described in section 4.2.3. However, a study that would be based on sole system data would be possible but incomplete, as the environment in which the vessel evolves is ignored. In this scope, the addition of other data, which is not coming from the AIS system, is presented.

4.2.1.1 Necessity of data integration

The fact to concentrate on the sole data coming from the system itself is interesting for the integrity assessment of the system, and would be perfect if the system were an isolated system. However as the world around the system evolves such configuration is never found and it is always useful to rely on additional data in order to have a more accurate study. A proper understanding of a situation sometimes needs several points of view, and the point of view of a sensor might not be enough to discriminate a situation considered normal from a situation considered abnormal. Indeed, a situation considered abnormal with respect to one system data might be explained from another data source, and in a contrary case, an expected situation from a system point of view can be highlighted as abnormal in light of non-system data.

And of course, as the AIS is set on a vessel which has some characteristics, and evolves in a environment which has some others features, other non-AIS data can be used to deepen the analysis. As the environment itself evolves, the understanding of the behaviour of the vessels can be enhanced by those external sources of information. Indeed, on the one hand a piece of information or a group of pieces of information can look casually with perfect data integrity with only inner data assessment and some discrepancies from this normality could then be provided by external databases (e.g. a fishing vessel has a valid MMSI number and a classical fishing behaviour, however it is not registered in the official fishing fleet register); and on the other hand a piece of information or a group of pieces of information that can look anomalous on the basis of sole inner data could then be cleared by the use of external data and turn back into a normal behaviour case (e.g. a vessel which would deviate from its classical route due to the will to avoid an obstacle such as a storm).

The variety of possible datasets enables an approach on multiple frames, although it is an enhancement from the message-only study which constitutes the core of the integrity assessment.

4.2.1.2 Integrable databases

The databases that may be added for analysis extension are in general various, but they depend on the nature of the main system data.

Basically, every single source in which a single of its data fields can be useful in any type of assessment with the data coming from the system can be considered. As the system data can cover a wide range of information, the sources in question can be varied and come from several different domains. In general, it is not possible to establish an exhaustive list of such usable sources, because of several reasons: it is not possible to be aware of all available sources on a given subject, the sources evolve, appear and go out of date in an unpredictable pattern.

Those sources can come from several domains (albeit sometimes there is no clear belonging to a domain for a source), and the more close will be the domain in question to the data transmitted by the system, the more there is a chance that this database fits for any assessment. The variety of the domains covered by the selected databases (*cf.* section 5.2.1.3) shows the variety of information inside the system, that can therefore be assessed.

In the case of AIS messages, the selected databases must at least be related to maritime navigation, even by far. Three main families of databases have been discriminated: external information can be split into environmental, vessel-oriented and navigation-oriented databases. The AIS presents the advantage of having 27 different messages, each one carrying specific pieces of information, and as a whole, the system has a quantity of information coming from a number of data domains which is particularly important. The precision of some pieces of information and the large opportunities offered by some particular messages are far from being fully covered in our study.

Environmental data would embrace all kinds to database with a relation with the environment in which the vessel evolves. Meteorological databases with data such as temperature, pressure, wind force, waves height and rainfalls can be useful for behaviour understanding as stated before. In another category tidal information and bathymetric maps can be useful for the understanding of coastal navigation, particularly when it comes to notions such as draught and under keel clearance. In addition, databases representing sea areas enter in this category, as they give clues to the environment in which a vessel evolves. Such areas can include anchorage areas, protected areas, fishing grounds, exclusive economic zones and all zones related to a degree of sovereignty of a coastal state towards a vessel sailing off its coast (such as the notions of internal waters, territorial sea, archipelagic waters, contiguous zone or continental shelf), areas where undersea material in located, military restricted areas, port areas and in general any two-dimensional feature standing for a navigational-useful tool.

Vessel-oriented databases would gather the different fleet registers available, from the freely online available European Union Fishing Vessel Fleet Register to charged Lloyd's Register. In our case, we used the ANFR (*Agence Nationale des Fréquences*, the French National Agency for Frequencies) fleet register. Such registers contain data and a comparison of AIS data with them will then be possible. Insurance databases could also be used for such assessment, by themselves for a further study or from the outside with

publicly available information. In addition, receptor-specific pieces of information can be added in this category, such as the location of AIS data receptor, as well as their coverage areas: theoretical with respect to the local topography models and the Earth curvature or practical with respect to actual data reception, which may vary with time, meteorological conditions, time in the day or season in the year.

Navigation-oriented databases would concentrate all kind of information linked to the navigation and the route of the vessels, for instance all kind of traffic separations (such as TSSs), the aids to navigations such as navigational lines or fairways. The coastline, enabling several analysis, or the location of ports can be included in this category, as well as location of aids to navigation such as buoys, semaphores, beacons and lighthouses. Other sensors such as radar can be included, as well as origin and destination habits of vessels.

4.2.2 A range of falsification scenarios

4.2.2.1 General considerations

A falsification scenario is a case considered when we are involved in integrity analysis of a system. As systems in general can be falsified, it is important to point out the different cases in which they can undergo a falsification. As a falsification is the fact to transmit erroneous data or the fact to trick the system making him behave a way it is not supposed to do, a falsification case will be one particular falsification, one particular way to change data, input false data or force the system to behave the wrong way.

The diversity of the falsification cases will tend to reflect the diversity of possible ways to flaw the system, *i.e.* the possibility offered by the data itself: the more complex, the more data, the more complete the system is, the more possibilities for falsify data we will have; but also the possibilities conveyed by the way the system works and its interactions with the outer world (for instance a system based on electromagnetic transmissions will be able to suffer from interferences or any signal-related issues); as well as the possibilities conveyed by the exposure of the system to human interaction, *i.e.* how easy it is to modify the parameters of the system, to change the normal functioning of the system or the easiness to shut down the system.

Each one of those cases, once clearly stated, becomes a falsification case with a clear definition. Then, it is possible to assess those cases by associating to each case assessment elements in order to check the reality of the selected falsification. The advantage to consider falsification cases is that despite the fact that several individual assessment provide information about a discovered issue in the data, it will be possible to gather all those pieces of information in those falsification cases, being expected, in the frame of a risk analysis, that all cases belonging to a single falsification case will cause and imply the same kind of risks.

4.2.2.2 Selected cases

Several falsification scenarios are possible in the case of AIS falsification and spoofing, this section presents a list of falsification scenarios which is not exhaustive, but which corresponds to the ones we chose to implement in our work[1]. The scenarios are presented in the Table 4.5 and a description of each scenario is proposed subsequently, with an exception of the signal branch of the study, which is not the subject of this section.

Case #	Case Description
1.1	MMSI issue
1.2	Identity issue
1.3	Identity change
1.4	Ubiquity issue
2.1	Wrong position
2.2	Kinematic inaccuracies
2.3	Disappearing/Reappearing vessel
2.4	Spontaneous unexpected appearing
3.1	Message 22 alert
3.2	Message 23 alert

Table 4.5: Various considered falsification scenarios

The first family of cases is about static information and identity data of the vessels. In this family, we chose the issues related to the MMSI number, the identity issues, the identity change (that might be normal but might be suspicious) and the ubiquity issues (which is the fact to receive positions too remote from one single MMSI). The second family gathers analyses upon all dynamic and kinematic information of AIS messages, and the scenarios selected are about the wrong position of a vessel (such as inland reporting), kinematic inaccuracies, the fact to disappear and reappear in unexpected location (in this case a voluntary switch off of the system may be suspected) or the fact to spontaneously appear in an unexpected location. In addition to those classical approaches, a third one is proposed with the last family, with two messages which are amongst the most peculiar messages of the system: the message number 22 (channel management) and number 23 (group assign command). Only sent by base stations, those messages send operational parameters to mobile stations which are of paramount importance: they assign and can change the frequency of transmission (more particularly the transmission channel) in the case of message 22, and impose a transmission interval or a forced quiet time to mobile stations in the case of message 23.

A thorough presentation of those scenarios will be done in section 5.2.3.

4.2.3 From the integrity assessment items to the scenarios flag raising

4.2.3.1 Definition of flags

Inside the scenarios themselves as described in section 4.2.2, there are several ways to assess data, and several ways to point out the problems in the data, the discrepancies or

[1]Others have been implemented in the frame of the DéAIS project, such as the scenarios linked to the analysis of the signal, or the number of messages received by one station by unit of time, or the number of messages received from one given MMSI number (saturation)

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 basic elements of the scenario part of the study, they will serve as elementary bricks of the risk determination and risk level assessment presented lately in section 6. 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. The more available databases we have, and the more those database are able to provide pieces of information for a great number of flags, the more flags we will have.

Let S_i be the i^{th} scenario, n being the number of scenarios, C'_{S_i} be the number of flags directly linked to integrity assessment items and system data, C''_{S_i} be the number of flags linked to assessments with data coming from outside the system, we can say that the total number of flags F is:

$$F = \sum_{i=1}^{n} C'_{S_i} + C''_{S_i} = F' + \sum_{i=1}^{n} C''_{S_i}, \text{ as } F' = Cst = \sum_{i=1}^{n} C'_{S_i}$$

In this section, in the scope of the study of the AIS system, four kinds of flags are presented, two belonging to the family of the flags linked to integrity assessment items and system data (so which number does not vary over time): the integrity assessment items flags (section 4.2.3.2) and the vessel type flags (section 4.2.3.5); and two belonging to the family of the flags linked to non-AIS data (so for which the number of flags varies with respect to available data): the scenario-specific flags (section 4.2.3.3) and the maritime situational indicators flags (section 4.2.3.4).

4.2.3.2 Flags linked to the integrity assessment items

In section 4.1.3 was defined a method for determining the integrity status of every single integrity assessment item. However, this method treated data fields separately and it was not possible to easily drag any information from it. However, as it was demonstrated in section 4.1.2.7 that items can gather around families, the purpose is to extract from each set of items corresponding to each message type issues that are humanly easily understandable, which are the flags, presented in section 4.2.3.1.

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.

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.

In this example, the case "remoteness" for a message 1 is taken. For it, the associated items are: "0106I01", "0107I01", "0107I02", "0107I03", "0107I04", "0110I01", "0112I01", "0113I01", "0113I02", "0113I03", "0113I04", "0115I01", "0115I02", "0116I01", "0116I02", "0125I01" and "0126I01".

$$\exists K = \{0106I01, 0107I01, 0107I02, \ldots, 0125I01, 0126I01\}$$

$$\forall m(t) \in M_1, t \in T_c$$

$$(\bigcup_{i \in K}(R_m^i = \bot) \vdash f\_remoteness \leftarrow \bot)$$

$$(\neg(\bigcup_{i \in K}(R_m^i = \bot)) \vdash f\_remoteness \leftarrow \top)$$

As several scenarios have been set, and several families of items discriminated, several flags can be set, each one representing a given understandable type of issue. In addition to the "Remoteness" flag presented before, the flags that have been defined and tested will be presented in section 5.2.2.

Other flags, oriented towards the signal analysis part of the whole system can also be defined and raised if needed, for instance in order to know is a vessel is reporting too much in general, reporting too much in a given area, sending too many times the same message, or on the contrary if it does not send enough messages, or if it failed the signal consistency analysis performed.

4.2.3.3 Addition of scenario-specific data flags

In addition to the flags raised after a study on the data field, other flags coming from additional data can be raised. Those flags are totally dependent on the available databases, and each flag will be tied on the content of the database. Therefore there is no fixed list of those scenario-specific flags, as it will vary according to the available databases.

The fact to use such databases 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 database. As in 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.

The large amount of data within the AIS system and the variety of possible databases in the maritime domain increase the possibilities to find cases in which matching pieces of information are available, and therefore increase the possibility of integrity checks. A list of those databases will be presented in section 5.2.1.3. Two assessment examples of the many possible integrity checks and flag determination are presented here.

Exemple 1: f_fleetRegisterConsistency

This item assesses the conformity of AIS data with a given fleet register, in our case the European Union Fishing Vessel Fleet Register (which contains the list of EU fishing vessels). It turns out that the fields in common are the call sign (which will serve as foreign key, usable for a join), the vessel dimensions and the vessel name (which will be the values compared).

Let B be the EU fishing vessel database, b be an element of B, ϵ be a Boolean standing for the fact for B to be exhaustive ($\top$ = exhaustive), $Dist^{\alpha}$ be a semantic distance (here an Edit distance), $Dist^{\beta}$ be a Minkowski distance (here a Manhattan distance), Ξ and Υ be the respective thresholds for semantic and Minkowski distance for data compliance.

$$\forall m(D,t) \in M_5, D = \{id, callsign, name, dimensions\}, t \in T_c$$

$$((\exists! b(D_b) \in B, D_b = \{callsign_b, name_b, dimensions_b\}, Dist^{\alpha}(callsign, callsign_b) = 0) \vdash$$

$$((Dist^{\alpha}(name, name_b) < \Xi \cup Dist^{\beta}(dimensions, dimensions_b) < \Upsilon) \vdash (f\_fleetRegisterConsistency \leftarrow \bot),$$

$$(\neg(Dist^{\alpha}(name, name_b) < \Xi \cup Dist^{\beta}(dimensions, dimensions_b) < \Upsilon)) \vdash (f\_fleetRegisterConsistency \leftarrow \top)),$$

$$(\neg(\exists! b(D_b) \in B, D_b = \{callsign_b, name_b, dimensions_b\}, Dist^{\alpha}(callsign, callsign_b) = 0) \cup \epsilon = \top) \vdash f\_fleetRegisterConsistency \leftarrow \top$$

$$(\neg(\exists! b(D_b) \in B, D_b = \{callsign_b, name_b, dimensions_b\}, Dist^{\alpha}(callsign, callsign_b) = 0) \cup \epsilon = \bot) \vdash f\_fleetRegisterConsistency \leftarrow \bot$$

Example 2: f_disapreap

This item assesses checks if a vessel disappears in an unexpected disappearance area and reappears later in a unexpected reappearance area. For convenience, and as we do not have reliable practical coverage map to rely on, the area designated as Unexpected is defined by: the bay of Brest minus the port of Brest.

Let A_{bay} and A_{port} be the polygons representing respectively the bay and the port of Brest, and τ be the minimal time between two consecutive messages.

$$\forall m(D,t) \in M_1, D = \{id, mmsi, lon, lat\}, t \in T_c$$

$$(\exists! m'(D',t') \in M_1, D' = \{id', mmsi', lon', lat'\}, t' < t, t' \in T_a, \min_{\forall t' \in T_a}(t'-t), t'-t > \tau) \vdash$$

$$(((((lon,lat) \in A_{bay}), \neg((lon,lat) \in A_{port}), ((lon',lat') \in A_{bay}), \neg((lon',lat') \in A_{port})) \vdash (f\_disapreap \leftarrow \top)),$$

$$((\neg(((lon,lat) \in A_{bay}), \neg((lon,lat) \in A_{port}), ((lon',lat') \in A_{bay}), \neg((lon',lat') \in A_{port}))) \vdash (f\_disapreap \leftarrow \bot)))$$

$$(\neg(\exists! m'(D',t') \in M_1, D' = \{id', mmsi', lon', lat'\}, t' < t, t' \in T_a, \min_{\forall t' \in T_a}(t'-t), t'-t > \tau)) \vdash (f\_disapreap \leftarrow \bot)$$

4.2.3.4 Addition of MSI flags

Indeed, as it is not possible to rely only on system data, a peculiar category of non-system data gathers the flags that are not only related to system data but the assessment of which does not enter in any scenario case. By non entering any scenario case, they will not directly lead to any following risk assessment, however they are useful as they provide additional pieces of information which will be added to the other flags in the risk analysis.

In the maritime domain those flags represent relevant facts of the maritime navigation that are relevant for such assessments. Such artefacts are named Maritime Situational Indicators (MSI), after the name of the concept found in literature, where such pieces of information about the vessel and its neighbourhood have been developed by (Roy and Davenport, 2009) (called Maritime situational facts) and (Pallotta and Anne-Laure Jousselme, 2015) (called this way), used in (A.-L. Jousselme et al., 2016).

Therefore, in addition to the previous flags, other issues about the neighbourhood of the vessel, or its status, can be investigated. Those issues, linked to the environment (its location) or the surrounding vessels have the purpose of clarifying the navigational situation and helping the understanding of a maritime given situation.

A great amount of flags can be raised with MSIs, and some of them, the most interesting for the cases we are interested in, will be presented in section 5.2.2. Here is presented one simple algorithm of this kind, and as before the default value is False, changed to True when the event in question is verified.

Assessment Example: f_isinTSS

This item determines wether or not the vessel is in the TSS.

Let A be the TSS area,

$$\forall m(D,t) \in M_1, D = \{id, lon, lat\}, t \in T_c$$

$$(((lon, lat) \in \text{A}) \vdash (f\_isInTSS \leftarrow \top))$$

$$((\neg((lon, lat) \in \text{A})) \vdash (f\_isInTSS \leftarrow \bot))$$

4.2.3.5 Addition of vessel type flags

This last section, particular to our assessment of AIS, gathers all the flags that do belong to the category of system-only data but are not based on data integrity items. In our case, this section is made of the flags standing for the vessel type, as the vessel type has been discriminated as a key factor for the risk assessment of falsification cases that will be presented in section 6.

In our case, four vessel types have been discriminated, so each one 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. Three additional flags have been set for this case: if the vessel has not a valid vessel type (as a vessel can display a number which is not affiliated to any type), if a vessel has a type which does not enter the four main categories as we will define in section 6.5.1 and if, for a vessel, it is not possible to know the type because of lack of static information message linked to the MMSI (for instance if we get a message number 1 from a MMSI for which we do not have a message number 5, it is not possible to know its vessel type).

So seven flags have been set, of which in every single case one and only one is True and the remaining six are False. Those flags will be used in combinations for risk assessment as it will be stated in section 6.4. Here is presented an example of such flag assessment.

Assessment Example: f_isFishingVessel

This item determines whether or not the vessel is a fishing vessel (or if it emits a type corresponding to a fishing vessel).

$$\forall m(D, t) \in M_5, D = \{id, vesseltype\}, t \in T_c$$

$$((vesseltype = 30) \vdash (f\_isFishingVessel \leftarrow \top))$$

$$((\neg(vesseltype = 30)) \vdash (f\_isFishingVessel \leftarrow \bot))$$

Conclusion

In this chapter a methodology for system message assessment was presented, leading to the determination of flags for the vessel behaviour for the message. All system messages are assessed with respect to all the different integrity items, in order to point out the cases for which non-compliant or non-coherent data is shown. System data is also compared to non-system data in order to point out issues that could not have been revealed only by using system data. The scenario defined triggers different analysis according to their nature, and eventually raises flags if some item analysis or non-system data analysis

turns out to demonstrate an integrity failure. An implementation of this methodology is proposed in the next chapter with the use of AIS messages, the 935 integrity assessment items presented before, the AIS database enhanced by several non-AIS data, and the flags to assess that we are interested in.

Chapter 5

Implementation of a system of detection of corrupted AIS messages

Chapitre 5 : Implémentation d'un système de détection de messages AIS corrompus

Ce chapitre présente l'implémentation de la méthode proposée au chapitre précédent. Du point de vue du traitement de l'information, une approche à plusieurs récepteurs a été choisie. En effet, bien que notre validation ne reposera que sur les données d'un seul récepteur, son déploiement opérationnel complet nécessiterait le traitement de données issues de plusieurs récepteurs (dans le cadre d'une analyse centralisée des données par exemple, et cette perspective a été prise en compte.

L'analyse en temps réel se base sur le principe de l'analyse asynchrone des messages, avec un pas de temps, où à chaque nouveau pas tous les messages reçus n'ayant pas encore été traités le sont. Ainsi, nous sommes assurés que chaque message soit traité une seule fois. L'implémentation a été réalisée en python et les données ont été stockées au sein d'une base de données relationnelle postgres/postgis. A chaque boucle de traitement, les résultats intermédiaires et les résultats finaux de l'analyse sont stockés dans des tables spécifiques de la base de données, et peuvent être amenés à faire l'objet d'une requête SQL dans le cadre des traitements.

Ainsi, pour chaque item et pour chaque scénario proposé à l'étude, le programme python effectue une requête sur la base de données afin de récupérer les informations utiles pour l'étude en question, puis le programme analyse l'item, assigne une valeur et ce résultat est enregistré dans la base de données sous la forme d'une requête au sein du programme.

Afin de mener à bien les expérimentations, nous bénéficions de données AIS recueillies par une antenne située à Brest durant six mois entre 2015 et 2016, couvrant une grande partie de la baie de Brest, le goulet d'entrée ainsi que le trafic passant au large, dans le dispositif de séparation du trafic d'Ouessant. En plus de ces données AIS recueillies, des données AIS de synthèse ont été utilisées pour pouvoir bénéficier de cas dans lesquels une situation donnée se réalise.

Outre les données AIS, la base de donnée contient des données contextuelles permettant une étude croisée, ainsi des données relatives aux stations radio côtières, aux zones naturelles protégées, aux zones de mouillage, aux zones de pêche, au port de Brest, à la baie de Brest, aux zones économiques exclusives sont disponibles, de même que des registres de flottes de navires, les couvertures théoriques et pratiques du récepteur de Brest, les traits de côtes ou les positions des ports.

Parmi les fanions principaux sélectionnés, on peut noter ceux concernant une distance trop grande pour la communication, des problèmes avec le code pays du navire, son numéro de matricule, sa trajectoire, ou encore le fait qu'il présente de l'ubiquité ou une période importante sans transmissions. Des fanions liés aux données contextuelles viennent enrichir la connaissance de la situation, tels que le fait de ne pas être dans un registre de navire, ou d'y être mais de n'avoir pas des données cohérentes, ou le fait d'apparaître soudainement dans une zone inattendue.

Dix cas d'études ont été définis dans lesquels il est constaté que les fanions levés correspondent au comportement qui est attendu en de telles circonstances. Aussi, la réaction du système pour quatre cas qui sont l'ubiquité, la cohérence avec les registres de pêche, la position vis-à-vis des valeurs cinématiques et l'apparition inattendue ont été vérifiés. Il s'agissait, pour chacun de ces cas d'études, de s'assurer que les éléments que le système a mis en avant comme relevant d'une anomalie consistait bien en une anomalie au regard des données AIS et éventuellement contextuelles correspondantes. De plus, le temps de calcul s'élevant à environ 40% du laps de temps étudié, le système est assez rapide pour pouvoir effectivement être utilisé en temps réel.

Introduction

This chapter presents the actual implementation of the methodology presented in the previous chapter, leading to the risk level assessment of AIS messages. First are presented the implementation of the program, the architecture and the choices made in the coding part of the project. Then the available data is presented, the AIS training dataset as well as non-AIS data, and the evaluation scenarios are presented. Then, the validation of the approach is presented, consisting of the application of the information system in the previously stated evaluation scenarios and the observation of the flags raising.

5.1 Software and implementation

This section presents the implemented system in its various sides. First the fact that the implementation is made for a multi-receptor approach is highlighted, although only one receptor is used for the validation, the theoretical frame of the use of several receptors have been thank up. Then the principles of real-time analysis as implemented in the program are presented, followed by the implementation choices and the schematic architecture presented with deployment and sequence diagrams of how does the program process data.

5.1.1 A multi-receptor approach

5.1.1.1 From the reception of the raw AIS frame to the database storage

Upon reception from an *ad hoc* antenna, the AIS message has the shape of a raw frame of data, that must be processed in order to get exploitable data. This step is called parsing and occurs in a parser.

Despite the existence of software built-in parsers, and as our study require full handling of all dimensions of the process, we designed our own AIS parser in Java language, derived from an already existing parser[1].

The parser has the function to split the raw message into the data fields corresponding to the given message, the number of fields, the sequence of fields and the number of bits associated to each field, in accordance to the data specifications, as it was presented in section 3.3.2.

However, the AIS messages do not, in their large majority, carry date and time information. In order to have usable dates and times for the AIS messages we receive, the parser uses a clock to put a timestamp on each frame. The fact to put a timestamp is done at the time of parsing, however, as parsing is performed upon arrival of the message, it can be taken together with the reception time and, with respect to the distances in question and the speed of electromagnetic emissions in the air, the printed timestamp will in most cases be the emission time of the message.

Once all data fields have been discriminated, they are stored in a relational database (one table per message), the columns of which matching with the parsed elements. Two timestamp columns are added at the end of each table: the timestamp under the form date and time in day, for explicit understanding of the time of the message reception, and the timestamp transformed under the form of an integer, using UNIX epoch full seconds, allowing simple handling and computations on time values.

5.1.1.2 Various data source consideration

The AIS system is a global system. Therefore, the system must be used with several stations and must be able to take into consideration several cases. Indeed, as illustrated by Figure 5.2, both terrestrial and satellite reception must be handled, particularly in the case of a worldwide analysis, as non-coastal areas are not covered by terrestrial AIS. In addition, the same message can be received by several stations, and those messages, while being identical, might be (slightly) diversely timestamped.

In order to deal with those different receptors, a receptor id has been created and integrated in the database: in each message table, a column “receptor”, of type integer, have been created, with the purpose of uniquely discriminate each reception station. In our case, as we only use data from one reception station, this column value is always “1”, but the feature have been anticipated for further software evolutions.

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

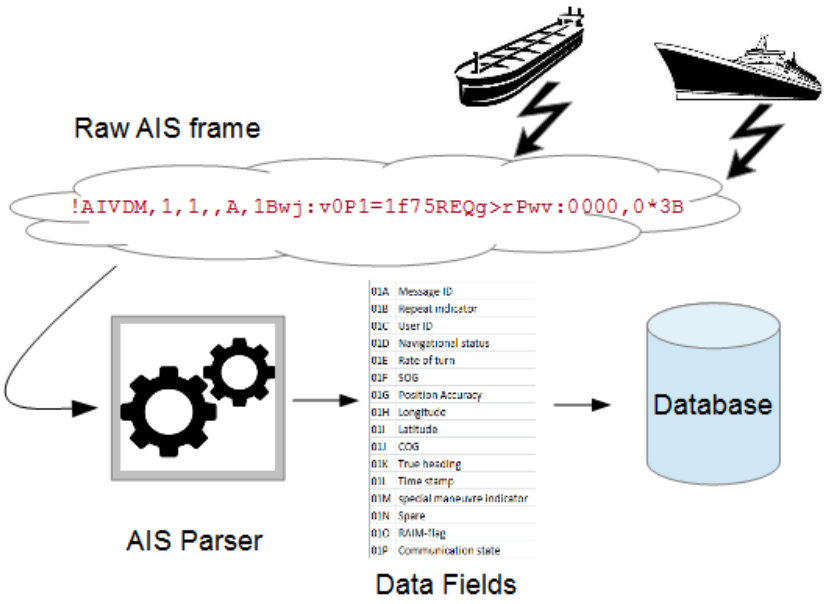

Figure 5.1: Process of AIS message parsing

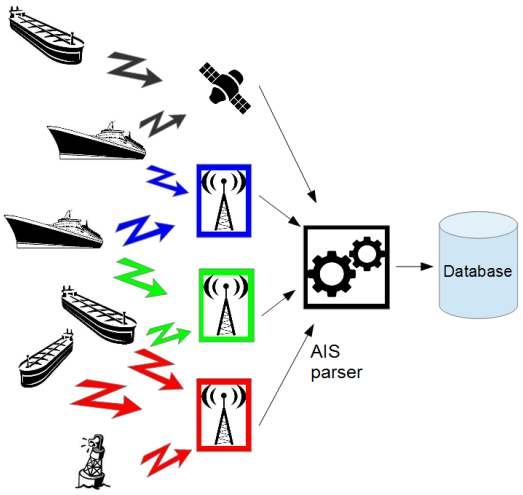

Figure 5.2: Integration of diverse data source

Such use of receptors opens a new dimension for integrity items. Indeed, in addition to the four principal orders of data treatment presented in section 4.1.2.1, a specific receptor-based order could be developed. As we do not have several receptors, such inter-receptor items have not been developed, but the nomenclature is flexible and opened for further evolutions.

5.1.2 Real time analysis

The system proposed in this section is designed to handle both real-time analysis case and work with archived data. As the handling of the case with archived data is quite straightforward, the handling of real-time data needs some particular features in the architecture.

As messages arrive continuously, and as some messages arrive at the same time, it is not possible to treat all the messages one by one, on the fly. However, it is possible to treat messages by small groups with respect to their time of arrival, *i.e.* at a given time, all messages received in the last t seconds are assessed, and the process is repeated, so that every message is treated at least and at most once. We consider $t = a + s$, with a being the assessment time, *i.e.* the whole computational time of the program and s being the waiting time, *i.e.* the time when the system pauses. This waiting time can be set at 5 seconds, 10 seconds or one minute according to the needs of the final user. This makes the system to be not an on-the-fly real-time system but an asynchronous quasi-real-time system. Figure 5.3 illustrates this method.

The need for this architecture is directly inducted from the data treatment process, where a group of messages with, for each of the 27 messages, their id between given bounds are consecutively assessed for the items, the scenarios, the flags and the associated risks, as described in chapter 4.

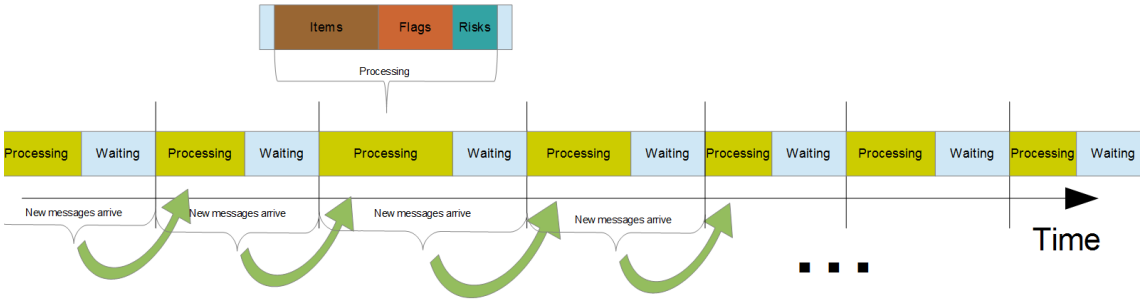

Figure 5.3: Data Analysis Flow

As it was stated in section 4.1.3.2, two temporal windows have been defined for computational purposes: T_a and T_c. T_c is defined by the temporal boundaries of the processed data in a given processing loop. At each loop, the new T_c must directly follow the T_c of the former loop, with no message loss and with no temporal overlap. T_a is defined by the temporal boundaries of the data taken into consideration in the cases of former data request, in items seeking for former data in order to make data comparison, or temporal series assessment.

T_a and T_c are defined as follow for the loop number N, considering t_{mini} = time of analysis beginning, t_N = time of beginning of the analysis for the loop N, t_{N-1} = time of the end of waiting time for loop $N-2$ (also time of beginning of the analysis for loop $N-1$).

$T_a = [t_{mini}, t_N]$ $T_c = [t_{N-1}, t_N]$

Figure 5.4 illustrates the functionning of continuous time sections assessments.

From the implementation point of view, a table was created in the database, with 27 lines and 4 columns. The 27 lines correspond to the different AIS message numbers: indeed, as each message has its own identification number counting, each message must have a different entry in the database, as the same time bracket will not correspond to the same identification numbers for the same message. The 4 columns stand for the message number and the three id numbers of the corresponding message, corresponding to the

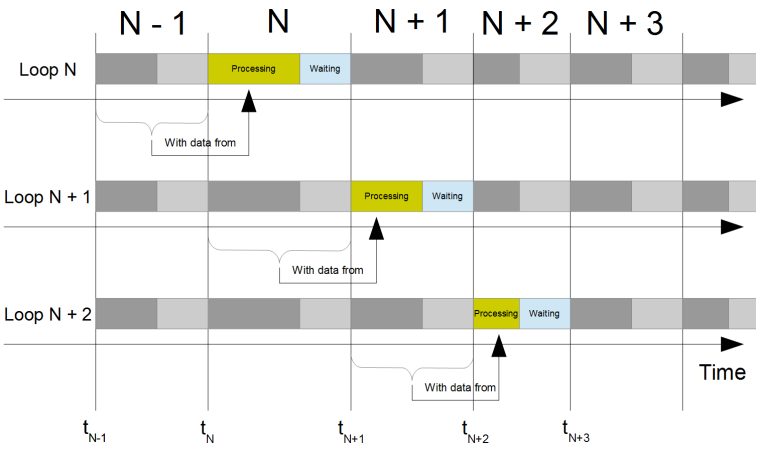

Figure 5.4: Time Sections Handling

times t_{mini}, t_N and t_{N-1} discriminated before. At each loop, the table must be updated with the new up-to-date data so that the analysis can be performed correctly, according to the correct time brackets and message spans.

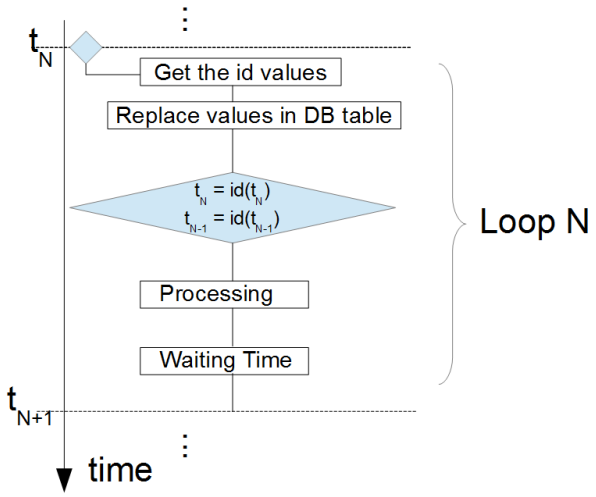

Figure 5.5: Functionning of a loop

At system initialisation, $t_{N-1} = t_{mini}$ (as defined by the user, either 0 or a given minimum value), and t_N takes the id at the time the first processing unit begins.

As the system is also usable with archived data, it works as follow: the system is made of a single loop, processing all messages at the same time. However, as the database table is used in the problem, it must be filled in with fixed values, corresponding, for each message, to the minimal (for t_{mini} and t_{N-1}) and the maximal (for t_N) values of id the user wants to assess. Of course, the id bounders must be consistent with time for the different messages, so that the multi-type multi-message assessment defined in section 4.1.2.1 is possible.

5.1.3 Implementation choices

5.1.3.1 Use of Postgres/PostGis

For data storage and data manipulation, it was chosen to use a relationnal database management system. This choice was made for the ability of such systems to find data, write, sort, modify or transform data in database, and ensuring the user of a level of robustness of the analysis by avoiding information loss or partial assessment. The choice of the widespread relational database management system Postgres was made, using the SQL querying language, with the adjunction of the Postgis extention, for the treatment of spatial features.

5.1.3.2 Use of Python

As there was a piece of software to be built, the choice of a programming language was made. The language Python was chosen for several reasons: easy to handle, Python enables the database querying with embedded SQL and convenient handling of query results. In addition, Python has good math libraries for statistical computations.

5.1.3.3 Use of user interactions

User interaction and user choice occurs at several points of the process. Although the user is not expected to input any information while the program is running, some parameters and input data are needed. Those are the director file, the scenario list and the waiting time.

The director file is a text file taken as input by the program. In this director file are listed all the items the user want to be assessed by the program. Each new item must occupy a new line in the text file, and each one of the lines will trigger the study of this item in the program, as it will be explained in section 5.1.4. By default, during a standard assessment, all implemented items must be assessed, and therefore the default director file is the full list of all available items, but the choice to remove any item or set of items that would be of no interest for the user is up to him or her. It is also possible to leave the director file empty, so that the previously computed item results can be re-used for scenario and risk assessment, as it will be presented in section 5.1.4.

The scenario list is specified by the user, in which the user designates the scenarios he or she wants to be assessed. Indeed, some scenarios might not be of interest for the user. However, as the risk assessment is based on flag combination, as presented in chapter 6, and that the flag determination is based on the several scenarios assessed, the fact not to choose all scenarios for assessment will prevent all the flags from being assessed, and therefore induct a non-encompassing risk assessment, which could be acceptable with regard to the user needs. As the scenario computation is based on item assessment, each scenario is linked to a list of items which must be present in the director file. Should only one of the needed items be absent from the director file, the corresponding scenario assessment could not be performed properly. By default, as and alike all items which are

listed in the director file, all scenarios are present in the scenario list.

The waiting time is, as presented in section 5.1.2, the time between the end of one loop and the beginning of the following loop. By default, the time is set at 10 seconds, but the user might want faster refreshes (up to 1 second) or longer interval time (several minutes or hours are conceivable).

5.1.3.4 Separation between item execution and item computation

The proper use of the program requires the assessment of a list of items. For practical reasons, it was decided to separate two main bodies of each item assessment: the execution, in which the program queries the database to get all the needed information (information about the message in question, information about all other messages that are involved in the item assessment) and the computation, in which the algorithms take as inputs all data field information. In this way, many algorithms will be similar (as in the same family of assessment, as defined in section 4.1.2.7, algorithms tend to look alike). It is a way to factorise the coding, and a way to facilitate algorithms changes if needed.

5.1.3.5 Keep open to new features

As the program is evolutive, and as the AIS system itself it not fixed, the way the program was conceived is explicitly done for enhancement and evolution. Indeed, the list of items is not fixed, as the AIS system still evolves, the items might come up and be included in the program. Similarly, some deep features of AIS were not processed, such as the content of binary data message. Their adjunction would create new items to be integrated in the system.

The nomenclature is also flexible, as it allows new kinds of item nomenclature, involving more messages if needed, and more importantly the items of another order (that would be the fifth one) in the case of the simultaneous use of several receptors.

The scenario case is also open, as new scenarios with new flags might come up, adding new features to the flag combination list and new ways to compute risk levels.

5.1.3.6 Storage of intermediate results

For the storage of intermediate results, it was chosen to keep nothing as variable in the program, but to store everything in the database right away after each item assessment and after each scenario computation. This enable the systematic querying of the database by the program, and the storage of data for future reference, particularly for comparisons between assessments. Are stored in the database: the item computation results, the flags after scenario computation and the risk level associated with each AIS message.

Are also stored in the database pieces of information useful for the computation itself, such as the current work window (the minimal and maximal id of the computation for

each message, as it was presented in section 5.1.2) and the risk level tables (that will be presented in section 6.5.1).

5.1.3.7 Independent treatment of scenarios

The several discriminated scenarios are treated separately for various reasons. On the one hand, such separation enables, as displayed in section 4.2.3.2, not to run every scenario if not needed. On the other hand, it is a implementational help as it helps us to discriminate several files and parallelise the implementation of the program.

5.1.3.8 Use of non-AIS data

The use of non-AIS data has been soon discriminated as an important feature of this work, as it takes into consideration the environment in which the vessel evolves. However, as it is not possible to know which non-AIS data will be available, it was not possible to include those analyses into the scheme of items, which are only built for AIS information which can be assessed at each message and whatever information available. Therefore, the integration of such external assessment was added to the scenarios analysis, as those database are in general oriented towards one particular scenario, and specific flags are displayed with respect to each database available.

5.1.4 Schematic architecture

5.1.4.1 Database properties

In the database, messages must be treated as they arrive (according to the process defined in section 5.1.2), without any conjecture on their timestamp, therefore the primary key must be an identifier which increments as messages arrive. AIS messages will be stored in a relational database in which each message type must have its own table (each one with its incremental id then), the properties of receptors must be stored, as well as external information.

The database gathers several main parts (which are presented in Figure 5.6): the AIS message database, with its 27 tables standing for the different messages, as presented in section 4.1.1.1. The real-time info gathers all information in relation to the treatment of data in near-real-time asynchronous mode, especially the values of the minimum and maximum id that must be treated at each loop for each message, as described in section 5.1.2. External data is a database gathering all non-AIS data useful for the further analysis of scenario cases, as described in section 4.2.1.2. The databases available in our case are presented in section 5.2.1.3. The receptor data database gathers all information about the various receptors used, such as the type of material used, the location of the receptor, the theoretical coverage area and the practical coverage area. The analysis results database gathers all tables created during the analysis and used as analysis intermediates. A final result table presenting the highlighted anomalies with the degree of risk associated is also present.

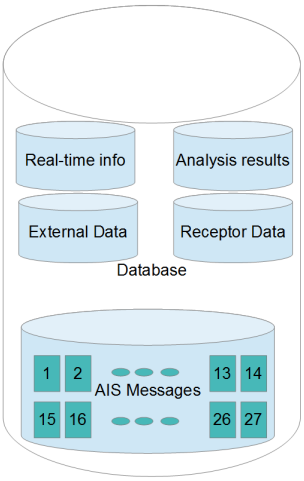

Figure 5.6: Database composition

5.1.4.2 Deployment diagram

The deployment diagram presented in Figure 5.7 displays the different parts of the system.

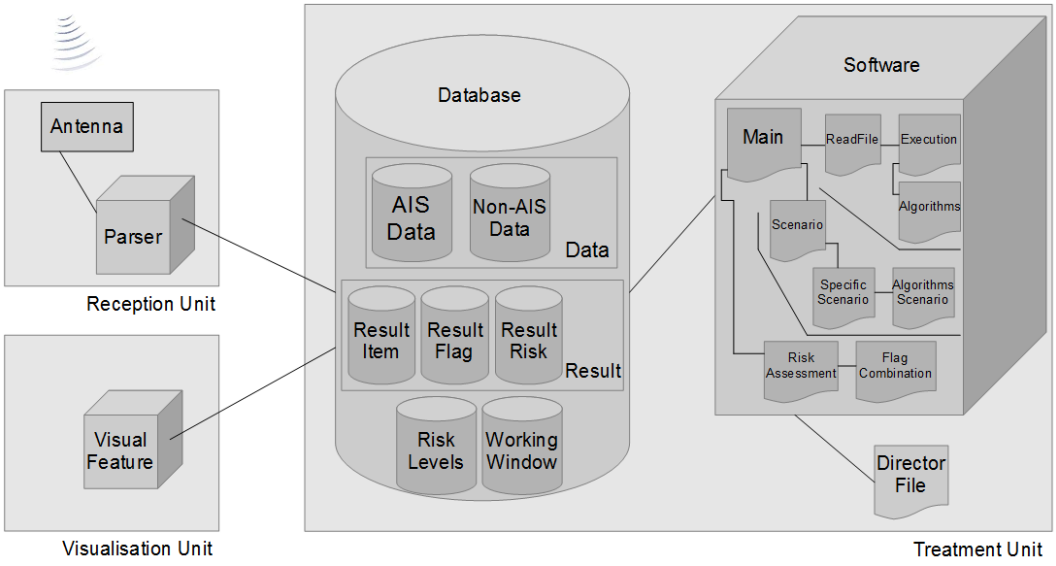

Figure 5.7: Deployment diagram

The reception unit has the purpose of receiving the physical signal, process it and parse the AIS messages, then push them into the database. The software uses the director file and database information to process data, as it will be presented in the following subsections, and the database presents the features presented in section 5.1.4.1, as receptor data is considered as non-AIS data and risk levels come in addition for risk assessment. The visualisation box is the feature enabling the visualising feature for the end user. Although the development of this unit is not part of this study, it is necessary to consider it as it will take in entry parameter one of the outcomes of our piece of software.

The program functions according to the following steps: working window update, Item Assessment, Flag assessment, Risk assessment, waiting time and it goes all over again.

More precise information about the way the program works for the item, flag and risk assessment are presented in the following sections (in this chapter) 5.1.4.3, 5.1.4.4 and (in the next chapter) 6.6 respectively.

5.1.4.3 Item assessment in the program

In the program, as presented in Figure 5.8, the item assessment involves the external file in which the items are listed, various elements of the database (the AIS messages, the working window table and the result tables), as well as several elements of the program which are the main file, and some functions, including the functions for item execution and the functions for algorithm calculation.

This part of the program works as a loop, looping on the lines of the director file, with an initialisation done at the first line. Then, four cases are possible, and four alternative computation cases occur at each loop. The read item is either of order 1 and 2 (so with only one message to query), or of order 3 and 4 (so with several messages to query), or with a bad format (non-existent item), in this case the program returns the fact that this item has not been treated) or no value, in the case the last line has already been computed at the previous loop, and in this case the loop ends right away.

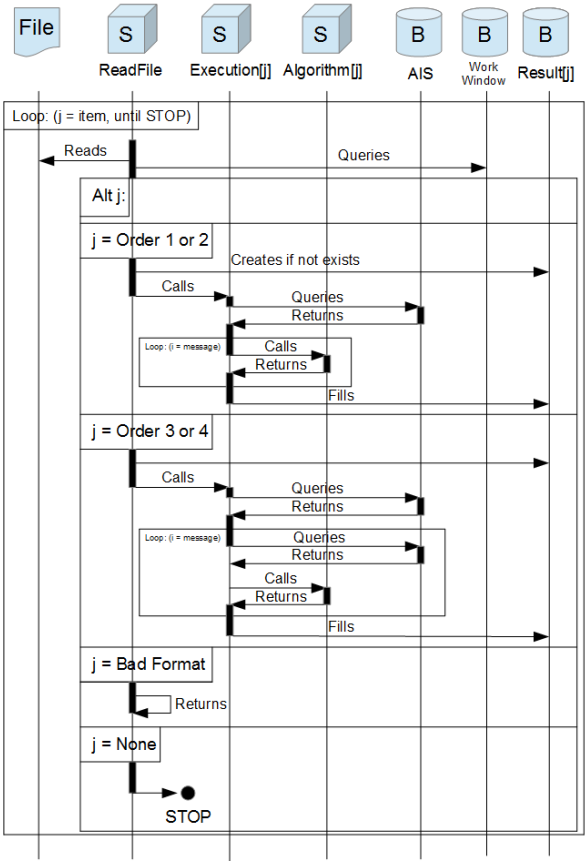

Figure 5.8: Sequence Diagram of the Item Assessment

In both order 1 and 2 and order 3 and 4, the table of results for the item is created in the database if it does not exist yet. Then the AIS database is queried for the interesting data fields for this item and for the temporal span corresponding to the working window. Once

the AIS values are returned, they are stored in a table and a loop occurs on it, treating one by one the messages within the working window. At this point, the treatments differ with respect to the order of the algorithm.

If the item is of order 1 or 2, the values are directly assessed by the corresponding algorithm, and filled in the result table of the item once all the messages in the working window have been treated.

If the item is of order 3 or 4, another query to AIS messages database is necessary in order to get all the other pieces of information from the other messages, either from the same message type (order 3) or from another message type (order 4). Once the result of the query has been stored, the assessment via the corresponding algorithm can occur, followed by the filling in of the result table in the database once all the messages in the working window have been treated.

Out of the 935 defined items of all order, a total number of 666 have successfully been implemented into our system.

5.1.4.4 Flag assessment in the program

The way the flag assessment is done in the program is presented in Figure 5.9 and involves several parts of the program (the main scenarios file, the specific scenarios file and the algorithms related to the scenarios) and several parts of the database, which are the AIS messages tables, the non-AIS features tables, the results of the item algorithms, the result of the flag assessments and the working window table.

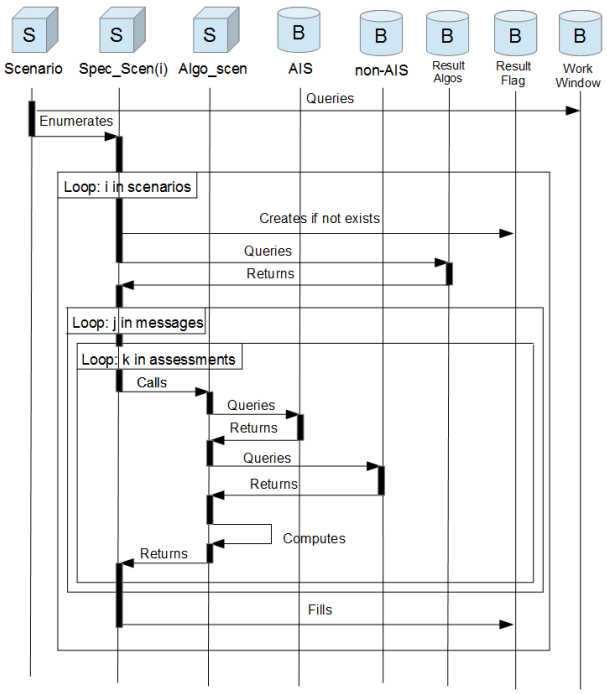

Figure 5.9: Sequence Diagram of the Flag Assessment

First, the working window table is queried in order to get the corresponding data. Then the main scenario files contains a vector in which all the scenarios to be assessed

are defined, and a loop is performed in the enumeration of this vector (in order to assess only the scenarios we choose to analyse).

For each of the scenarios, the flag table corresponding to the scenario in question is created, then the corresponding item results are queried and stored in the program for further flag studies. Then, for each one of the messages in the temporal working window, and for each one of the various assessment leading to the determination of a flag, the same process is repeated.

In each case, the specific scenario case calls the algorithms corresponding to the given assessment, and this algorithm successively calls AIS and non-AIS data in order to perform a computation leading to potential raising of the flag. The flag results are then returned to the specific scenario file, and once all assessments for each message of the temporal window have been performed, all the computed flags are stored in the table created in this respect.

5.2 Experiments

In this section, the available data are presented, on the one hand the AIS data, with both the dataset from the Brest antenna and the messages constructed *ad hoc* for this analysis, and on the other hand all the non-AIS databases available which can be, as stated previously, of environmental, vessel-oriented or navigation-oriented nature. Then a selection of the various flags that have been put in place are presented, and the selected cases in which those flags will be assessed are presented, belonging to three families of analyses: the one based on the identity of the vessel, the one based on the kinematics of the vessel and the one based on the use of highly unlikely types of messages.

5.2.1 Available data

5.2.1.1 Received AIS data

By setting up an antenna in the Brest Bay, near the Brest city, in direct sight of the Brest bay bottleneck, it was possible to get AIS data from a great part of the bay, from the entering and exiting traffic and on the passing-by traffic in the Ouessant TSS.

All the data received by this antenna during a time span of six months is used for our study, from October 1^{st}, 2015 to March 31^{st}, 2016. The number of messages of each type is presented in Table 5.1.

As the messages were divided in families, Table 5.2 presents the repartition of message number by family. This table shows that the positioning messages form the vast majority of all received AIS messages.

The image in Figure 5.10 show the spatial extent and repartition of our spatial AIS messages, a close-up on the Brest harbour, the data being reduced to the amount of data received during one single day by our antenna (Figure 5.11).

Message #	Number	%
1	15003029	62.4
2	194	0.001
3	3225148	13.4
4	2803971	11.7
5	882708	3.7
6	0	0
7	2	ϵ
8	150026	0.6
9	303673	1.3
10	2769	0.01
11	315	0.001
12	0	0
13	0	0
14	46	ϵ
15	11	ϵ
16	0	0
17	0	0
18	954462	4.0
19	128	0.001
20	1	ϵ
21	505764	2.1
22	0	0
23	0	0
24	201567	0.8
25	11	ϵ
26	5	ϵ
27	63	ϵ
Total	24033893	100

Table 5.1: Number of messages per message type

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 5.2: Number of messages per family type

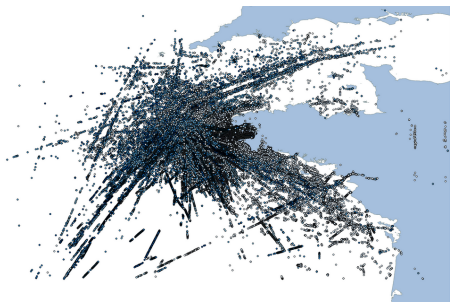

Figure 5.10: A view of the location of the geolocalised points in our AIS dataset

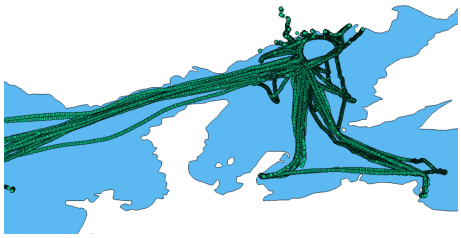

Figure 5.11: A view of the messages in the Brest Bay received during one full day

It can be demonstrated that some AIS messages come from circa 700 km, although the theoretical maximum distance is about 50 km. This is due to the atmospheric ducting effect. Figure 5.3 shows the distance repartition for AIS messages number 1.

Area	# of messages	% of all messages
$\leq$ 5km	2489174	17.01
5 km $\leq$ D $\leq$ 10km	7832507	53.53
10 km $\leq$ D $\leq$ 15km	412234	2.82
15 km $\leq$ D $\leq$ 20km	424469	2.90
20 km $\leq$ D $\leq$ 25km	499194	3.41
25 km $\leq$ D $\leq$ 30km	843719	5.77
30 km $\leq$ D $\leq$ 35km	1252174	8.56
35 km $\leq$ D $\leq$ 40km	329931	2.25
40 km $\leq$ D $\leq$ 45km	290382	1.98
45 km $\leq$ D $\leq$ 50km	61844	0.42
50 km $\leq$ D $\leq$ 55km	56087	0.38
55 km $\leq$ D $\leq$ 60km	58947	0.40
60 km $\leq$ D $\leq$ 65km	39516	0.27
65 km $\leq$ D $\leq$ 70km	19211	0.13
70 km $\leq$ D $\leq$ 75km	13391	0.09
75 km $\leq$ D $\leq$ 80km	10346	0.07
$\geq$ 80 km	369903	2.53
Total	15003029	100

Table 5.3: Number of messages 1 per distance section in our dataset

5.2.1.2 Synthetic AIS data

In addition to genuine AIS data, some AIS frames were built intentionally in order to be able to validate some scenario cases. Indeed, some of the cases involve rare or never received messages, other require a condition on data which is rare (for instance an AIS location on shore, or a weird-looking trajectory such as the one presented in (Balduzzi, Pasta, et al., 2014)). In order to have data to assess, and test and validate the algorithms, some *ad hoc* AIS frames were done, each one corresponding to a given scenario.

The fact to built those frames and use them directly rather than broadcast them and insert them into a stream received by the receptor is linked to the nature of those messages, which can carry information which is about a potential threat of terror attack, or about acts of cyberattacks. The experimental broadcast of such messages is not welcome, particularly as the station is in the neighbourhood of a Sub-Surface Ballistic Nuclear Basis.

In order to do so, a software prototype has been developed to generate the frame, either by selecting each value out of the various data fields, or by dynamic generation of a vessel behaviour by the program.

5.2.1.3 Non-AIS data

As stated in section 4.2.1.2, three kinds of non-AIS databases are discriminated: environmental, vessel-oriented and navigation-oriented. 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 global. Of course, such datasets must be in accordance with the location and the spatial extent of the data assessed.

Environmental

World Seas. This database is made of polygons standing for the main seas of the main contiguous body of water. It can be useful to determine of two vessels are broadly in the same region of the world, or as a quick test for communication between a coastal station and a vessel

Dredge material areas. In some maritime area, caution in the activities must prevail as some material lay on the ground. This database gathers the location of areas where dredged material or other potentially harmful materials (such as explosives or chemical waste) have been deliberately deposited. Thus, some particular assessments can be done in those areas when a dredging vessel or any other vessel with a vessel type unveiling possible action of the bedrock is located in those areas or in close proximity to them.

Radio Coastal Stations. This database gathers radio beacons which are on the shore of the French region of Brittany.

Natura 2000 areas. In this database, a collection of maritime Natura 2000 areas is shown for all the countries of the European Union. Those areas are protected from an environmental point of view and human activities inside the area or in its neighbourhood must be assessed.

Anchorage areas. In this database are gathered a series of anchorage areas in the proximity of the Brest harbour. Those areas are dedicated areas for vessels which must wait before entering the harbour, or in its proximity, so that stopped vessels are not staying within communication routes. Then, if a vessels presents a very low or null speed, it is possible to check whether or not this vessel, according to its type, is in an area where anchorage or loitering is logical (*i.e.* such anchorage areas, or ports). As it is a spatial feature, trajectory intersections are possible, and inquiries on the vessels speed within this area can be done.

FAO fishing areas. This database gathers all information about the worldwide regions that the Food and Agriculture Organisation of the UN has set for the world seas. In our case, its use is restricted to the fishing industry, for example to know if fish coming from a given vessel has a declared FAO fishing area consistent with the areas in which the vessel effectively sailed and had a fishing ground behaviour.

Polygon of an harbour. In our database, we have a polygon representing the harbour of Brest. It is then possible to do spatial request on this basis in order to understand some behaviours, monitoring the vessels entering or exiting this area. As some operations are likely to occur in a port, such as a name change, it would then be useful to see if the location of identity changes intersects with ports polygon, particularly

when it comes to raising alerts.

Polygon of a bay. In our database, we have two polygons: one representing the Brest Bay strictly speaking and another one representing the extended Brest Bay. Likewise with the harbour, it is then possible to manage spatial request in order to be aware of the traffic, and in relation to AIS falsification, it can be proceeded to the verification of the appearance of the vessel, as the vessel coming to Brest are expected to be visible before their entrance in the bay.

Fishing locations. A database providing usual fishing grounds can be used to assess if a vessel displaying a fishing behaviour is doing it inside an usual fishing ground, or if it is not the case. An assessment on the fishing pressure can also be extracted from this database.

Exclusive economic areas. In this database, all the Exclusive Economic Zones of the world are gathered. This can be useful to determine the quality of some at-sea operations as well as the competent court in some activities.

Vessel-oriented

Fishing Vessels Fleet Register. The European Union provides a list of all fishing vessel that uses a flag of one of the countries of the Union, free of charges. This fleet register is very partial because it only concerns fishing vessels, representing only a fraction of the navigating vessels, but it can provide a fair training sample for some algorithms, that could be extended if a more complete database is available. The data field to be matched with AIS data would be the international reference call sign, then the comparable data (*i.e.* same data present or inferable in the two databases) being the name and the vessel length.

ANFR Fleet Register. This table represents the fleet register of the French *Agence Nationale des Fréquences*, which includes a great number of French-registered vessels.

Receptor location. This table gathers the location of the various AIS receptors. In our case only one is used, however the method has covered the integration of several receptors. As the receptor location is known, the conformity of message reception can be assessed, and the communication between stations can also be checked.

MMSI country codes. The three-digit country code at the beginning of each MMSI number are paired in this database table with the name of the country. It is then possible, with another table, for instance the country polygons, to check if a vessel mainly deserves ports of its flag (detection of flags of convenience), or if a coastal station with fixed coordinated is well located within the country its country code displays.

Theoretical coverage of the receptor. In this table, for each receptor, its theoretical coverage region is materialised by a polygon. Thus, it is possible to assess the location from which an emitted message is received, particularly if it is far outside the area. In addition, the arrival of a new vessel and the disappearance of a sea-going vessel are expected to happen around the limit of the theoretical coverage for a given receptor, and it is then possible to assess if it is the case. The range of the theoretical coverage can be computed by the formula for radio communications provided by the IMO.

Practical coverage of the receptor. In this table, for each receptor, its practical coverage region is materialised by a polygon. With respect to the theoretical coverage geometry, it has the advantage to take into consideration the possible masks that the antenna has with respect to some sea areas, and possibly to consider variations of the range due to particular conditions.

Navigation-oriented

European coastline. This database provides the coastline for European shores. Yet it is not worldwide, it is more than enough for us as we focus on French coasts. The algorithms can then be extended to other continents if an usable database of the coastlines of this continent is added. The knowledge of the coastline enables several analyses, mostly spatial, such as the proximity of a vessel from the coast, to ensure the proximity of a coastal station from the coastline, or to give clues on the possible masks between stations that could be caused by topography.

TSS of Ouessant. This base contains the area of the TSS of Ouessant, off the coast of Brittany, separating the traffic in both directions that are from or are going to either the English Channel or Cape Finisterre in Spain. As a TSS is a security tool in maritime navigation, security assessment can be performed, with for instance the presence of a vessel outside the navigation channels, or the fact for a vessel to leave its channel, or even to find out a vessel that would optimally cross the TSS, thus augmenting the risk of boarding.

Location of ports. In this database, the location of ports around Brittany is gathered. As ports are supposed to be designated in the "Destination" field of message 5, the fact to have the name and location of ports will enable studies on vessel trajectory, for example to check if a vessel is heading towards the declared port or not, and even to know if a vessel if heading towards a port or if it is heading towards the coast. As a vessel can head to a port without physically pointing its course over ground towards it, a study on the profusion of vessels declaring the same destination while not heading to it can also be performed. Similarly, a database of fishing ports in provided in another database, for related studies.

Navigational lines. This database gathers recommended lines for maritime navigation. As those lines are recommended, vessels are welcomed to follow them for optimal security and vessels are expected to follow them as much as possible. Studies on vessel trajectories and distance to the recommended line can then be performed.

Location of fairways. This database gathers fairways around Brittany. Fairways are the main bodies of water on which vessel are located. It is commonly expected to find a vessel on those fairways, and whereas navigation is free in authorised areas outside fairways, it could be considered as an anomalous behaviour, so such an assessment based on such database has its place in our study.

5.2.2 Discriminated flags

As seen in section 4.2, flags that can faithfully and clearly describe the situation must be set, and four families of flags have been discriminated: the flags linked with the integrity

assessment and system data items, the flags that describe the vessel type, the flags that are linked to scenario-specific analyses and those standing for maritime situational indicators.

The flags describing vessel types have all already been presented in section 4.2.3.5. Their number might be extended in the future if more precise vessel type families are designed, but as for now, the flags are: is a cargo or tanker, is a cargo or tanker carrying hazardous goods, is a passenger vessel, is a pleasure, fishing or service vessel, is of other type or has an incorrect vessel type, given that for each vessel one and only one of those flags is raised. An additional flag is here in case no static information message have been linked to the studied message (in this case, it is not possible to know the vessel type).

As for the flags linked to the items, several scenarios have been set, and several families of items discriminated, several flags can be set, each one representing a given understandable type of issue. In addition to the "Remoteness" flag presented before, the flags that have been defined and implemented are:

- f_country: This flag is raised when the country code of a vessel is not valid
- f_MMSI: This flag is raised when the MMSI has not a valid form, in any of the possible shapes a MMSI number can take (as presented in section 3.3.2.3.1)
- f_ubiquity: This flag is raised when a vessel displays diverse locations in a short amount of time
- f_nextposition: This flag spots the case when the position of a vessel is not in accordance with the kinematic and positional values of the message before
- f_trajectory: This flag is raised when one point out of a trajectory is not in accordance with the remaining of the trajectory
- f_bigTemporalGap: The flag is raised when two messages are separated with an amount of time too important according to the technical specifications
- f_outOfScope: The flag is raised if the location coordinates are not valid
- f_outOfArea: This flag is up when a vessel transmits in a location where it should not locate itself due to its declared position fixing device
- f_unusualLocation: This flag is raised when a vessel displays a location which is highly unusual for it

This list is not exhaustive, and other flags, oriented towards the signal analysis part of the whole system can also be defined and raised if needed, for instance in order to know if a vessel is reporting too much in general, reporting too much in a given area, sending too many times the same message, or on the contrary if it does not send enough messages, or if it failed the signal consistency analysis performed.

Some of the flags describing scenario-specific situation, as presented in section 4.2.3.3 are presented here. Those flags, in addition to the flags raised after a study on the data fields, are other flags coming from additional data that can be raised. Those flags are totally dependent on the available databases, and each flag will be dependent on the given

database used. Therefore there is no fixed list of those scenario-specific flags, as it will vary according to the available databases. Some examples of such flags are:

- f_notInFleetRegister – Needs a fleet register database. The flag is raised if the vessel is not in the database while it should (as a cargo is not expected to be in a fishing vessel register, but a fishing vessel is). This flag has been implemented in the program.
- f_fleetRegisterConsistency – Needs a fleet register database. This flag is raised if the studied is in the database and if the data within has discrepancies with the AIS data. This flag has been implemented in the program.
- f_isInBlacklist – Needs a vessel blacklist. The flag is raised if the vessel is in the blacklist
- f_notHeadingTowardsDeclaredPort – Needs a port list database with port locations. The flag is raised is the vessel is not following a route that leads to the port declared in the "Destination" field
- f_hasBathymetricDiscrepancies – Needs a bathymetric database. The flag is raised if the vessel is located in a location it should not be according to local bathymetry and declared draft value
- f_disapreap – Needs expected appearance areas for the station. The flag is raised if a vessel disappears from a location located outside the expected appearance/disappearance area and reappears a long time after in a location which is outside the expected appearance/disappearance area. This flag has been implemented in the program.
- f_suddenapp – Needs expected appearance areas for the station. The flag is raised if a vessel suddenly appears in a location which is outside the expected appearance/disappearance area. This flag has been implemented in the program.
- f_slowSpeed – Needs anchorage areas, fishing grounds. The flag is raised if a vessel has a slow speed without being in a area where having a slow speed is normal

As described in section 4.2.3.4, a great amount of flags can be raised with MSIs, and it is not possible to extract an exhaustive list of them. However, the Table 5.4 presents some flags for cases we might be interested in. Not all of those flags have been implemented yet, however a thorough study may need such an implementation.

5.2.3 Assessment cases

In section 4.2.2.2 were presented the selected cases at a glance. In this section, all those cases that have been named will be presented in details, in order to highlight their legitimacy for being case studies acknowledging our hypotheses. Three families of cases are present, linked to the identity (beginning by "1"), linked to the kinematics (beginning by "2") and linked to the peculiar messages 22 and 23 (beginning by "3"). In the remaining of this manuscript, all MMSI numbers presented in cases in which real data have been used have been anonymised.

f_isHeadingTowardsAPort	f_isInRestrictedFishingArea
f_isHeadingTowardsTheCoast	f_isInExclusionArea
f_isLoitering	f_isInProximityToACoast
f_isCarryingHazardousCargo	f_isComingFromADubiousLocation
f_isInTSS	f_isHeadingTowardsADubiousLocation
f_isNotRespectingATSS	f_isNotFollowingAMaritimeRoute
f_isInPort	f_isInCollisionCourseWithVessel
f_isInAnchorageArea	f_isInCollisionCourseWithInfrastructure
f_hasPassengerVesselBehaviour	f_hasAlledgedLocationInHazardousArea
f_hasAlledgedLocationInExclusionArea	f_hasAlledgedLocationInFishingRestrictionArea
f_hasAlledgedLocationInAnchorageArea	f_hasAlledgedLocationInCollisionCourseWithVessel
f_hasAlledgedLocationInCollisionCourseWithInfrastructure	f_hasFishingVesselBehaviour
f_hasCargoTankerBehaviour	

Table 5.4: List of MSI flags

5.2.3.1 Case 1.1: MMSI value and country code

In this scenario, the fact for a vessel to sail with an impossible MMSI number or an unattributed country code is assessed. Indeed, the MMSI layout can only follow some patterns, at it was shown in section 3.3.2.3.1, and in addition in each MMSI number, three of the digits stand for the country, and there is a list of possible combinations. If the vessel displays a number which does not match with any country, it is a case of falsification.

Experimental Case (A):

In this case, one item per message is directly linked with the validity of the MMSI number. Several cases must be assessed, as MMSIs are different for mobile stations and coastal stations. In addition, the country code is verified and the problems are raised under the flag f_country. All the integrity assessment items used in this case are of the first order, as the expected format for a MMSI is given by the specifications and the list of country prefixes is fixed (flag f_MMSI). In this example, we took messages number 1, supposed to have vessel-only MMSI source field (9 numbers, included the country code) and messages number 4, supposed to have base station-only MMSI source field (7 numbers, included the country code). The system response is presented in Figure 5.12 and the Table 5.5 presents the flags raised for each of the cases.

Case #	Mess #	MMSI	f_country	f_MMSI
1	1	227111111		
2	4	227111111		√
3	1	2271111		√
4	4	2271111		
5	1	282111111	√	
6	4	2821111	√	
7	1	2821111	√	√
8	4	282111111	√	√

Table 5.5: System reaction to several MMSI numbers

5.2.3.2 Case 1.2: Identity incompatible with database

This scenario deals with the cases where the values linked to the vessel are not in accordance with some data that might be available through databases. The feasibility of this scenario highly depends on the external database (mainly a fleet register), as a common

	id bigint	messnum integer	idmess bigint	warningmessage text
1	1	1	100011101	Message 100011101 from vessel 227111111 has a correct MMSI number
2	2	4	100011401	Message 100011401 from vessel 227111111 has an incorrect MMSI format
3	3	1	100011102	Message 100011102 from vessel 2271111 has an incorrect MMSI format
4	4	4	100011402	Message 100011402 from vessel 2271111 has a correct MMSI number
5	5	1	100011103	Message 100011103 from vessel 227111111 has an incorrect country code number
6	6	4	100011403	Message 100011403 from vessel 2271111 has an incorrect country code number
7	7	1	100011104	Message 100011104 from vessel 2271111 has an incorrect MMSI format and an incorrect country code number
8	8	4	100011404	Message 100011404 from vessel 227111111 has an incorrect MMSI format and an incorrect country code number

Figure 5.12: System response of MMSI treatment

field must be found out and used as the comparison basis of the analysis. Most matches will be done with the MMSI number or the call sign of the vessel. Typical comparisons will be about the name of the vessel, the length of the vessel or its gross tonnage, for instance. The completeness and accuracy of the database must be determined prior to the analysis, as the completeness assesses the number of vessel in the database with respect to all the vessels we might receive a message from, and the accuracy the fact for the database to be more or less up-to-date, with more or less accurate data.

Experimental Case (B):

This case is directly linked to the scenario-specific flags as a fleet register database is needed. Integrity is assessed between the AIS messages and the fleet registers available, where first the fact to belong in the database is assessed (which will result in the raising of the flag f_isNotInFleetRegister if it is not the case) and second the checking of the various data in both AIS and fleet register databases in case there is a match, in order to assess the integrity of information within (raising the flag f_fleetRegisterConsistency). Figure 5.13 displays the process for the study of this case. As it involves static information, only messages 5 are assessed. In our case, the elements belonging to both databases were the name of the vessel and the dimensions of the vessel. The Levensthein distance was taken as edit distance, with a maximal admissible distance of 5 (in order to take into consideration the small discrepancies between string values standing for the name of the vessel) and a total difference of 2 meters was the maximal admissible value for length and width of the vessel, as rounding errors makes any value beyond it possible with genuine data. Figure 5.14 shows the verbose version of messages undergoing this treatment.

5.2.3.3 Case 1.3: Identity changes

In this scenario, the identity changes of vessels are recorded and analysed. In the AIS messages, the identity of a vessel is displayed in static information messages through four identity items. In a current use, we expect those fields to remain largely unchanged. Those fields are the name of the vessel (data field 05G), the MMSI number (05C), the IMO number (05E) and the international reference call sigh (05F). In the case of class B vessels, only three of those fields are displayed, which are the MMSI number (24C), the name of the vessel (24E), and the international reference call sign (24H). Out of those four fields, only the IMO number, attached to the physical structure of the vessel, is never expected to change. The MMSI number and the international reference call sign are assigned by the country of the flag, so when a vessel changes its affiliation, new data are allocated and those fields can change. For the name, it can change even more often, at the inclination of the owner, providing the fact to let the authorities know. The treatment of such data

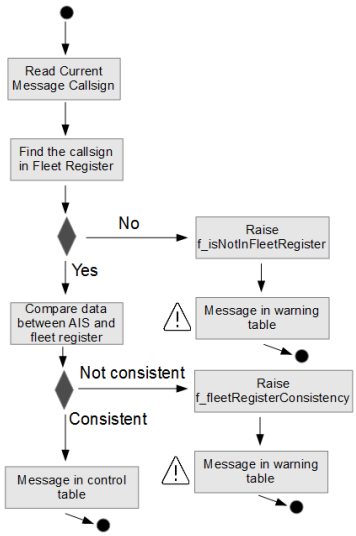

Figure 5.13: Processing of the presence in the fleet register database

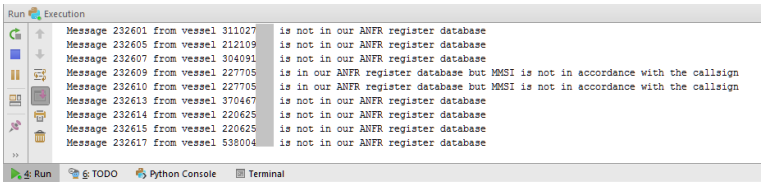

Figure 5.14: System response of the presence in the fleet register database treatment with real AIS data

quadruplets (or triplets in the case of class B vessels) has the purpose of highlighting the cases when the quadruplet change, as it can occur when any one of the four fields change. A change on the IMO number is likely to be a falsification as changes on this field are not expected. In the case of the name of the vessel, it can either be an actual name change (then the location of occurrence and authorities must be taken into consideration), or it is an attempt to conceal its identity. As the flag country assigns the MMSI number and the international reference call sign, the analysis for mismatching with those fields must be done using a comparison with a state fleet register, and the location where the change has occurred.

Experimental Case (C):

This case is about the identity changes and the inconsistencies between declared identities between various messages number 5. The principle of data within quadruplets was explained just before, as a quadruplet is a unique combination of { MMSI number, IMO number, Name, Call Sign }. In this part, the program is discriminating every unique quadruplet, highlighting the cases where one or several of the data fields that constitute the quadruplet have changed. Figure 5.15 displays the process for the study of this case, Figure 5.16 shows the system response to such quadruplet analysis and the Figure 5.17 shows the quadruplet table as shown in the result database. A new entry for which at least one of the fields has already been seen will trigger the flag f_severalIdentities.

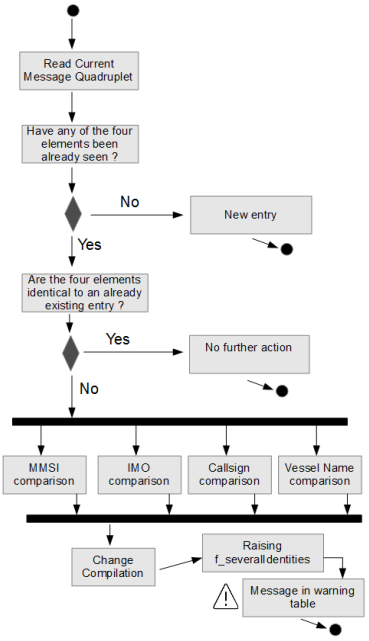

Figure 5.15: Processing of the compliance with the fleet register database

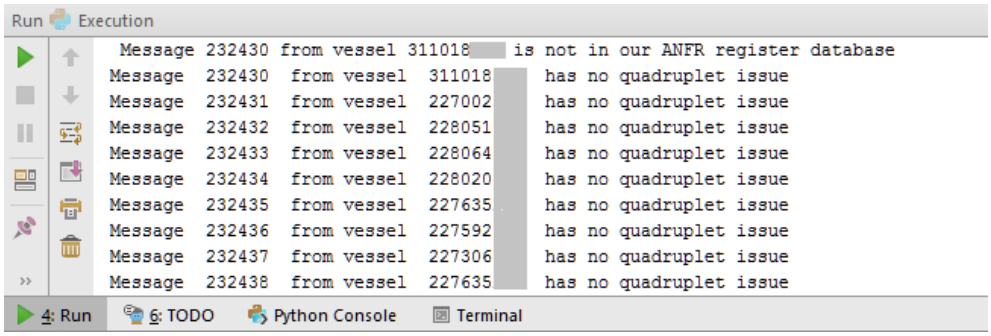

Figure 5.16: System response of the compliance with the fleet register database treatment with real AIS data

5.2.3.4 Case 1.4: Ubiquity cases

This scenario consists of the fact to have several vessels at the same time in different locations but using the same identity (*i.e.* the same MMSI number). This phenomenon, that we call ubiquity, can have several causes: the malfunction of the GNSS of a vessel, the fact that several vessels in the same area or belonging to the same company use the same identification number, or most probably the identity theft of one vessel by another one. Those kind of identity concealing is the fact of vessel owners willing to hide their identity and present a friendly one, for instance in cases of troubled areas or to conceal embargo violation.

Experimental Case (D):

As an example of this ubiquity case, a trajectory has been created with 9 points numbered temporally from 1 to 9, simulating two vessels, one going eastwards towards mainland France, and one going southwards in the Brest bay, as shown in Figure 5.18. The timestamps for each couple of points (1 and 2, 3 and 4) are similar as their difference

	id [PK] bigserial	sourcemmsi integer	imonumber integer	callsign text	shipname text	shiptype integer	idmess5 bigint
1	1	227002	0	FV6852	ENEZ SUN 3	0	172962
2	2	228186	9269518	FMAA	ARGONAUTE	51	172963
3	3	228211	0	FMDV	F/V L ESTRAN	90	172964
4	4	304091	9509255	V2GU5	HC JETTE-MARIT	70	232413
5	5	227003	0	FV5533	ENEZ EUSSA 3	60	232414
6	6	227635	0	FGE4002	TERENEZ	60	232415
7	7	227705	262144	FGD5860	BINDY	60	232416
8	8	227574	0	FGD5859	TIBIDY	60	232417
9	9	220625	9400708	OWBJ2	CHARLOTTE THERESA	89	232418
10	10	227580	0	FGD6565	LOUARN	60	232419
11	12	311027	9475600	C6YM6	SONANGOL SAMBIZANGA	80	232421
12	13	227148	7932214	F.G.B.P	LANGEVIN	33	232422
13	14	228190	0	FMAS	BOUGAINVILLE	30	232423
14	15	227005	0	FN9820	BREST-PILOTE	50	232424
15	16	248043	9480368	9HA2141	AMUR STAR	89	232425
16	18	226263	9308687	FZTC	ABEILLE BOURBON	51	232427
17	19	311153	9001772	C6WL6	POLAR SPIRIT	80	232428
18	20	234056	7703106	GKCT	VN PARTISAN	70	232429
19	21	311018	9410569	C6XP7	NORWEGIAN EPIC	60	232430
20	22	227002	0	FO4922	ANDRE COLIN	60	232431
21	23	228051	8617342	FHFO	SAINT DENIS	52	232432

Figure 5.17: Quadruplets table in the database

is only about 5 seconds. As presented in Table 5.6, the flag for ubiquity is raised from the second point on, as well as the flags related to the trajectory and the coherence of the consecutive points.

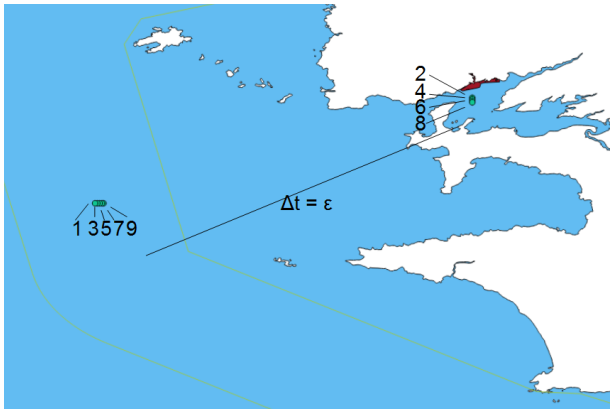

Figure 5.18: Ubiquity scenario cases

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_ubiquity		√	√	√	√	√	√	√	√
f_trajectory		√	√	√	√	√	√	√	√
f_nextPoint		√	√	√	√	√	√	√	√

Table 5.6: Table of flag raising in the ubiquity case

5.2.3.5 Case 2.1: Wrong position

This scenario deals with the cases of the outbreak of a vessel not only outside an expected area (as seen later in scenario 2.4), but in an impossible area, such as land or outside the latitude and longitude range, as shown in Figure 5.19.

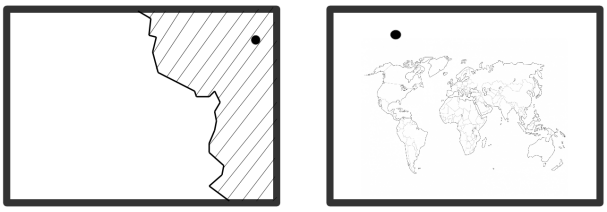

Figure 5.19: Wrong position scenario cases

The appearance on land represents the fact not to appear on a body of water, which can be caused by a rough falsification try, by the spoofing of the system, but it can also be caused by AIS signal emission attempts by people which does not want to disturb the marine traffic, or AIS switched on by accident or on purpose when the vessel is on dry cock, or when the vessel is being transported by another vehicle using terrestrial means. Such a study must be careful of the fact that inland navigation and therefore inland AIS does exist and a good modelling of navigable waterways is needed to avoid false positives.

The fact to appear outside the range of the map is the fact to receive an AIS message with at least one of those statements false: the vessel is within $[-90, 90]$ degrees in latitude ; the vessel is within $[-180, 180]$ degrees in longitude. As it is unlikely to be a misconfiguration of the system or any kind of GNSS failure, such scenario is characteristic of an AIS falsification (disappearance of the map) or signal spoofing cases, as AIS signal emission attempts could also use such coordinates in their location fields in order not to disturb the marine traffic.

Experimental Case (E):

For the case of wrong position, a set of 9 data points has been created which starts in the Brest Bay, goes north, crosses the restricted military area and finished on land. Speed, heading and distances have been set consistently so that the trajectory point could be real if they were not on land. Several flags have been raised, the sudden apparition for the first point, then trajectory that went in the direction of the Brest harbour, then inside the restricted area, triggering several alerts, before hitting the land and continuing its course. The risks triggered have been indicated in the table, however the level of the risks is not assessed, as it will depend on the type of vessel.

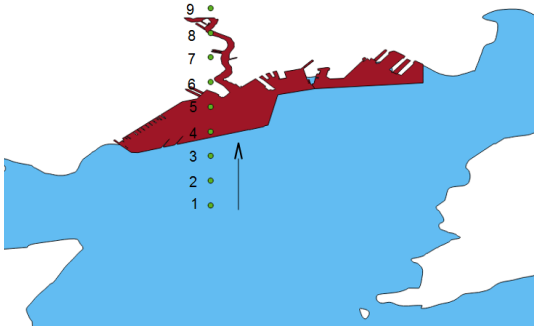

Figure 5.20: Location of points in the inland positioning case

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_restrictedArea				√	√				
f_isInLand						√	√	√	√
f_CoastProximity					√				
f_headingTowardsPort	√	√	√						

Table 5.7: Table of flag raising in the inland positioning case

5.2.3.6 Case 2.2: Kinematic inaccuracies

This scenario concentrates on cases of two incoherent consecutive points, and in this scope, four cases have been discriminated, as displayed in the Figure 5.21. The case a) is one single outlier point out of a regular-looking trajectory, that can be originated by an error of the system, a falsification test at the level of the station or a spoofing test from an external actor. The case b) shows the brutal shift of a trajectory which seems to be regular before and after it. Such a case can be caused by a continuous software or hardware malfunction in which a bias has been activated, a proper falsification from the vessel or a spoofing case. The falsification case could be favoured if the area in question is in the near location of a place where a vessel could be willing to hide some information. The case c) draws the case of a vessel changing its course in a regular-looking trajectory, but in which other AIS data would disagree with the observed change. The same causes as case b) can be proposed. The case d) displays a trajectory of a vessel going back and forth from two locations (more or less remote), actually forming two separate trajectories of two vessels sailing under the same identification number. This case would be typical of identity theft or identity sharing.

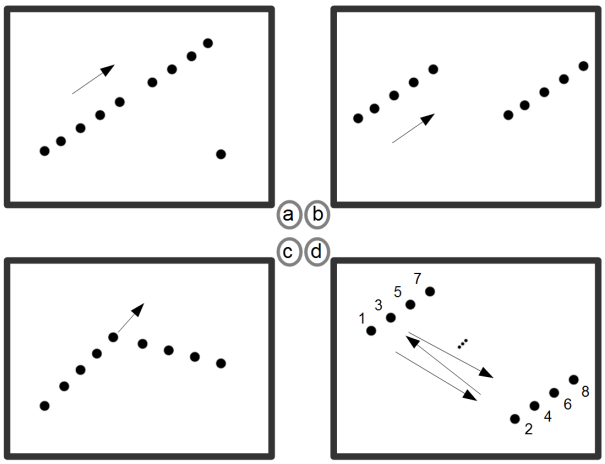

Figure 5.21: Kinematic inaccuracies scenario cases

Experimental Case (F-G):

For the case of kinematic discrepancies, two sets of 9 data points have been created. The first one, presented in Figure 5.22, represents the case of a normal trajectory for which only one point is out of the expected path. For the remaining points, all kinematic data are in accordance, particularly the speed, heading and physical distance between the points. The point number 5 has a offset of 0.02^o south of its expected position. For the points number 5 and 6, the flags of next position and ubiquity are raised, as shown in Table 5.8. Note that the ubiquity flag is only raised because of the lack of proximity

between the points: would that point number 5 appeared with an offset small enough to be within the accessibility range of the vessel, this flag would not have been raised.

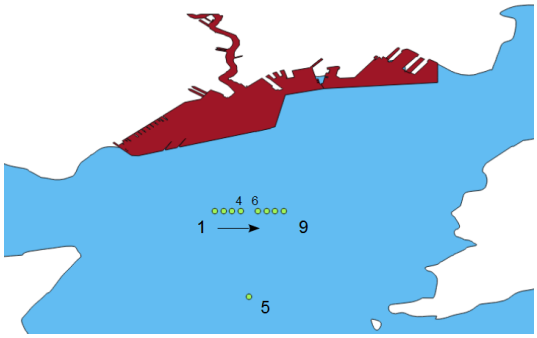

Figure 5.22: Location of points in the whereabouts spoofing case

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_nextPosition					√	√			
f_ubiquity					√	√			

Table 5.8: Table of flag raising in the whereabouts spoofing case

For the second case, presented in Figure 5.23, the trajectory is shown as going northwards until point 5, then eastwards from point 5 on. However, the kinematic data field of heading displayed only one value: 0 (so northwards trajectory), resulting in the points 6 to 9 to raise the flag of incoherent next point, as it should be north of the previous one and not east (Table 5.9). However, the flag ubiquity is never triggered as each point is within the accessibility range of the previous one.

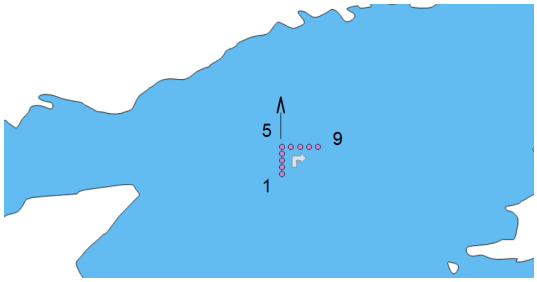

Figure 5.23: Location of points in the dynamic inconsistencies case

5.2.3.7 Case 2.3: Vessel disappearance and later reappearance

This scenario gathers cases of vessels disappearing and reappearing after a long timeframe, the value of this gap being a variable of the study. In Figure 5.24, the case of a reappearance in the same location (case e) and in a different location (case f) are presented. Several causes have been discriminated for finding the reasons of such observed behaviour, which include the fact to turn off the system, the crossing of masked locations, the fact to be too far to be received, an attack on the signal (jamming or saturation attack) or a natural saturation of the system. If the vessel never reappears, the hypothesis of a shipwreck can be taken into account.

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_nextPosition						√	√	√	√

Table 5.9: Table of flag raising in the dynamic inconsistencies case

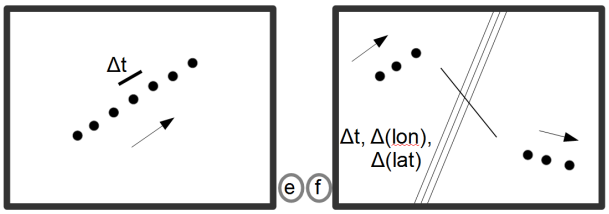

Figure 5.24: Vessel disappearance/reappearance scenario cases

In the case of the AIS switched off, we have to concentrate on the area of the last received message, whether or not it is in a good visibility area, and assess, according to the speed stated in the last received message, the number of missing expected messages. The status of the vessel, whether in blacklist or not, must also be assessed, as the historicity of the vessel must be taken into consideration. For the cases of the crossing of a masked area or being at the edge of the reception area, both the expected trajectory and a map displaying the coverage area at the given time must be provided, in this scope, the expectance of the fact not to receive messages can be assessed. The natural saturation of the system mainly occurs in the case of airborne AIS reception, when several organised areas are in the sight of the reception, as seen in section 3.2.3.3. In this case, an important number of vessels will be affected by this problem in the area.

Experimental Case (H-I):

For the case of temporal issues, two cases have been discriminated and studied with two created sets of 9 points: the fact for a vessel to stop emitting for a long time without significant position change between the last point before the silence and the first point after it, and the fact for a vessel to instantaneously display a huge spatial gap between two seemingly normal trajectories.

The first case is displayed in Figure 5.25, with the temporal gap taking place between the points 4 and 5. For our experiment we chose a gap of 10,000 seconds, between normal trajectories. The flag temporal gap was raised, as expected, for the point number 5, as shown in Table 5.10. The flag of unexpected disappearance followed by an unexpected reappearance has also been raised. This is because we defined two expected appearance/disappearance areas which are the port and the limit of the coverage area, as shown in section 5.2.3.8. As we have both Brest Bay and Brest Port geometries (section 5.2.1.3) in our study, we can consider the geometry Brest Bay minus Brest Port as an unexpected location for disappearing or reappearing.

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_temporalGap					√				

Table 5.10: Table of flag raising in the big temporal gap case

The second case is more complex, presented in Figure 5.26 with results in Table 5.11. A big spatial gap occurred between points 4 and 5, without out-of-normal temporal gap

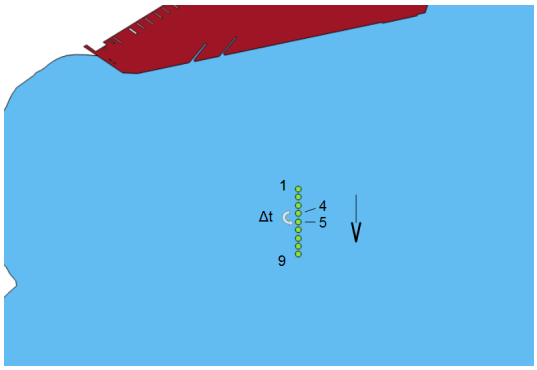

Figure 5.25: Location of points in the big temporal gap case

between those points. This scenario raises several flags: the next position flag for point 5, but also the trajectory flag between points 3 and 6, as well as the coast proximity flag due to the location of the points 5 to 9 (which is the reason why the risk boarding have been selected), and the ubiquity flag, only for the point 5.

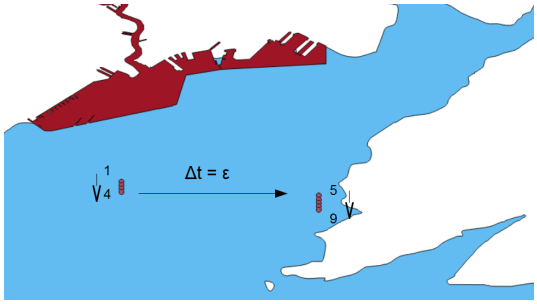

Figure 5.26: Location of points in the big spatial gap case

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_trajectory			√	√	√	√			
f_ubiquity					√				
f_coastProximity					√	√	√	√	√
f_nextPosition					√				

Table 5.11: Table of flag raising in the big spatial gap case

5.2.3.8 Case 2.4: Spontaneous unexpected appearance

Scenario 2.4 is about the spontaneous apparition of a vessel in an area in which the apparition of a vessel is of low probability (*i.e.* not in coverage area limits or in a port). Several reasons can be spotted, such as the fact to switch on the system, the presence of a ghost vessel, the modelling of the coverage area and port area, a change in the software or hardware of a reception antenna or an installation of a new antenna (Salmon et al., 2016).

In the case of the AIS switched on, we can focus on the status of the vessel (for blacklisting), and if it has a last known position which constitutes a disappearance in a low probability area. In the cases of ghost vessels, the existence of the MMSI number can be verified, and if it exists we can check if it exists somewhere else at the same time, if we

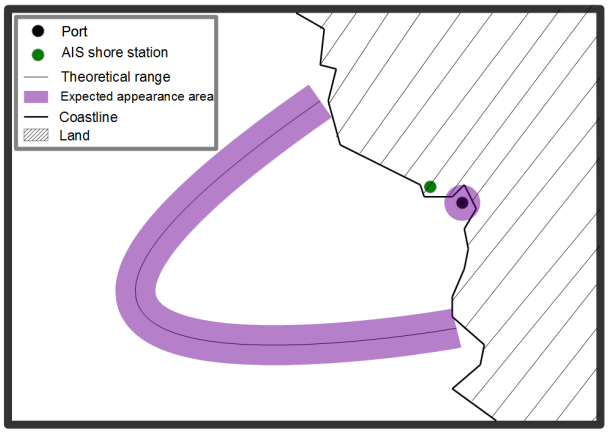

Figure 5.27: Vessel sudden appearance scenario cases

already saw it before. Several behavioural algorithms can then be applied to it, such as the fact to cross the trajectory of another vessel (interfere in the navigation), to cross the land or to have crossed over another vessel (*i.e.* the trajectories have met and such a case should have provoked a collision). It is also possible to broadcast an addressed message to the (allegedly ghost) vessel and wait for its answer (addressed inquiring messages needing acknowledgement are number 6, 10 and 12). A change in the software or the hardware of an antenna, as well as the installation of a new antenna will bring several changes such as signature changes, a great number of vessels appearing in unusual areas (as the coverage map will need to be readjusted). In addition, a bad implementation of the coverage determination algorithm will bring a distorted view of the actual coverage capabilities of antennas and will spot a great number of vessels.

Experimental Case (J-K):

This case deals with sudden apparition, and the way they are treated according to the location of such sudden apparition, as defined just before in section 5.2.3.7. The first case (Figure 5.28) shows an appearance in the middle of the Brest Bay (Blue geometry), where it should not happen, and the second case (Figure 5.29) shows an appearance at the limit of the coverage area (red geometry). As it can be expected, the first case (Table 5.12) shows a sudden appearance flag for the point number 1, and the second case (Table 5.13) shows no flag at all, as the remaining of the trajectory does not display any kinematic problem.

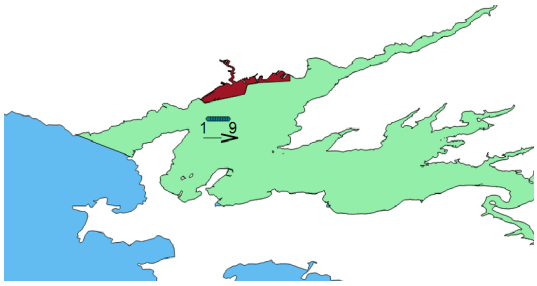

Figure 5.28: Location of points in the unexpected appearance case

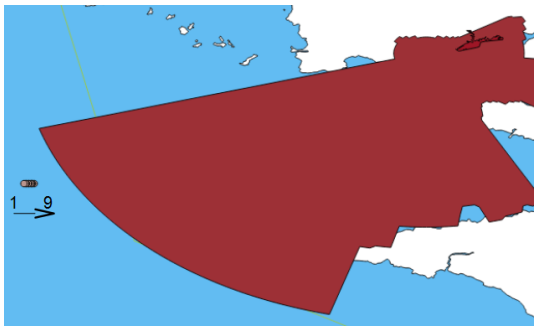

Figure 5.29: Location of points in the expected appearance case

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								

Table 5.12: Table of flag raising in the unexpected appearance case

5.2.3.9 Case 3.1: Message 22 alert

Message number 22 can be addressed to given vessels or broadcast for all vessels within a (spherical) rectangular area between longitude and latitude coordinates. It orders vessels to change their VHF transmission channel to a given channel (other than 2087 and 2088 *i.e.* 87B and 88B if they want to quit the worldwide assigned channels, or 2087 and 2088 if they want to have the vessel back in those worldwide assigned channels) and change the maritime situational picture of AIS stations. Indeed, the stations continue to emit but on another channel, and if other receptors did not take it into consideration, those stations are blind to them. Message 22 is used in some particular areas for traffic management, and broadcast by competent authorities, for its use in an usual area could be a hint of a spoofing case in order to lose the control of a proper monitoring of the system, force several vessels to disappear from and AIS point of view (such vessels could then only communicate with vessels and coastal stations using the same frequency as them). An accidental broadcast of message 22 is also possible as it was demonstrated by (USCG, 2010). The peculiarity of the use of this message encouraged us to create a dedicated flag in the flag assessment for the simple fact for this message to show up, and this flag has been called f_mess22alert.

Experimental Case (L):

This case deals with the handling of Message 22. As for now, as this message have been highlighted as rare and its use judged dangerous, every single appearance of a message number 22 will trigger an allocated flag, putting all risks to their maximum level, the handling of such a message having to become a priority for any operator. Made-up messages 22 (Figure 5.30) were created and underwent the treatment of the program, successfully displaying the flag, as shown in Table 5.14, where the two messages are named P1 and P2.

	id [PK] bigserial	receptor smallint	repeat smallint	sourcemmsi integer	spare smallint	channela smallint	channelb smallint	transmitreceivemode smallint	power boolean	longitudene real	latitudene real	longitudesw real	latitudesw real	destinationmmsi1 integer	destinationmmsi2 integer	addressed boolean	channelabw boolean	channelbbw boolean
1	220000001	1	0	2280000	0	2080	2082	1	TRUE	-5.1	49.1	-4.1	48.1	227000000	227000001	FALSE	TRUE	TRUE
2	220000002	1	0	2280000	0	2080	2082	1	TRUE	-5.1	49.1	-4.1	48.1	227000000	227000001	TRUE	TRUE	TRUE
*																		

Figure 5.30: Made-up Messages 22 in the database

	1	2	3	4	5	6	7	8	9
No Flag									

Table 5.13: Table of flag raising in the expected appearance case

	P1	P2
f_mess22alert	√	√

Table 5.14: Table of flag raising in Message 22 case

5.2.3.10 Case 3.2: Message 23 alert

Message number 23 cannot be addressed and is only broadcast to all vessels within an area, following the same pattern as message 22. This message orders vessels either to change their regular rate of communication (as defined by their speed and course, as seen in section 3.2.2.1) to a given rate of transmission, or to remain silent for a given amount of time. This order can be directed towards all vessels in the area or only to some vessels according to their type of station (Class B, Airborne station, Aid-to-navigation station for instance). Its use is reserved to competent authorities as it changes the perception of the maritime environment and can force vessel to remain permanently quiet (if sent at a sufficient rate). It is extremely rarely used, and its reception shall raise a warning on a spoofing case which would want to obstruct a proper view of the current marine traffic within an area. As for the message 23, an accidental use of this message by the authorities is still possible. The peculiarity of the use of this message encouraged us to create a dedicated flag in the flag assessment for the simple fact for this message to show up, and this flag has been called f_mess23alert.

Experimental Case (M):

This case deals with the handling of Message 23. As for now, as this message have been highlighted as rare and its use judged dangerous, every single appearance of a message number 23 will trigger an allocated flag, putting all risks to their maximum level, the handling of such a message having to become a priority for any operator. A made-up message 23 (Figure 5.31) was created and underwent the treatment of the program, successfully displaying the flag, as shown in Table 5.15, where the created message is named P1.

	id [PK] bigserial	receptor smallint	repeat smallint	sourcemmsi integer	spare text	longitudene real	latitudene real	longitudesw real	latitudesw real	stationtype smallint	shiptype smallint	transmitreceivemode smallint	reportinginterval smallint	quiettime smallint	spare2 text	ts timestamp with time zone	ts_second bigint
1	230000001	1	0	2280000		-5.1	49.1	-4.1	48.1	8	20	1	1	5			1444629600
*																	

Figure 5.31: Made-up Message 23 in the database

5.2.4 Program response

5.2.4.1 Computational time

The running time has its importance as we aim at using this program in a real-time frame. In order to assess it for a reasonable amount of time, running time for all the messages received during 30 minutes, 1, 2, 3, 6, 12 and 24 hours have been performed. The results are shown in Table 5.16.

	P1
f_mess23alert	√

Table 5.15: Table of flag raising in Message 23 case

Timespan of assessed data	30min	1h	2h	3h	6h	9h	12h	24h
Time in seconds	1800	3600	7200	10800	21600	32400	43200	86400
Running time in seconds	663	1352	2746	4154	8452	12856	17410	36375
Computing density (in %)	36.8	37.6	38.1	38.5	39.1	39.7	40.3	42.1

Table 5.16: Program running time for various timespan of AIS data

All computations have been made on a laptop running on Windows 10, Intel Core i3-5005U CPU 2 GHz with 4 Go of RAM. The results tell us that we are at an occupation rate of 40%, which means that there is still room for program features to be added. An increase in the running time rate is observed as the time span of the study gets larger. This can be explained by the increase of the tables in the database, forcing the program to query bigger tables, therefore taking more time for getting a response.

This increase in time would let us think that eventually the program will meet the 100% mark. However this mark has not been assessed, given that is it technically easy to cut an analysis into smaller successive analysis (instead of treating 30 days at once, to treat 30 1-day analyses with consecutive mutually exclusive collectively exhaustive time spans).

5.2.4.2 Flag raising rate

In this part the program response with the number of flags raised is shown for some of the scenarios. From a small sample of data, the number of each flag raised for the scenario identity (Figure 5.32), the scenarios consecutive points and temporal gap (Figure 5.33) and the scenarios whereabouts spoofing and the vessel type flags (Figure 5.34) are presented.

It can be seen that 4 vessels have consistency issues between the AIS database and the fleet register, 45 cannot be found in the register (which is not necessarily a problem, unless the fleet register is expected to be exhaustive, which is not the case for us), one has an ubiquity issue and quite a great amount (132, so 5%) have characteristics issues with the length and the width of the vessel. In most case, it is due to fields with the default value of 0 for them. No temporal gap issue have been spotted, but some trajectories are not fully trustful. Nine sudden and unexpected appearances were highlighted, and the vessel type distribution show a domination of vessels of the type "*fishing, pleasure and service*", out of which most are actually fishing vessels.

5.2.4.3 Cases of spotted integrity breaches in AIS dataset

This section shows the outcome of an analysis for four cases, namely the ubiquity, the consistency with the database, the consistency between two consecutive points and the unexpected appearance. In each case, the program line is highlighted, then the database is queried in order to get the corresponding data and the location or the value of this data is displayed in order to demonstrate that the indicated problem on the spotted message

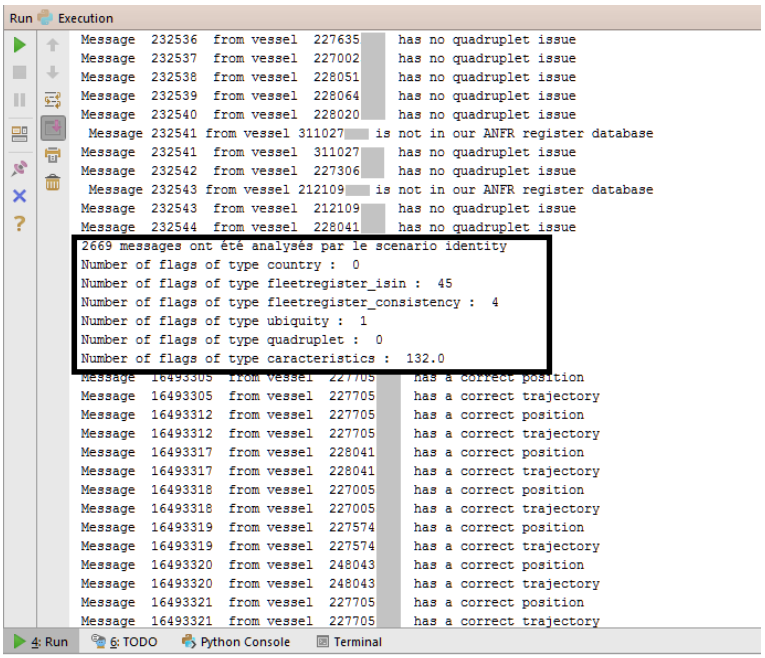

Figure 5.32: Program sum up of the identity scenario

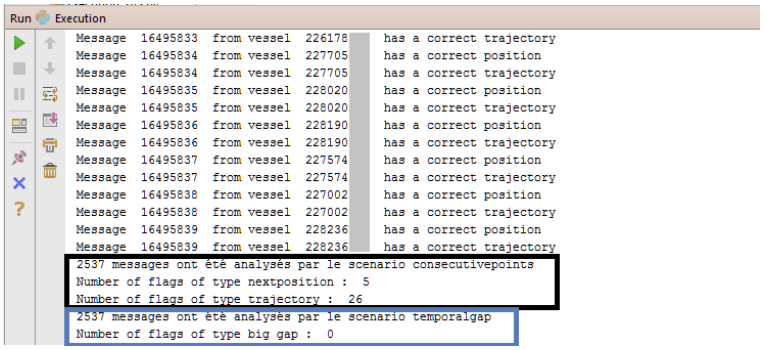

Figure 5.33: Program sum up of the scenarios of consecutive points assessment and temporal gap assessment

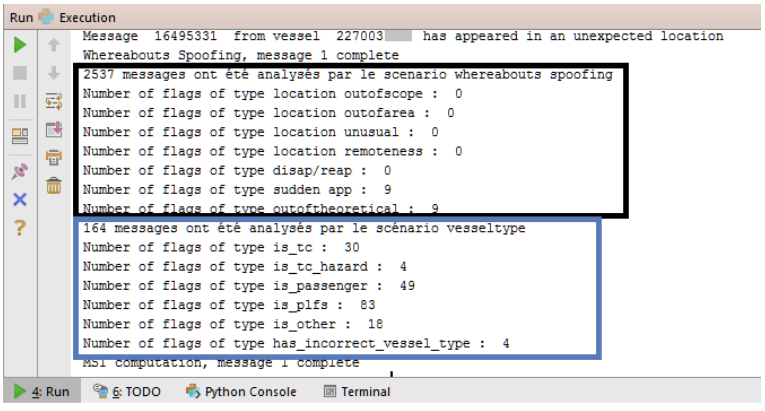

Figure 5.34: Program sum up of the whereabouts spoofing scenario and the vessel type flag assessment

actually occurred.

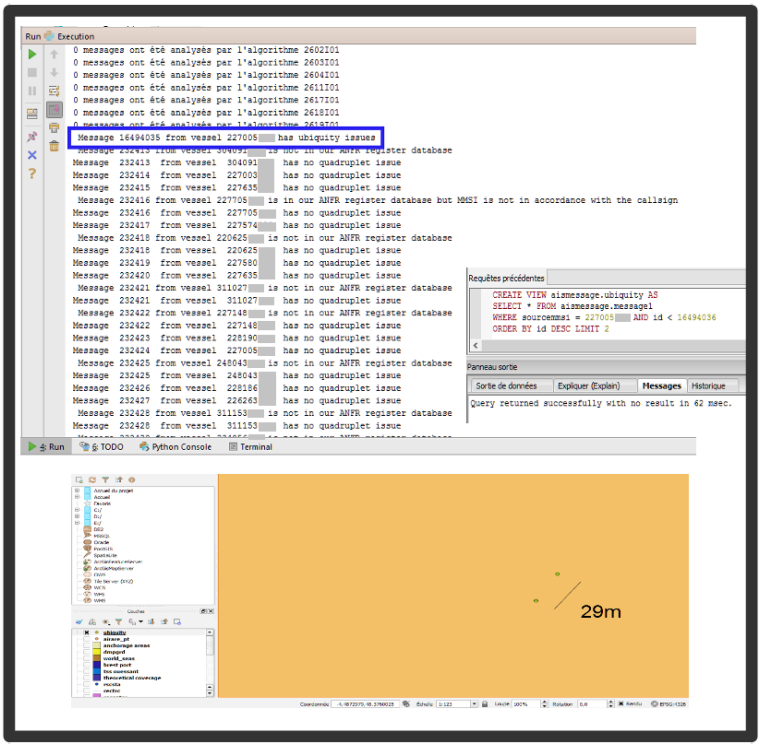

Figure 5.35: Verification of an ubiquity case

Ubiquity Case

In the ubiquity case, it was necessary to query the message in question and the last message sent from the same vessel. It was shown that their time difference was 0 seconds and their position difference was 29 meters, as shown in Figure 5.35. Whereas it is supposed to be a unwanted and accidental glitch, it remains a positioning issue as a vessel is not expected to move this much in less than one full second.

Fleet Register Consistency Case

In this case, as shown in Figure 5.36, two queries were performed, one on the AIS database and one on the fleet register, showing that a same call sign was associated with two distinct MMSI numbers.

Position with respect to kinematic values case

The Figure 5.37 proposes the case of two messages for which the spatial position are not compatible with the kinematic values, as output of the item "**01I05**" presented in section 4.1.3.2. The two positions are queried, as well as the course over ground, speed over ground, rate of turn and the timestamps. Then the expected position is computed, as well as an error buffer. In this case, the value of the second point is outside the buffer, triggering the alert

Unexpected appearance

This last case we present deals with unexpected appearance of vessels, *i.e.* as presented before the fact for a vessel to appear for the first time in a location that would not have been expected for such a first appearance. The geometry of the bay of Brest to which is

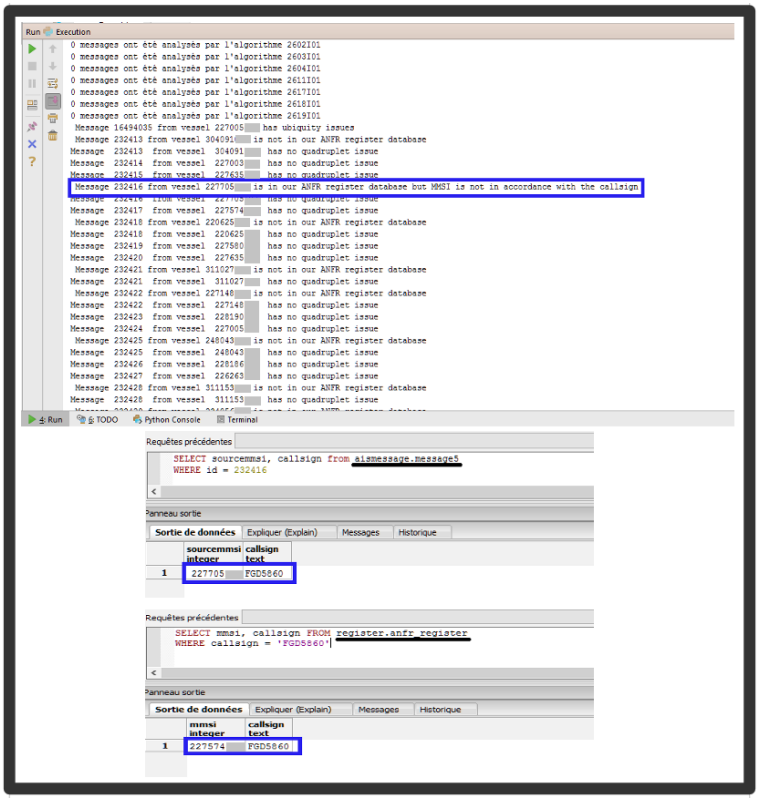

Figure 5.36: Verification of a fleet register consistency case

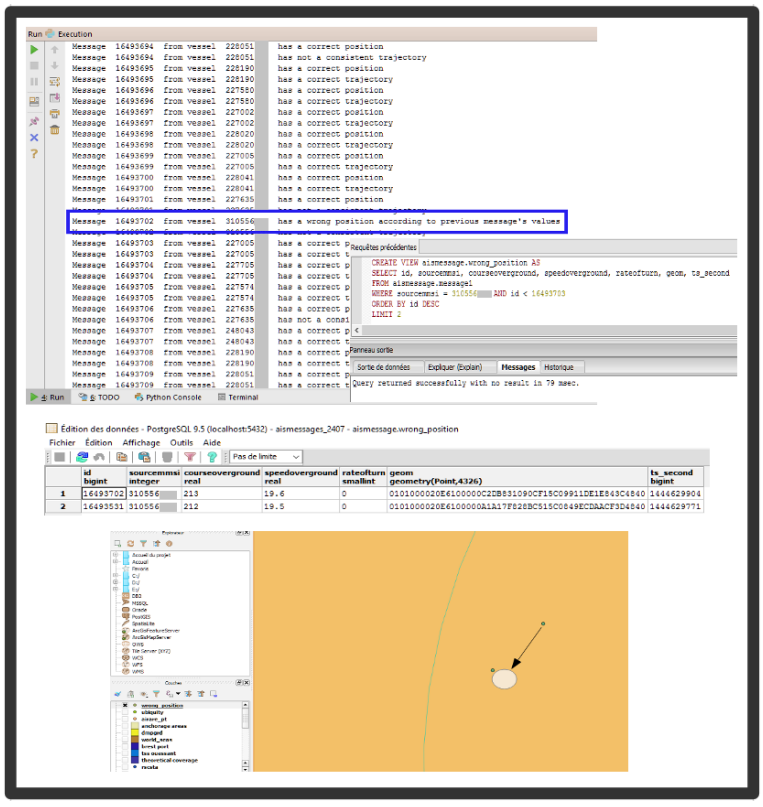

Figure 5.37: Verification of a spatio-temporal position case

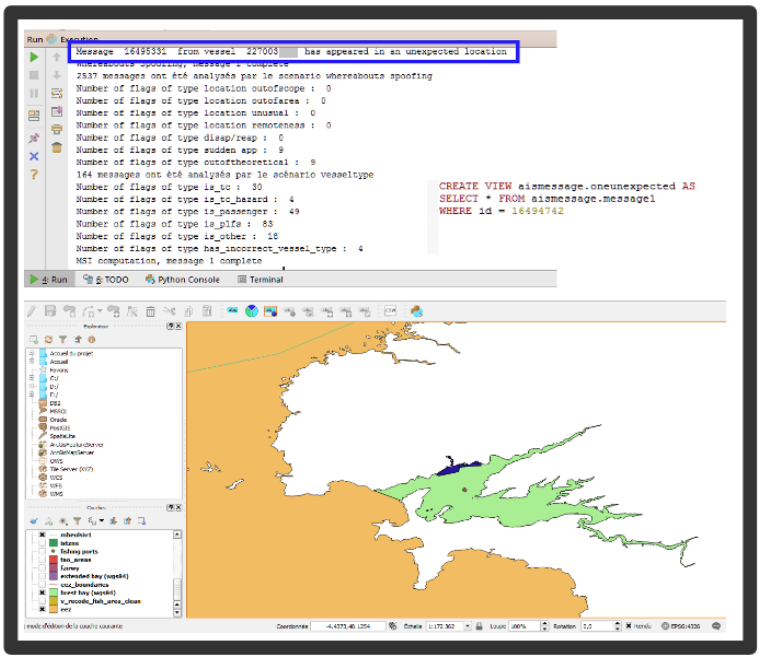

Figure 5.38: Verification of the case of an unexpected appearance

cut off the geometry of the Brest port is considered as an anomalous place for a vessel appearance, as the vessel is either expected to appear outside the bay entrance or in the port itself. The location of the given point is queried and displayed in the map, showing that the position is effectively an unexpected place for its appearance. The program output, the SQL query and the map in question are presented in Figure 5.38.

5.2.5 Discussion

The information system that was set enables the treatment of AIS messages on-the-fly, as the running time of the program for k seconds of data is inferior to k seconds (by far, which means that more treatments can easily be added), and it was tested on both real AIS data and created AIS data for scenario modelling.

This system is based on a methodology presented in chapter 4, consisting of an integrity assessment of AIS data and an associated risk assessment (which will be the subject of the chapter 6). The program is based on integrity in order to discover issues in AIS data demonstrating a data handling error, falsification or spoofing. The item lists have been developed with the system specifications, using system settings, as well as field comparison based on physics and coherence, with the help of maritime domain experts for the definition of thresholds. Those items have been developed independently from the scenario cases that emerged later in order to have data to formerly assess the system without requiring real data for some cases for which such data is either not available or nowhere to be found.

Another layer of this study is about the risk level determination, also in this case expert knowledge have been used for vessel segmentation and risk level assignment.

As the program was running on data, it successfully pointed out the cases in which

further investigation is needed, on real data with the massive treatment of AIS messages and on data built on purpose, for which the system based on integrity assessment of messages displayed expected flags in the selected cases. In this scope, the first two hypotheses presented in section 1.2 can be validated by our experimental approach.

Conclusion

This chapter showed the application of the methodology to AIS messages and more particularly to the dataset available and some made-up AIS messages through scenario assessments that led to the raising of the proper flags, the triggering of the associated risks. The architecture of a Python software querying and filling in a postgres/postgis relational database in the several steps that are item assessment and scenario assessment was shown to be efficient as it successfully triggered the flags and risks in relation with the expected outcome, given the input data and given that the program was developed independently from the application scenarios. Still, this program constitutes a proof of concept for AIS data falsification discovery and the raising of situational flags, and must be adapted and refined to become an operational tool for maritime surveillance for competent authorities, and some other features might be added in this respect, particularly the risk and the risk level assessment, which will be the topic of the next chapter.

Chapter 6

From flags to risk assessment

Chapitre 6 : Vers une méthode d'évaluation des risques basée sur les fanions

Les risques maritimes sont variés et peuvent être classés en quatre grandes familles : naturels, anthropiques, environnementaux ou maritimes. Les risques naturels peuvent être prévisibles telles les tempêtes ou imprévisibles tels que les raz-de-marée de les collisions avec des cétacés. Les risques anthropiques sont liés à l'humain, notamment le fait qu'il existe beaucoup de navires sous pavillon de complaisance, ou l'existence de munitions immergées. Les risques environnementaux regroupent tous les types de maladies liées à la navigation et au fait d'être loin de la terre dans un environnement clos et isolé. Les marées noires font également partie des risques environnementaux de la navigation maritime. Enfin, les risques dits maritimes sont directement liés à la présence d'autres navires, telles que les collisions ou le risque terroriste.

Dans le cadre de notre étude, cinq familles de risques principales ont été retenues, du fait de leur adéquation avec les problématiques liées à l'AIS : le risque de collision et d'abordage, le risque d'échouement, le risque de pêche illégale, le risque de piraterie et de terrorisme, et enfin le risque de transport illégal de biens ou de personnes.

Dans l'objectif de lier les familles de risques qui ont été déterminées aux processus de découverte de la falsification de l'AIS, l'établissement de typologies décrivant l'environnement du trafic maritime et un cadre ontologique liant les enjeux, les acteurs, les anomalies et l'environnement maritime en général est nécessaire. Ainsi, une typologie a été effectuée pour chacun des domaines permettant la description de la situation maritime telle que nous la désirons. Une typologie des anomalies (qu'elles soient de comportement, de contexte, légales ou de qualité), une typologie des navires, une typologie des comportements à risque, une typologie des environnements (zones régulées et conditions de navigation), une typologie des enjeux et une typologie des acteurs sont proposées, complétées par une typologie des modèles de mouvement. Avec l'aide du logiciel Protégé, une architecture ontologique a été proposée afin de lier les typologies et bâtir les bases d'un possible futur moteur d'inférence.

Afin de lier les fanions issus de l'analyse des messages AIS aux risques, il est nécessaire

d'effectuer une analyse de risques sur la base des fanions, considérés seuls ou en groupe. Ainsi, une liste de scénarios d'activation de fanions a été mise en place, chacun de ces scénarios consistant, pour un message, à voir un ou plusieurs fanions s'activer. A chaque scénario sont associé un ou plusieurs risques présents dans la liste des cinq familles de risques retenues, et quand tous les fanions d'un scénario sont activés, le scénario est considéré réalisé et tous les risques afférents sont activés, leur niveau de risque étant évalué plus tard. Si plusieurs scénarios sont activés, leurs risques associés sont aggrégés. Une table de relation de type déterministe est nécessaire pour cette étude.

Afin de déterminer le niveau de risques, plusieurs éléments ont dû être pris en compte : le type du navire, les dimensions du risque et le niveau de risque. Les types de navire considérés sont : les navires de charge, les navires de charge transportant des matières dangereuses, les navires de passagers et les navires de plaisance, pêche ou service. Les dimensions du risque prises en compte sont les dimensions humaines (risques liés à la vie humaine en mer), liés aux infrastructures (navires, plate-formes, ports) et environnementales. Les niveaux de risques sont au nombre de quatre : risque mineur, risque modéré, risque majeur, risque extrême. Ainsi, pour chacune des familles de risques, une table a été définie donnant le niveau de risque par rapport à la dimension considérée et au type du navire en question. L'étude des fanions nous a fourni une liste de risques à évaluer, et cette évaluation est effectuée avec ces tables, en prenant en considération les éléments sus-nommés.

La principale limite de cette évaluation du risque est le caractère déterministe de l'étude. En effet, une approche déterministe a été préférée à une approche probabiliste pour son adéquation avec une preuve de concept et sa complexité relative de mise en œuvre au regard du temps disponible avant la fin du projet ANR au sein duquel cette thèse est incluse. Cette approche, bien qu'imparfaite, permet néanmoins la détection de risques et l'assignation de niveaux de risque, suivant strictement un ensemble de règles considérées comme étant de la connaissance d'experts. Cependant cette approche ne permet pas de gérer le flou, qui est un facteur important de l'analyse de risques. Un moteur d'inférence pourrait orienter cette étude vers une approche statistique, en prenant en considération les liens déjà effectués entre les typologies.

Introduction

This chapter focuses on the risks of maritime navigation which are assessed in this study. The various flags, representing explicit issues about AIS, can then trigger scenarios and associated risks if a given combination of flags is raised. Then, according to the risk in question and according to vessel types, a risk level is assigned to each of the human, infrastructural and environmental dimensions of the study, to be delivered and presented properly to the rightful competent authorities.

In this chapter are first presented some risks of maritime navigation and more particularly those chosen in our study. Then the various maritime domain typologies that have been constructed in order to build an ontology are presented. In the following section is presented the deterministic link between the various flags assessed previously in the analysis and presented in section 4.2. The risk level assignment method is explained before

the exemplification with the cases of section 5.2.3 and a special case made to show the differences of risk levels according to the vessel type. Then, the way the risk is assessed in the program is shown before a presentation of the limitations of our approach.

6.1 The risks of maritime navigation

6.1.1 Overview

At sea, people are exposed to several kinds of risks, some of them are considered here, namely the natural, anthropic, environmental and maritime ones.

Natural risks include storms, that endanger mariners at sea, workers on shores and harbour infrastructures. As some of them are predicable, thanks to weather forecast for instance, others are unpredictable, such as tidal waves or a collision with a cetacean.

Anthropic risks include risks related to submerged mines and munitions, which are a direct threat to fishermen and the environment, and an indirect threat to the 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 (scurvy) 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 on shore. The breadth of oil slicks is reducing for the fifty last years. Today, it is about 3 Mt per year. Notable oil slicks involve *Amoco Cadiz*, *Exxon Valdez*, *Erika* ships and *Deepwater Horizon* platform.

Maritime risks are linked to the use of ships by humans. Collisions and boarding are maritime risks, as they can be caused by carelessness, priority denial or bad visibility when two vessels have secant trajectories. Another risk for a ship is to run aground, and can be a result of bad manoeuvres, an erroneous estimation of the water depth or a bad or not up-to-date documentation. Other risks are fires, waterways or terrorism.

The vulnerabilities are thus numerous, for instance for energy transportation, as it has a geostrategic importance, it is particularly delicate and a particular care should be taken to it, as some countries vitally require their energy income to be sufficient. All transportation by the means of boats implies the risks associated with the goods transportation. Moreover, some energy transportation is done via lines (between countries, or between offshore platforms and the shore), laying themselves open to sabotage. Offshore platforms themselves are vulnerable to pirate attacks because of their immobility and isolation. Some ships such as freighters are subject to thefts, and all the ships are subject to pirate attacks, for ransom of the crew and of the vessel itself. The vulnerability is increased with the transportation of hazardous goods in fragile environment. The vulnerability of the global maritime traffic is particularly important in strategic points such as straits or canals, or offshore weak states (piracy). One of the purposes of international

cooperation is to reduce the danger linked to those vulnerabilities.

In our study, it was decided to concentrate around five main risk families, namely collision and boarding, grounding, illegal fishing, piracy and terrorism, and illegal transportation, all of them presented in the remaining of this section and in Figure 6.1.

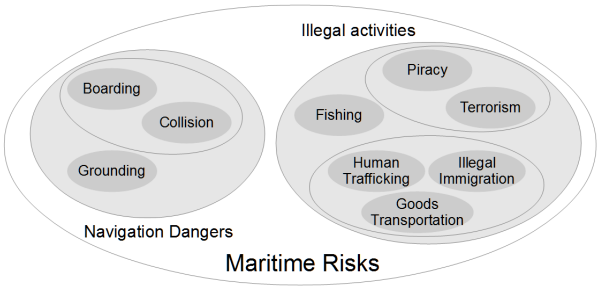

Figure 6.1: An overview of the studied maritime risks

This list is not exhaustive, as other risks do exist while at sea (such as illnesses that can endanger people and bring diseases to new places). The choice was made to select only the risks that could reasonably be spotted out by the study of AIS messages, as they can be susceptible to be triggered by an error or a falsification of the AIS.

6.1.2 Collision and boarding

The boarding is the fact for two vessels to enter in physical contact, voluntarily or not. As the repartition of vessels is uneven throughout the globe, boardings are more likely to happen in crowded regions of the sea. Accidental boarding occurs when two vessels having crossing trajectories cannot change their course quickly enough to prevent the boarding to happen. In order to prevent boarding to happen, COLREGS (IMO, 2009) (or International Regulations for Preventing Collisions at Sea) have been written.

A collision is the fact for a vessel to enter in physical contact with a fixed body such as in a port or with an off-shore infrastructure.

Figure 6.2: A vessel after a collision, from (The Maritime Executive, 2012a)

6.1.3 Grounding

The grounding is, for a vessel, the fact to meet the shore and to lie on it, while sailing in a too close proximity to the shore, such as there is no enough clearance behind the vessel to that it can rely on water. Groundings can be voluntary or not, and can be dangerous as they can lead in casualties.

Figure 6.3: Costa Concordia grounding disaster, from (The Telegraph, 2012)

6.1.4 Illegal fishing

Overfishing occurs when the amount of fish taken from the ocean is more important than the reproduction ability of the species. It has serious consequences as it impacts both the oceanic life balance and the economy of coastal communities. Today about 85% percent of all fisheries are at or beyond their biological limits and some species like Albacore and Bluefin tuna are particularly exposed to overfishing. The open access nature of the fishing areas is one of the problems, alongside with the poor fisheries management, particularly in developing countries that cannot ensure the enforcement of international laws. Moreover illegal fishing is rampant, accounting for a global estimated figure of 20%, going up to 50% in some fisheries.

In order to prevent overfishing, laws sometimes limit the amount and the size of the fish, as well as the location of the catches. Fishing laws are done at the national level, with the addition of some international conventions and agreements.

6.1.5 Piracy and terrorism

Defined in the Convention on the High Seas (United Nations, 1958) as "*any illegal acts of violence, detention or any act of depredation, committed for private ends by the crew or the passengers of a private ship*", piracy has always existed at sea. The purpose is mainly pecuniary, and marginally politic. Some pirate crews are trained on shore, with a strong hierarchy and the involvement of local dignitaries, while others are completely disorganised. The states deployed an important effort, and the number of attacks is currently decreasing, especially in the Horn of Africa. For the year 2013, only five countries observed more than 10 attacks in their neighbourhood: Indonesia (106), Nigeria (31), Somalia (15), India (14) and Bangladesh (12).

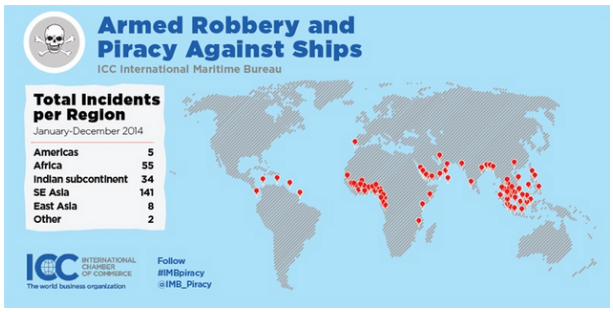

Figure 6.4: Map of 2014 maritime piracy attacks, from (The Maritime Executive, 2015)

Although maritime terrorism has not been demonstrated as of 2017, the fact to use a vessel as a weapon against other vessels, ports, coastal facilities and off-shore infrastructure must be taken into consideration. Terrorism coming from inside the vessel, outside the vessel or via electronic networks (cyberterrorism) is considered in our study as being a rising threat.

6.1.6 Illegal transportation

Illegal transportation is about the illegal transportation of goods (smuggling) and the illegal transportation of human beings, either voluntarily (human trafficking) or not (illegal immigration).

Smuggling consists of the illegal trade of goods, which can be legal goods hidden for tax purposes or illegal goods such as counterfeited goods, cigarettes or narcotics, as defined in the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UNODC, 1988). The drug traffic generated over 320 milliards of US Dollars as of 2003 (UNODC, 2005), and the counterfeited goods activities generate over 250 milliards of US Dollars per year (UNODC, 2013), mainly dominated by clothing goods, but also involving car parts, chemicals, electronics, food, drinks, pharmaceuticals, household products and tobacco.

Illegal immigration and human trafficking is the fact to have on-board people who are willing to reach illegally the territory of a foreign nation. It is a current problem (as the migrant crisis is ongoing as of 2017, with over 360,000 illegal migrants arriving in the EU soil for the 2016 year (IOM, 2017), and an expected 200 million to 1,000 million people who could potentially try to escape by vessel the impacts of climate change (Nepal, 2014) in the 2015-2055 period.

6.2 Domain typologies

In order to link the risks families that have been selected to the process of discovery of AIS falsification, the establishment of typologies describing the environment of marine traffic and an ontological frame linking the stakes, the actors, the anomalies and the maritime environment is necessary. This section presents the various typologies that have been set

(Iphar, Aldo Napoli, Ray, et al., 2016).

6.2.1 Typology of anomalies

Anomalies are not all the same of a kind, their spectrum is wide and a classification in families and subfamilies is not trivial. In the scope of the study of AIS messages and according to the research presented in (Roy and Davenport, 2010) and (Roy, 2008), a classification in four main families has been chosen: the behaviour, the content, the lawfulness and the quality, as presented in Figure 6.5.

By its size, the behavioural anomalies family is the largest. Kinematic anomalies are the main sub-family, with on the one hand the position-based (about either the destination or the area of location) and on the other hand the movement-based (about either the route or the speed, with or without engine on) anomalies. The other subfamily is route-based anomalies, including unexpected change of destination, illogical or non-understandable behaviour.

As for the content anomalies, two subfamilies are distinguishable: the anomalies in the content of the message itself that do not come under the vessel's behaviour (such as static data, data which usually do not change over time) and anomalies about the people on board (crew or passengers). As for static information, are concerned the cargo (if it does not match with the vessel type, or if two cargoes that are hazardous together are nearby), the dimensions of the vessel (for instance when the declared width is higher than the declared length, or with a draught incompatible with the vessel type) or the vessel type (incompatibility with the declared activity or the dimensions of the vessel). As for the people on board, the crew (for issues such as the number too high or too few, the fact to belong to any criminal or terrorist organisation) and the passengers (the number on board, the fact to be an illegal immigrant or to be a hazardous person) are distinguished.

The lawfulness anomalies can be split in two sub-families: criminal issues (terrorism or organised crime) and breach-level issues, such as undeclared change of flag, undeclared change of owner or an unauthorised seafaring behaviour (navigation in a forbidden area, navigation in an area where restrictions of navigation are in force, or a forbidden behaviour such as the failure to respect the right navigation direction in a TSS).

About data quality anomalies are distinguished the unexpectedly changing data (of static information for instance), the impossible data so as the piece of information is out of the possible scope for it, or impossible with respect to others pieces of information (when a comparison is possible), and missing data due to poor signal reception or voluntary lack of data providing.

6.2.2 Typology of vessels

The typology of vessels is presented in Figure 6.6. In the frame of the studies on the AIS, a typology of vessels based on the classes of messages sent is possible. Two families of vessels are then distinguishable: the ones for which the use of the system is compulsory and which are equipped with a class A transceiver, and the ones for which the use of

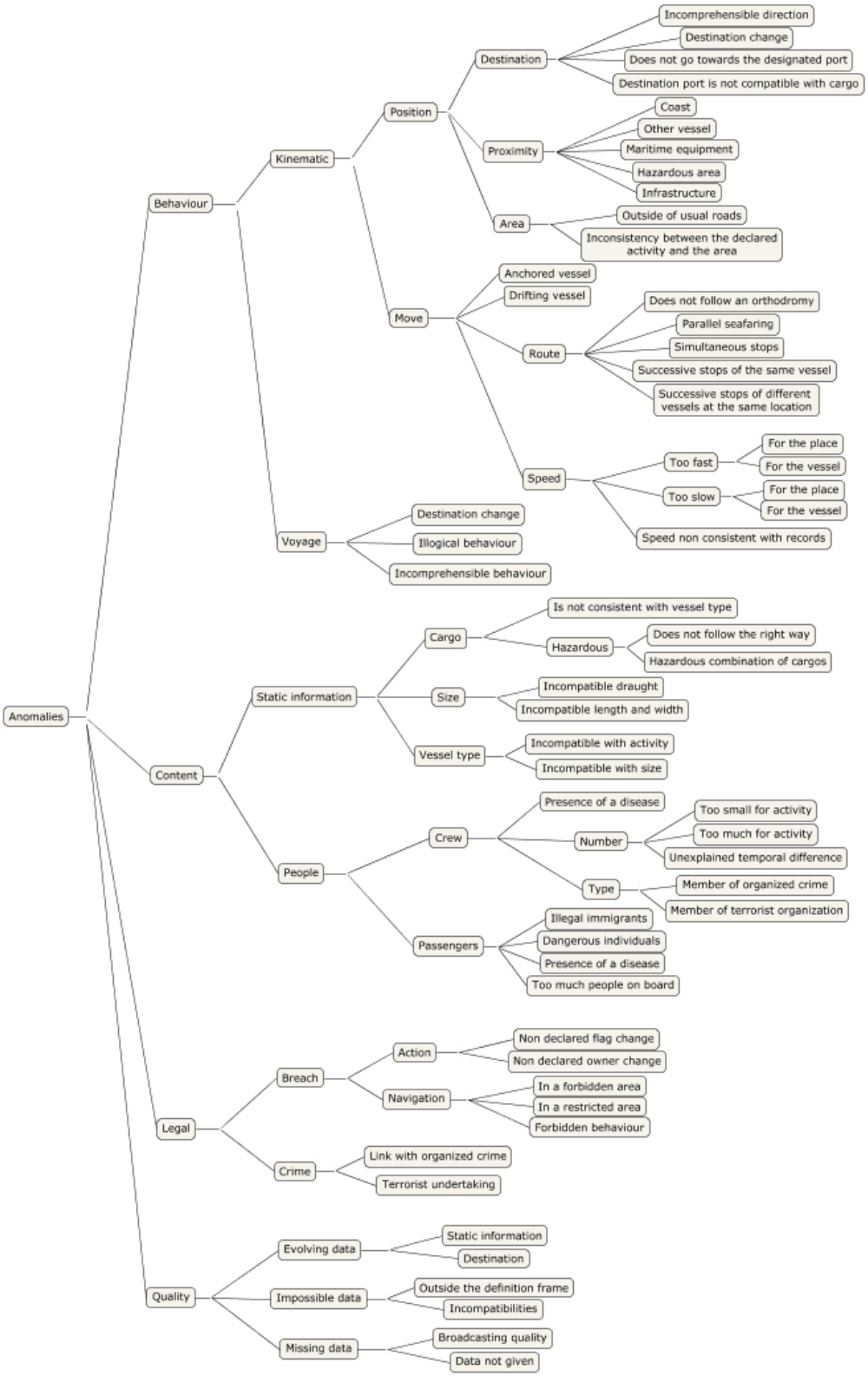

Figure 6.5: Typology of anomalies

the system is not an obligation and which can be equipped with a class B transceiver, as presented in section 3.2.1. Thus when a vessel enters in the first category it emits as a class A vessel, and when it enters in the second category, it emits as a class B vessel if it is equipped with the system or it does not emit any message.

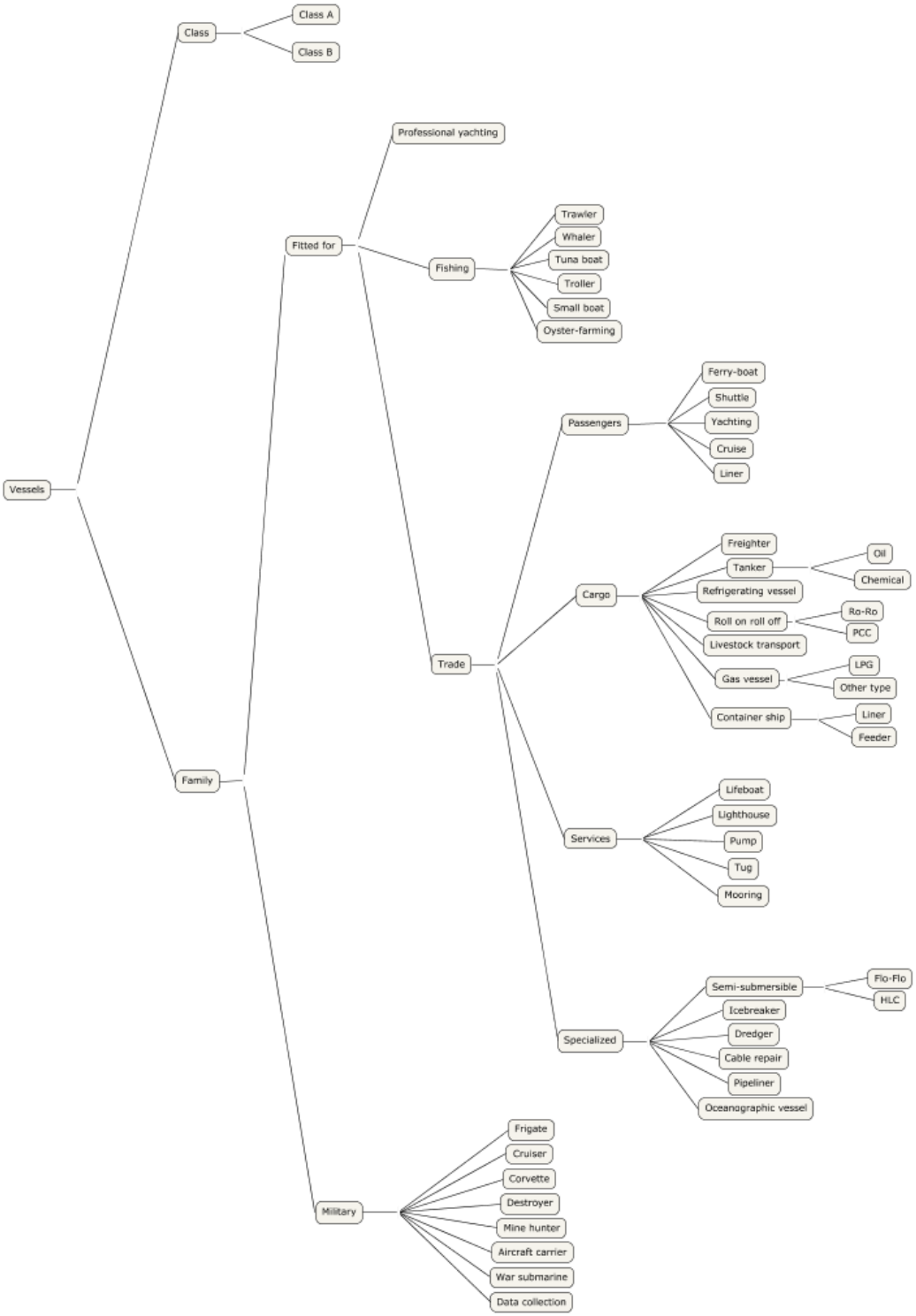

Figure 6.6: Typology of vessels

The diversity of navigating vessels enables us to build a typology of them according to the domain it is fitted for and their applicative domain. Apart from the military vessels, a vessel can be fitted for trade, for fishing or for professional yachting. In the first category (trade-fitted vessels), several families of vessels are possible, such as passengers, cargoes, service or specialised vessels.

6.2.3 Typology of hazardous behaviours

Hazardous behaviours, as presented in Figure 6.7, are of various kinds and can cover collision or boarding, as well as a falsification dimension such as the fact to cut the telecommunication channel, to falsify navigation data by the modification of messages or the input of wrong information of some data fields (including leaving blank fields on purpose). In general, each infringement of the maritime code is a hazardous behaviour, this can be related to the speed, the heading, the respect of navigation areas, the respect of rules in force for the protection of environment or the respect of helm rules. In this typology, the behaviours purely linked to navigation are separated from those linked to the system (including the errors and the falsifications).

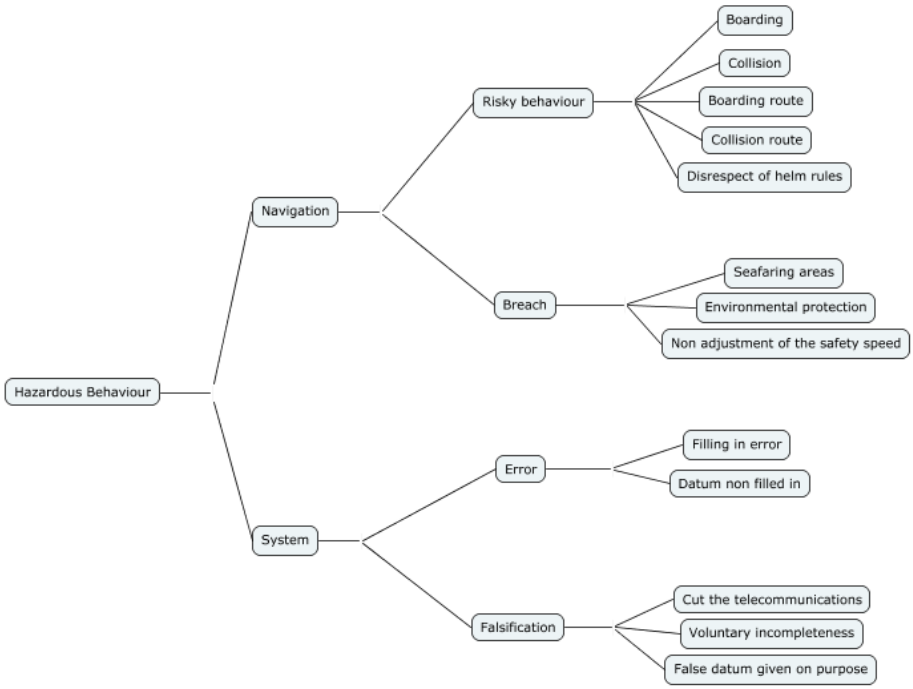

Figure 6.7: Typology of hazardous behaviours

6.2.4 Typology of environments

The environment can be assessed in different ways: one can be interested by the location in or out of the regulated areas, by the meteorology and the diversity of the states of the sea or by the oceanography in the case of a bathymetric study.

The two typologies relevant to this field are presented in Figure 6.8 for the regulated areas and in Figure 6.9 for the conditions of navigation.

Regulated areas are of several kinds: linked to the sovereignty of the states, to the security or to the safeguarding of the environment. Sovereignty areas are presented in the Introduction. Beyond the EEZ are the international waters, out of jurisdiction from

any coastal state. Regulated areas linked to the security can be anchorage areas, TSS or navigation channels, storage areas, moistening areas or military zones, amongst others. Limits that can be found in maritime maps (SHOM, 2016) show a wide spectrum of kinds of limits, highlighting their diversity. Regulated areas linked to the environment safeguarding include the protected marine areas or areas where fishing or underwater hunting are forbidden or restricted.

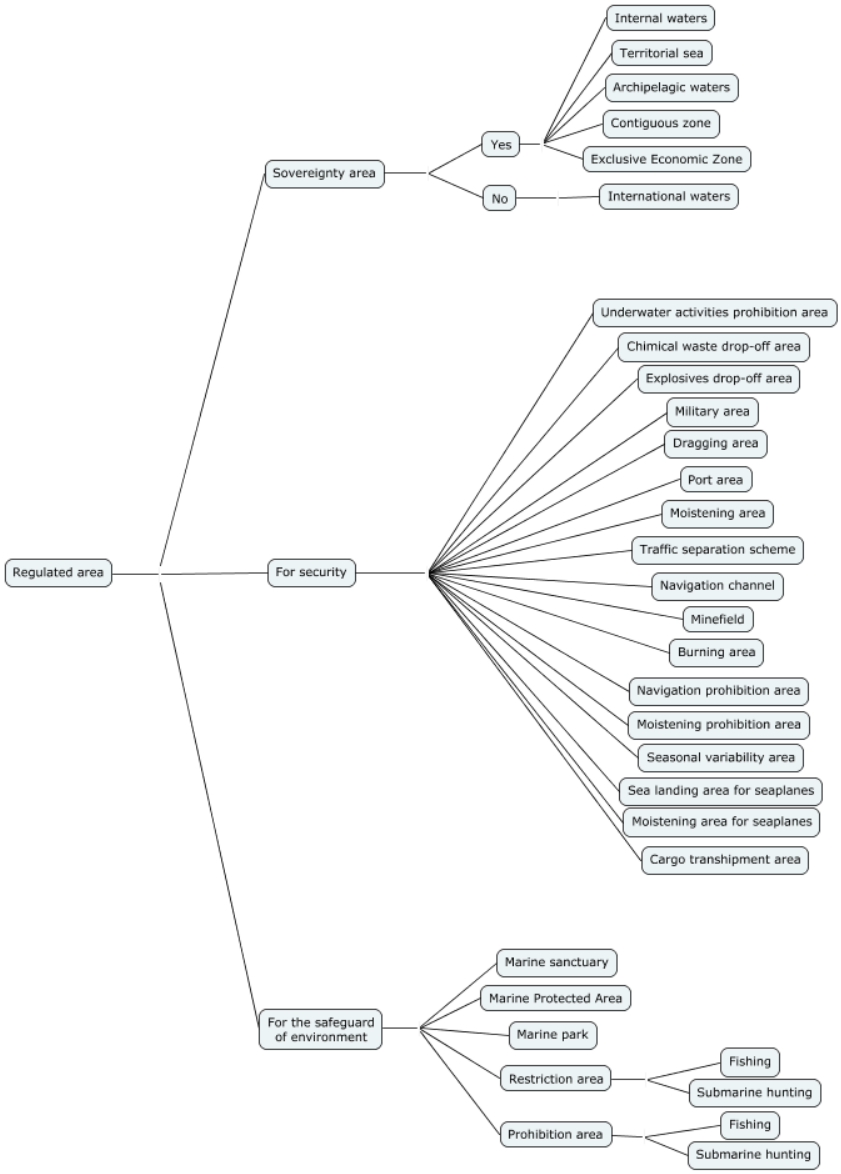

Figure 6.8: Typology of regulated areas

The state of the sea is characterised by the conditions of navigation that include the fact to navigate during the day or during the night, the visibility, the weather and the height of the waves such as on the Douglas sea scale with 10 degrees: from 0 to 9 going from calm to phenomenal. The discipline of oceanography that is interesting in the frame of this study is bathymetry, with the local depth of the seabed that enables a vessel knowing its draught to know if it can navigate. As the tidal phenomenon is observed and quantified, the navigation on foreshore, the under keel clearance and the fact for a vessel

to be hampered by its draught, which happens when the under keel clearance is poor.

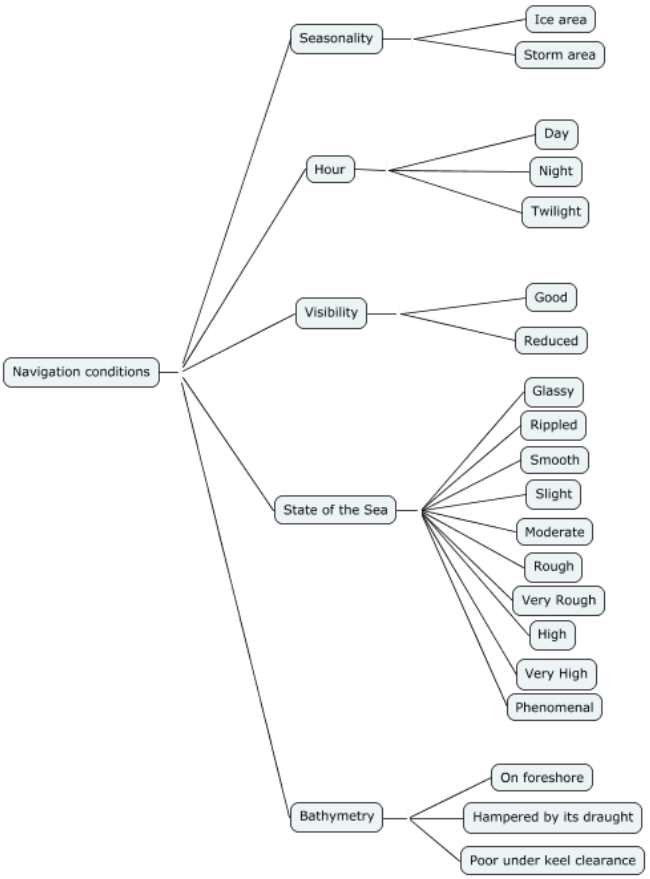

Figure 6.9: Typology of navigation conditions

6.2.5 Typology of stakes

The stakes on the subject of navigation and its safety are numerous, and can be divided in three main families: the human, the material and the environmental stakes. The human stakes are related to the crew and the passengers of the vessels, whereas the material ones concentrate on the structure of the vessel, their cargoes and the infrastructure, coastal and off-shore. Environmental stakes form around the protection of the wildlife, of the protected marine areas, of coasts and of the seabed to diverse kinds of pollution. A typology of those stakes in presented in Figure 6.10.

6.2.6 Typology of actors

Besides the humans actors present on board such as the crew and the passengers, the actors of the maritime world are also the companies for which the activity is linked to the sea by their action (fishing), their goal (merchant navy) or their nature (ship-owners). Moreover, ports as entities are actors, so are the states through their navy for the military

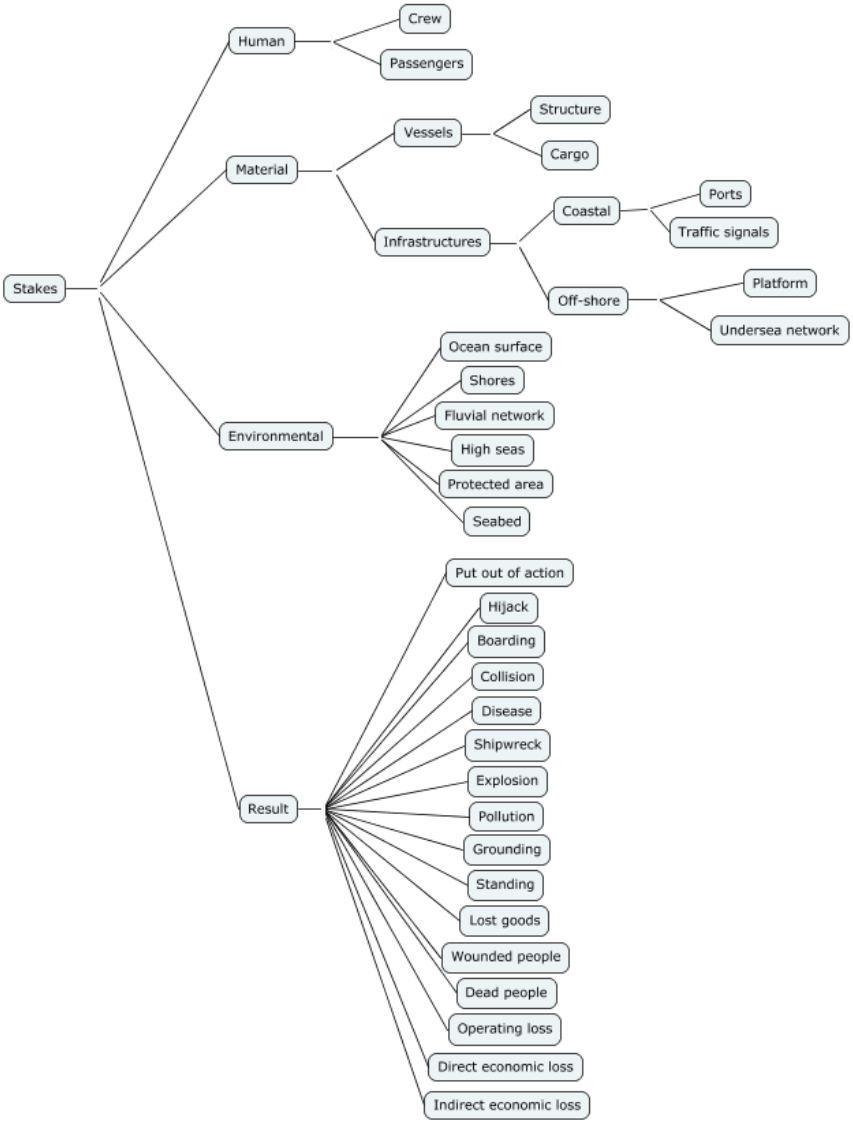

Figure 6.10: Typology of stakes

side or through their action for their civil side. In France, the action of the state at sea gathers all the civil actions that take place at sea and that come within the competency of the state. It is coordinated by several ministries and several public administrations. Alerts are triggered by the state towards the actors of the sea, aiming for the protection of people and goods. A typology of such actors is displayed in Figure 6.11.

6.2.7 Typology of motion models

In the motion models, presented in typology in Figure 6.12, are distinguished the generic models and the behaviour models according to the categorisation proposed by (Dodge et al., 2008). Behaviours models include the prevention, the pursuit, the migration or the fixation, amongst others. The generic models are themselves divided in composed spatio-temporal models such as isolation, symmetry, repetition, convergence, separation or meet-

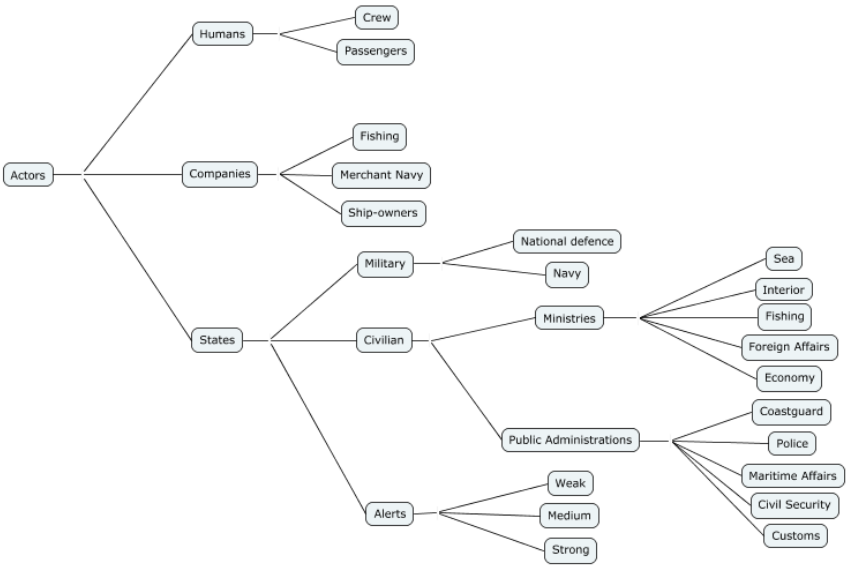

Figure 6.11: Typology of actors

ing for instance, whereas primitive models are divided into spatial, spatio-temporal and temporal models. Spatial primitive models include concentration or collocations, spatio-temporal primitive models classify the consistency, sequences, periodicities and incidents (simultaneity for instance). Eventually, temporal primitive models classify sequences, periodicities, temporal relations and total or partial synchronisations.

6.3 Domain ontologies

Once all the typologies have been set, the ontological frame enables the creation of links between the different typologies. Our ontology has been made in order to demonstrate the relationships between the various elements of the typologies, in a spirit of representation, and not in a spirit of interrogation as our ontology is not usable yet as an inference engine.

6.3.1 The Protégé software

The ontology software Protégé is one of the most renowned of its kind. Its development began in 1995 in the Californian University of Stanford. Since its fourth version, Protégé is based on the open source programming interface OWL API and is widely used, in the scientific community as well as in the developer community. The version used for ontology creation in our case, presented in section 6.3.2, is the 5.0 version.

6.3.2 Ontology architecture

As presented in Figure 6.13, the ontology is structured around three main classes: Vessel, Behaviour and Messages, the vessel having behaviour and sending messages. Eleven

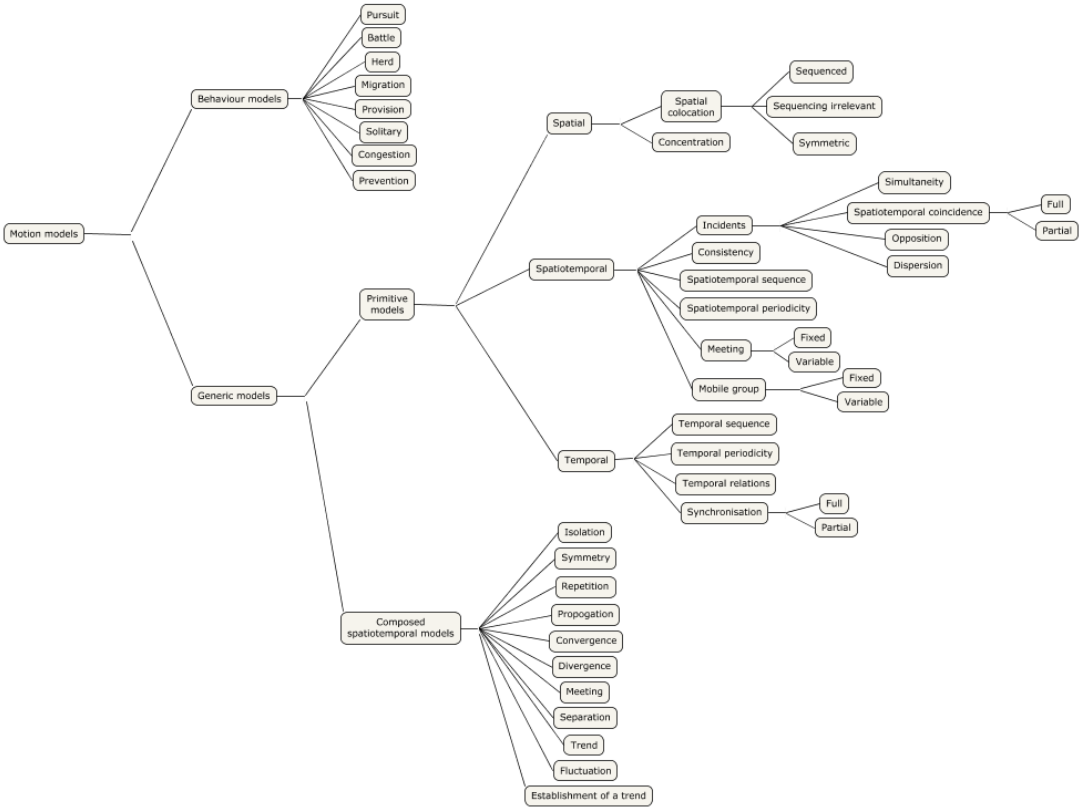

Figure 6.12: Typology of motion models

classes are directly associated with those three main classes: actors, vessels, stakes, content anomalies, quality anomalies, navigation conditions, motion models, regulated areas, hazardous behaviours, behavioural anomalies and legal anomalies. The vessel involves actors, has a particular type, with its own stakes. Messages are subject to content and quality anomalies. The behaviour of the vessel is subject to behavioural and legal anomalies, can produce risks, is regulated by areas, follows motion models and depends on navigation conditions. Those fourteen classes are presented in the ontological diagram presented below. Moreover, in each class are implemented sub-classes in order to refine the concepts. Those sub-classes are often divided in additional sub-classes so as to have the more refined description possible, according to the principles of ontology creation. From the first eleven classes, the total number of sub-classes in our ontology is over three hundred.

Moreover, in the Protégé interface, it is possible to watch the classes and sub-classes tree view. In Figure 6.14 the main classes and the relations that link them in a non-developed case.

In Figure 6.15, the classes Vessel and Regulated areas are developed and presented by tree view in the left-hand side of the image and in a graphic way in the right-hand side of the image, with the use of the Ontograf add-on, that enables the visualisation of the relations between classes.

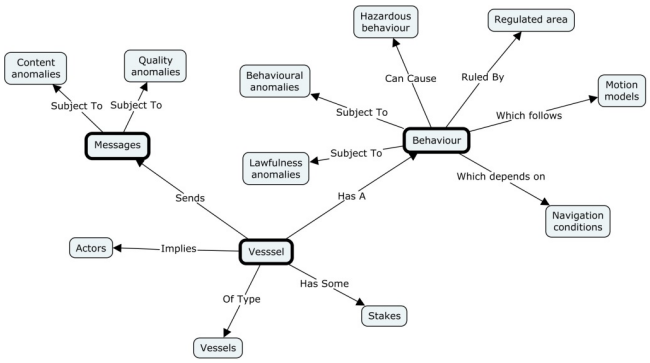

Figure 6.13: Ontological Diagram

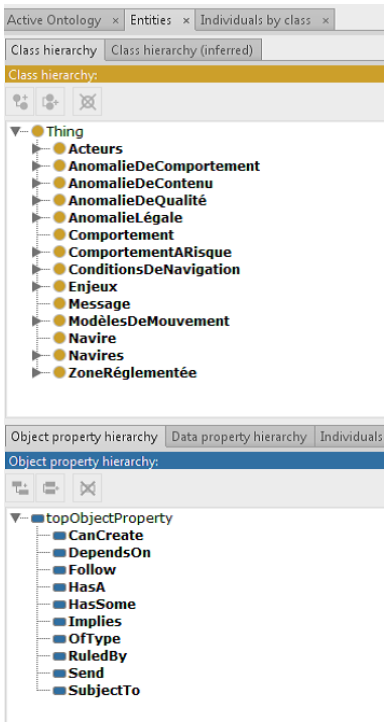

Figure 6.14: Ontological Architecture

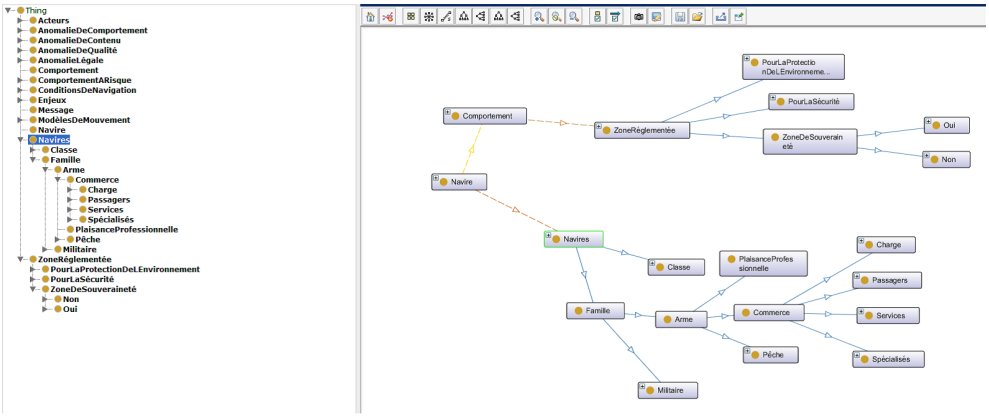

Figure 6.15: Class development in the Protégé Software

6.4 From the flags to the risk determination

A link between the flags and the risks must be set in order to link the facts that came out of the flag analysis, taking into account both system and non-system data. Indeed, it is necessary to link the outcome of the flag analysis and turn it into a risk assessment.

First, it is necessary to set a list of risks taken into consideration. This is done in order to restrict the risk study to the risks actually relevant to the case studied, and in order to remain in a closed world. Setting a fixed number of risks enables the computation of risk levels (by making things enter into general foreseen cases) and prevents from a difficulty to comprehend what is happening by restricting to risks known by users.

Then, it is necessary to make a match between any relevant combination of flags and one or several associated risks. This means that when all the flags of a combination are activated, the risks that are associated with this combination of flags will be triggered and assessed. However, if a non-insignificant number of flags is activated, combinations will appear, and it will be necessary to deal with several combinations. In such conditions, only maximal combination are considered for computation, *i.e.* if a given combination which is activated is a subpart of another activated combination, only the combination with the greatest number of flags will be kept, as it will be considered as a particular case of the other one. This is due to the fact that some general combination can trigger several risks, a precision of this combination is likely to provide a focus on a particular, more relevant risk.

Each one of the risks triggered by the analysis of the flag combination will later be assessed in order to determine the level of the corresponding risk.

In the case of AIS system, different risks have been presented in section 6.1, and each flag, as developed in section 4.2.3, carries on its own kind of information about maritime traffic, either about falsification scenario cases with all-AIS data or non-AIS data, or MSI assessment for the determination of the neighbourhood of the vessel. Thus, each flag representing a given situation, it can be linked to one or several of the risks described in section 6.1. But as several flags can occur on the same vessel, the notion of flag combination must be treated. Indeed, the combination of several flags can be performed and such a combination can highlight a given risk or group of risks. In the following of this section, flag combination designates a finite whole of selected flags as their combination demonstrates a given situation leading to a designated risk or a group of designated risks.

The different flag combinations set in the case of AIS messages that have been determined in our study is presented in Figure 6.16. It is considered as expert data, and any expert can modify, add or remove a column of this table (each column representing a given case with all the flags that need to be arisen and the associated risks with this flag combination). It is a result of the deterministic approach we chose, in which a fixed frame must be used, filled with combinations of flags taking the role of rules which are set and can be modified by an expert. In this Figure, each row represents a flag, and each column has a number standing for the flag combination. When a X is put in a cell, it means that the raising of the flag (on the corresponding row) is necessary to trigger the given flag combination. The flag combination is only active when all the flags marked with an X in the column have been raised by the analysis.

Figure 6.16: Table of flags combination for risk determination

6.5 Risk level assessment for maritime authorities

6.5.1 Levels, risks and domains

Once the determination of the risks has been performed, the level for each of the risks can be computed. As it depends on the environment and the stakes, several cases must be discriminated in order to provide to the relevant authorities trustworthy data. In the case of the maritime domain, this environment covers the type of vessel involved, and the type of dimension in which the risk expends, which will be presented hereafter. The risk level is then computed for each one of the selected risks in each of the dimensions with the help of tables, set by an expert of the domain.

Collision Boarding	T/C			T/C - H			P			Pl/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	
Pl/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	

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

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

Figure 6.17: Risks levels for the various risks

The risk level is given according to tables, each risk having its own table. For the risks of grounding, illegal fishing, piracy and terrorism, as well as illegal transportation (Figure 6.17, lower part), four kinds of vessel types are discriminated:

- **T/C** which stands for all cargo vessel, including tankers, for which the variety of goods carried in their tanks forces us to closely 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

The risks are assessed according to three dimensions:

- **H**: Human, risk linked to the human life at sea

- **I**: Infrastructure, risks linked to the structure of the vessel and the coastal and off-shore infrastructures
- **E**: Environmental: all kinds of environmental risks

For the particular case of boarding and collision, the table is more complex (Figure 6.17, upper part), as it involves: the studied vessel on the left entry, the other vessel involved (or the infrastructure: column I) on the top entry, each couple giving six risk levels, still on the dimensions of human, infrastructure and environmental (columns) but adding the dimension of damage inducted and damage undergone (lines).

The several risk levels have been defined after an extract from the CISE (which is a EU Maritime Domain Cooperation Project for the Common Information Sharing Environment[1]) as follow:

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

In order to fill in the table with the proper values, this part of the work shall be done by experts of the maritime environment. As it is expert data, it may evolve and be adapted to a new situation.

6.5.2 Risk level assignment

As we saw in section 6.4, one or several combinations can be completed and can trigger one or several risks. If only one risk is triggered, the corresponding values for H, I and E risks are taken as a result. But if several risks are considered, for each dimension of assessment (H, I and E), a result is computed which is the maximum value of the corresponding risk level for the considered risks. With R being the whole of all risks, CR the whole of the considered risks,

$$Risk_{H;I;E} = \max_{r \in CR; CR \in R} Risk^{r}_{H;I;E}$$

Similarly, if the vessel type is not specified, by default the highest possible risk value in all vessel types is assigned to the vessel in question, enabling further computations and the assignment of a risk level despite the fact that the vessel type is missing.

[1] https://joinup.ec.europa.eu/news/sharing-data-modelling-knowle

6.6 Implementation of risk assessment

The risk assessment in the program proceeds as presented in the Figure 6.18. Two main files are used in the program, one for risk analysis and one for flag combination. As for the database, the results of the flags are used, as well as the risk table and the information which are useful for the whole analysis: the risk level tables and the working window table.

Here, the program queries the working window in order to know what are the ids of the messages that must be treated for each type of message. Then the program queries and keeps in memory the risk level tables that will later be used for the risk level assessment.

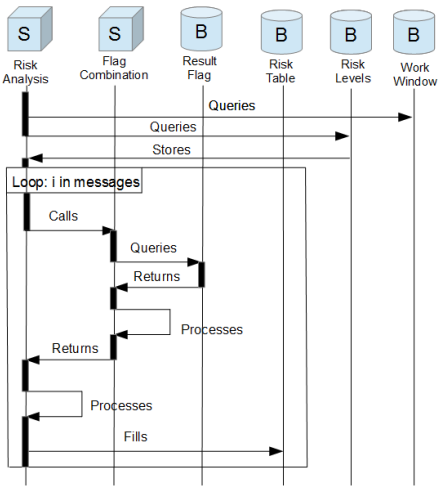

Figure 6.18: Sequence Diagram of the Risk Assessment

Then a loop occurs, and for each message present in the scope of the working window, the same procedure applies for the computation of risk levels. The main program calls the function of flag combination. This function queries the various flags raised in the previous analyses and stored in the database table, and stores them in one big vector. Then it processes on the vector itself to determine if any of the various flag combination defined in section 6.4 occurs. Once all the minimal combinations are determined (minimal combinations being combinations not included in another combination, so consisting of a more general case), the list of those selected combinations is returned by the function to the main risk analysis function. The last step of computation is done there, where the flag combinations are linked to the risks associated as determined in the Figure 6.16, and the risk computed with respect to the vessel type with the tables returned by a previous query. Once the levels determined, they are stored in an *ad hoc* database table. This loop is repeated for each message in the working window until no one remains untreated.

6.7 Risk displaying and analysis limitations

6.7.1 Program output

For each message having a risk issue, each of the raised risks will have its risk level in each of the associated risk that are selected in accordance with the table in Figure 6.16. It is presented in the program output as shown in Figure 6.19, and in parallel data is stored in the database table, as a table useful for further cartographic display of the anomalies[2].

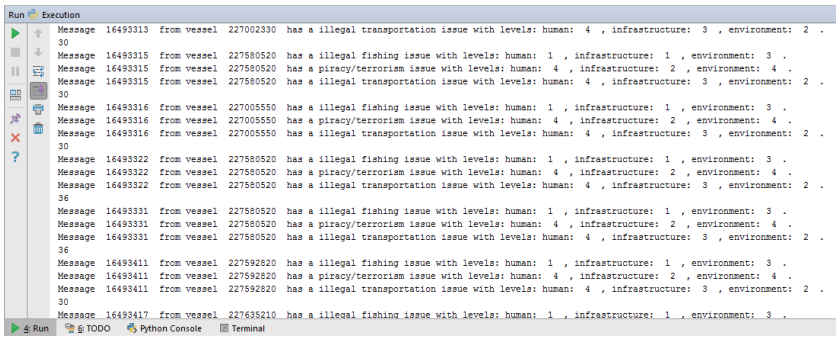

Figure 6.19: Visible outcome of the program for the risks

6.7.2 Outcomes of the experimental cases

In this part, we assess the risks associated with the case studies proposed in part 5.2.3, for which flags have been raised. In accordance with the method for linking the flags to the risks and the table presented in Figure 6.16, the risks in question are presented in the Table 6.1. As the risk level depends on the vessel type, it is not indicated in the table. In the Table 6.1, the first level of rows represent the experiments as defined in section 5.2.3, represented by their letter, and the second level of rows represent the risks that have been selected ; and the columns represent the points number that are defined for each experiment in the corresponding figure (which reference can be found on the left-hand side of the table, below the experiment letter identifier). The section 6.7.3 will deal with the importance of the vessel type for the risk level assessment.

6.7.3 Importance of the vessel type in the risk assessment

As explained before, so far in this section the vessel type was not taken into consideration, only the selected risks were displayed. Here is an example to demonstrate the influence of the vessel type on the assessment. In the example displayed we have a vessel demonstrating a sudden appearance in an unexpected area whose navigational pattern shows that he is coming from an area where fishing is prohibited, as shown in Figure 6.20. Table

[2]A web-based interface has been developed for the cartographic display of anomalous events with respect to the location of the event, the type of event, the risk level triggered and the possibility for an operator to see the surrounding traffic of the spotted anomalous vessel, as well as the possibility for the operator to discard any alert according to his or her appreciation of the situation

Experiment	Risk	Points								
D		1	2	3	4	5	6	7	8	9
Section 5.2.3.4	Collision		√	√	√	√	√	√	√	√
Table 5.6	Grounding									
	Illegal Fishing	√	√	√	√	√	√	√	√	√
	Piracy/Terrorism	√	√	√	√	√	√	√	√	√
	Illegal Transportation	√	√	√	√	√	√	√	√	√
E		1	2	3	4	5	6	7	8	9
Section 5.2.3.5	Collision	√	√	√						
Table 5.7	Grounding					√				
	Illegal Fishing	√					√	√	√	√
	Piracy/Terrorism	√	√	√	√	√	√	√	√	√
	Illegal Transportation	√					√	√	√	√
F		1	2	3	4	5	6	7	8	9
Section 5.2.3.6	Collision					√	√			
Table 5.8	Grounding									
	Illegal Fishing	√				√	√			
	Piracy/Terrorism	√				√	√			
	Illegal Transportation	√				√	√			
G		1	2	3	4	5	6	7	8	9
Section 5.2.3.6	Collision									
Table 5.9	Grounding									
	Illegal Fishing	√					√	√	√	√
	Piracy/Terrorism	√					√	√	√	√
	Illegal Transportation	√					√	√	√	√
H		1	2	3	4	5	6	7	8	9
Section 5.2.3.7	Collision									
Table 5.10	Grounding									
	Illegal Fishing	√				√				
	Piracy/Terrorism	√				√				
	Illegal Transportation	√				√				
I		1	2	3	4	5	6	7	8	9
Section 5.2.3.7	Collision			√	√	√	√			
Table 5.11	Grounding					√	√	√	√	√
	Illegal Fishing	√		√	√	√				
	Piracy/Terrorism	√		√	√	√				
	Illegal Transportation	√		√	√	√				
J		1	2	3	4	5	6	7	8	9
Section 5.2.3.8	Collision									
Table 5.12	Grounding									
	Illegal Fishing	√								
	Piracy/Terrorism	√								
	Illegal Transportation	√								
K		1	2	3	4	5	6	7	8	9
Section 5.2.3.8	Collision									
Table 5.13	Grounding									
	Illegal Fishing									
	Piracy/Terrorism									
	Illegal Transportation									
L		1	2							
Section 5.2.3.9	Collision	√	√							
Table 5.14	Grounding	√	√							
	Illegal Fishing	√	√							
	Piracy/Terrorism	√	√							
	Illegal Transportation	√	√							
M		1								
Section 5.2.3.10	Collision	√								
Table 5.15	Grounding	√								
	Illegal Fishing	√								
	Piracy/Terrorism	√								
	Illegal Transportation	√								

Table 6.1: Table of flag raising and risks selection

6.2 shows the flags and risks raised, in accordance with what was demonstrated in this section before.

Once the associated risks have been selected for each point, the risk levels are assessed in accordance with risk tables presented in section 6.5.1. In our example we take the

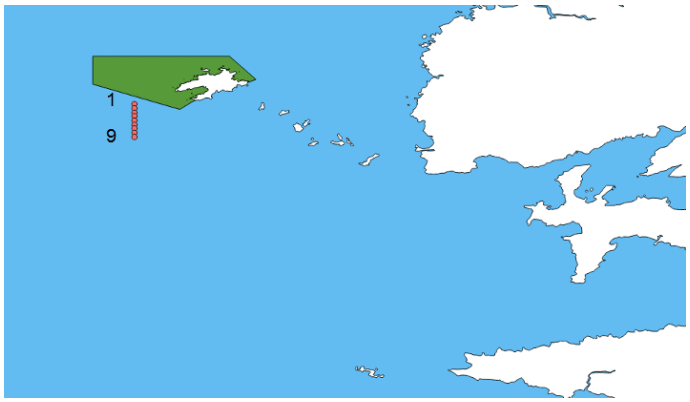

Figure 6.20: Location of points in the unexpected appearance outside a regulated area case

	1	2	3	4	5	6	7	8	9
f_suddenapp	√								
f_comesFromProhibitedArea	√	√	√	√	√	√	√	√	√
Collision									
Grounding									
Illegal Fishing	√	√	√	√	√	√	√	√	√
Piracy/Terrorism	√	√	√	√	√	√	√	√	√
Illegal Transportation	√	√	√	√	√	√	√	√	√

Table 6.2: Table of flag raising and risks selection for this case of unexpected appearance outside a regulated area

four vessel types and present the risk levels for human, infrastructure and environmental domains in Table 6.3.

Type of risk	Human	Infrastructure	Environmental
T/C	4	3	2
T/C - H	4	3	4
P	4	1	1
Pl/S	4	1	1
F	1	1	3

Table 6.3: Table of risk levels according to type of vessel

The analysis of the results provided by the Table 6.3 shows that all vessels but the fishing vessel display a high human risk level, whereas for the infrastructure risk only the tanker and cargo raises a high level of alert, the other types of vessels displaying a minimal risk level. For the environmental risks, the cargo and tanker vessels carrying hazardous goods shows a maximal level because of the risks linked to the cargo itself, whereas the risk is moderate for cargoes and tankers that are not carrying hazardous cargoes because of the risks linked to the presence of hydrocarbons in large tanks. Fishing vessels have high environmental risks because of the risks of illegal fishing in prohibited waters, over-pressuring fish stocks. Other vessel have minimal risk levels.

6.7.4 Limitations

The main limitation of this risk determination is the deterministic aspect of the study. Indeed, a deterministic approach was preferred over a statistical approach for its fit into a

proof of concept case and its relative moderate complexity of implementation with respect of the available remaining time, the DéAIS project coming to an end. This approach, while being imperfect, enables nevertheless to trigger the risks and to assign them levels with respect to the given situation, following a strict set of rules considered as expert knowledge.

Such an approach cannot handle fuzziness, which is an important feature of risk analysis. An inference engine should be able to turn this approach into a statistical one, taking into consideration the links that have already been created with the ontology presented in section 6.3.

Chapter 7

Conclusions

Chapitre 7 : Conclusion

Le travail de recherche présenté dans ce manuscrit se place dans le domaine de la recherche sur la connaissance de la situation maritime, de la découverte de connaissances et de la science des données, avec une application opérationnelle en sécurité de la navigation maritime. Cette problématique opérationnelle est une conséquence des questions de recherches levées après la démonstration de la falsification d'un système de localisation mondial de navires qui est supposé fournir des données utiles à la sécurité de la navigation aux navires environnants. L'objectif a alors été de proposer une méthode afin de mettre en avant les cas où les données semblent démontrer un défaut d'authenticité, et de proposer une évaluation des risques associés à ces cas.

A cette fin, une approche basée sur les dimensions de la qualité de la donnée a été étudiée. En effet, des dimensions de qualité de la donnée sont disponibles à l'étude du fait du caractère fondamentalement basé sur la donnée des systèmes d'information. Plus particulièrement, au sein de la diversité des dimensions de qualité de la donnée, l'intégrité a été discriminée comme étant particulièrement importante pour une évaluation fiable des systèmes à base de donnée, et la méthode d'évaluation est basée sur le développement d'éléments d'évaluation de la donnée basés sur l'intégrité.

Etant donné qu'une évaluation basée sur l'intégrité nécessite une compréhension profonde des mécanismes qui régissent le système en question, une analyse rigoureuse du système a été effectuée, en prenant en compte l'usage premier du système (l'anticollision) et les usages apparus par la suite (la surveillance) pour comprendre les volontés des personnes ayant rédigé les spécifications techniques du système. La partie technique du système a été étudié pour les informations précieuses fournies sur la mécanique interne de ce système, et la partie données du système a été scrutée afin de trouver toutes les combinaisons d'information pouvant tenir lieu de source pour une faille d'intégrité.

La falsification d'un système crée des risques liés à son domaine d'utilisation. Notre étude permet donc d'avoir des éléments sur les risques maritimes, et ces risques peuvent être énumérés afin que les différents cas de failles d'intégrité aboutissent sur la mise en avant d'un ou plusieurs de ces risques en relation directe avec la situation en question. Le

type de risque en question est particulièrement important pour les personnes en charge de la surveillance de la navigation du fait des besoins différents pour une possible intervention selon le risque en question.

La méthode proposée est générique, et peut être appliquée à tous types de systèmes d'information transmettant un taux substantiel d'informations géolocalisées. Certaines améliorations sont envisageables, notamment dans le domaine de l'optimisation du code du programme, de la complétude de la liste d'items proposée et de leur implémentation, de la diversification des scénarios et des cas d'application, de la diversification des sources de données externes et de l'implication d'experts du domaine.

7.1 Overview

The work presented in this manuscript is part of the research in the fields of maritime domain awareness, knowledge discovery and data science, with an operational purpose in maritime safety. The operational issue is a consequence of research questions raised after the demonstration that 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 is then to propose a methodology in order to point 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 that are assessing data.

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.

The falsification of any system raises risks that are related to its field of use. As our study is about a maritime system, its falsification raises maritime risks, and such risks must be enumerated and discriminated so that the various kind of integrity breaches in data will end up in the highlighting of the risks that are in direct relationship with the breach in question. The matter of risks is particularly important for the people in charge of the surveillance of the coast, monitoring of the activities and rallying of the various intervention units.

From the initial study of data assessment methods and the thorough analysis of the system, two axes give structure to this study. First, the modelling of system knowledge

and environment, in conjunction with knowledge of the system, enabled the creation of a methodology for the assessment of this system. Second, the implementation of this methodology using actual system data and leading to usable useful information for operational purposes was performed. This concluding chapter presents the main contributions and the taking stock of the proposed research approach before an opening on potential perspectives.

7.2 Thesis evaluation

The stating hypotheses that sustained this research work were that (1) A data integrity assessment, made possible by the existence of anomalies, allows for the assessment of a message and of its data, (2) It is necessary to process analyses of all sorts on messages, in order to detect anomalies of all sorts, without restricting oneself to spatial temporal messages and spatial analyses, and (3) An anomaly detection of the system enables the assessment of the risks associated to the field of study. This section shows our position with respect to those hypotheses.

7.2.1 An all-encompassing integrity assessment of a system provides anomaly detection

For modelling purposes it is necessary to know perfectly the system studied and its characteristics. In this scope, an all-encompassing analysis of a system would require a knowledge about each part of this system, and more particularly in an integrity assessment every single possibility for two or more elements, given their respective range of values, to disagree and therefore create an integrity breach.

The exploitation of such integrity breach can be done by individually labelling each possibly reported integrity issue, and assessing the available data with respect to those issues, so that it would be possible, for each piece of information, to determine its status in respect of every single integrity statement.

The gathering of the integrity issues under several uses cases brings to anomaly detection, under several assessment distinctive features, such as the fact to consider those issues individually or by group.

The purpose of this thesis was then to propose a methodology based on integrity for the falsification discovery in a message-based system using the data quality dimension of integrity and this approach was realised by the design of a program enabling such as integrity analysis of this system leading to anomaly detection and risk level assessment.

7.2.2 Design of a model for maritime surveillance

This approach on all-encompassing assessment and knowledge discovery was confronted to a real-case applicative domain which is the one of maritime surveillance. To this respect,

each data field from every single message type was taken into consideration and included into the analysis in order for it to encompass all possible cases of integrity problems. A list of 935 of elementary integrity issues was determined after the profound study of the system itself.

Such a problem necessitated the knowledge of maritime domain experts for the proper set of rules that led to the determination of truth or falsehood for every of the integrity items, those rules taking into consideration the system characteristics, the physics of radio transmission, the system technical specifications, the rules of navigation and the kinematics of vessels. The paradigm of a logical framework based on predicate logics was chosen is this respect.

The adjunction of additional non-system pieces of information enables a much deeper level of knowledge, by assigning to each message results from analysis of various kinds, in direct relationship with the vessel location, kinematics, identity and the regulation or environment such as specific geographical features (coasts, specific maritime zones).

The program for the integrity assessment of maritime Automatic Identification System was put in place and successfully displayed the messages for which an integrity issue was detected according to the data available in the dataset and outside the system.

7.2.3 Design of an analysis system linking anomaly detection and risk assessment

Once the program modelled, it is possible to integrate it into a more sophisticated system leading to risk analysis and aiming at helping decision making from the people in charge of maritime traffic monitoring.

In this respect, a set of maritime risks have been chosen for their relationships with actual demonstrated problems in maritime navigation, and for each situation, one or several risks were assigned to a message, the risk level being computed according to the vessel type.

In this scope anomaly detection is at the base of risk type and risk level determination for competent authorities, and by extension integrity analysis is the stem of the whole process of analyses which leads all the way to risk management in the dedicated centres. Typologies have been set with the purpose of describing the maritime environment, and link the flags to the risks. A part of this typology was implemented in the Protégé Software for ontology building. The links between the flags and the risks have been formalised in a table which is known not to be exhaustive as our approach is a proof of concept and not a full risk assessment yet.

7.2.4 A generic method

This research applied to a maritime positioning system and encompasses a way to enumerate, formalise and assess data of various kinds. A generic methodology has been proposed and implemented for the assessment of data quality and the situation of data with respect

to data quality dimensions. This assessment is based on predicates providing threshold-assisted binary results. We do believe this approach is appropriate for the management and assessment of many similar sensing and communicating devices. The nomenclature that has been set is adaptable to the situations and the predicates must be set in order to give a clear binary answer, as it is the way it has been designed in our analysis. Then *ad hoc* scenarios and flags must be put in place for an appropriate application to the studied domain.

This method had had the maritime domain as application domain. However other applicative models may fit for analysis, as it requires a message-based system that transmits a substantial rate of geographic data. Thus, any kind of moving objects could fit this definition, and for some of them such a system already exists.

As we noted in section 3.2.4.2, the aircrafts use ADS-B system, which is just as AIS a message-based geotagged reporting system. Also the vessels use several other reporting systems, such as LRIT.

In addition, a probabilistic approach could be proposed taking for instance into consideration the fuzziness of both treated data and results, and it would not be necessary to change the software altogether as the adding of some data coefficients linked to data fuzziness would be enough.

7.3 Improvement prospects

7.3.1 Code optimisation

There are several ways to optimise the information system, and as of today, in the proof of concept of the work, optimisation has not been a key point in the development thereof. Today, as shown before in section 5.2.4.1, the computational time is not a blocking factor, however it might become such if more items are developed and more analyses are computed. As this work has been designed for real-time analysis, the respect of the computing time is of paramount importance, and the system must process the messages in the allocated time frame, given that for a set of message received during a time span of x minutes, the computing time must not exceed x minutes (as it would delay later analyses and create a snowball effect in the analysis delays).

In our analysis, the database requests are particularly time-consuming, as the Python program asks the database in SQL to provide some data. There are two ways to reduce the time of the requests: act on the requests themselves or act on the number of requests performed. As the requests involve datasets and tables with an important cardinality, the number of entries in the table that will be assessed in the computation is important for time saving. Some actions have already been done in this prospect, by assigning to the SQL requests conditions limiting their research span and their number of returned data. However those limits have been roughly set and it is possible to refine them, adapting both the research span and the number of returned values to every single situation. For the management of the number of requests, some actions can be taken such as the centralisation of database requests prior to the analyses, as the current information system

makes a request at every single item, a single request before the concerned group of items is possible, then several functions would take the outcome of this main request as an entry parameter of their item analysis. This would be a scale reduction of computational time, however it would require small changes in the program architecture, and as it is not necessary for the proof of concept, has not been performed.

Optimisations should also been performed by factorising item analyses. As a matter of fact, as it was mentioned in section 4.1.2.7, items can be gathered into families, and the data in those items receive similar if not identical treatment. A centralisation of such individual function into a unique function that would be called from all similar items would be doable. It would reduce the total size of the code, reduce the risks of mistake in the coding process but most importantly ensure a consistency between all items. As for now those items, similar or perfectly identical, are computed in separate ways, they are subject to differ in the case where one is modified for any reason. The fact to use a centralised function would ensure the consistency of such computations throughout the analyses.

The optimisation of the information system would also go through parallelism computation, as for the items for instance, all items computation are not dependent on the results of the other items and can be treated at the same time if possible.

7.3.2 Complete item list

The current number of implemented and fully functional items is 666. However, as all the items for the most used messages have all been implemented due to the high number of messages to be treated, some items concerning some of the least used messages in the third and fourth order have not been implemented because of the lack thereof. Indeed, the time being limited, the choice to focus on messages for which we received actual messages made sense in our study, however, a complete study would require the completeness of the implementation of items, including the remaining ones that have already been described, the number of which is about two hundreds.

In addition to the items currently defined, a thorough study could be done in order to check if any remaining items could be defined. Indeed, the complexity of the AIS system makes it difficult to point out all the possible cases of data discrepancies, and in addition to those which have been already described could be added some additional items stemmed from an acute knowledge of maritime traffic or a precise understanding of peculiarities of some data fields.

The binary field of some messages could also be used to produce additional items. Actually, in addition to the regular data fields of the most common messages, there is one family of messages that have not been intensively used during our study, which is the binary messages family. In those messages, some data fields are the binary transmission itself, and the study of it can be very complex as it can theoretically transmit very complex and precise information. For instance, in the case of the message number 6, “Binary Addressed Message”, has a data slot of up to 920 bits is set for the transmission of binary data. Another field, namely the Functional ID field, is a integer which role is to tell the nature of the data presented in the binary data field, which can be “Dangerous

Cargo indication", "Tidal window", "Number of persons on board", "Clearance time to enter port" or "Berthing data", amongst other. Every single of those binary data nature has its own layout of the binary data field, providing information in direct relation with the declared nature of data. All those data fields in all the possible cases of all binary messages provide a tremendous amount of pieces of information that could present discrepancies and be transformed into items to be assessed. However, due to the complexity and the number of those pieces of information, this would require a great effort for possibly little result as how scarcely any binary message is received, and the percentage of binary messages received with respect to the total number of all messages is negligible, as seen in section 5.2.1.1.

7.3.3 Scenarios and application cases

At this point, some scenarios have been created, corresponding to the main identified cases in which it was possible to handle the data and provide flags that would later be used to point out different risks. However, with the development of new items, the fact that all items are still not used in the scenarios, and the possible integration of new databases, new scenarios corresponding to the use of both the new and unused items and the database-related assessment could be designed and emerge. As those new scenarios would produce new flags, new combinations could be done leading to a more precise risk assessment.

As the number of scenarios would increase, application cases linked to those scenarios could then emerge and complete the already existing application cases. Most application cases in the case of AIS messages are linked to spatiotemporal patterns of the vessels, because of the large domination of positioning messages

7.3.4 Diversification of the databases

As for now, the information system has been developed using a small variety of data sources that were easily available. However, a diversification of the databases to assess would produce beneficial effects as on the one hand it would offer several different databases representing the same subject, enabling double-checking and allowing to keep up-to-date on some information, and on the other hand offer a wider spectrum of analyses to be performed, enabling additional analyses at the scenario level, and allowing new flags to be created, as well as new flag combinations to be made, leading to the discovery of new kinds of risks.

7.3.5 Involvement of domain experts

A greater involvement of some domain experts in several fields such as maritime knowledge, risk management or risk level assessment would have been helpful to create a more accurate model for risk analysis, particularly for enhancing the knowledge in maritime domain, in behaviour understanding, in risk definition and in risk level assessment.

Experts in maritime knowledge could help refining the program by inputting their understanding of some maritime situation, maritime laws and good practices. Particularly in the items in which a threshold has to be set, the knowledge of a maritime expert is particularly valuable, as the expert will be in grade of deciding a proper threshold separating what is possible or plausible from what is clearly not feasible. In addition, their knowledge of the interactions in the maritime domain will provide information about expected behaviours and possible new relationships between AIS data fields, leading to the implementation of other items. Such experts in maritime domain could also set a proper list of item combination, for an acute modelling based on actual mariners experience.

In this study, only five risks have been defined, gathered in families. Involving experts, this number might go up, as it would be easier to distinguish between the various cases that the families gather. By expending the number of different risk families, a more accurate assessment of the ongoing situation would be given to the people in charge of the monitoring of marine traffic.

In addition to the risk themselves, the risk levels could be adjusted by both maritime domain experts and risk assessment experts, in order to have risk levels that would be more adapted to a maritime danger situation and appealing to both mariners and people in charge of the monitoring of the maritime situation. The risk levels presented in the tables in section 6.5.1 have been evaluated and modified by a maritime expert, however other points of views on those tables may induce a change in the values.

The needs in terms of maritime surveillance depend on the scale of the study. Indeed, a person in charge for coastal surveillance in a MRCC will have different needs than a person in charge of a worldwide fleet monitoring from a ship owner company. Even inside authorities, MRCC, police, civilian or military authorities will not require similar needs. The scalability of the analysis of AIS data (or any geotagged system) would require a whole set of technical adjustments, but remain possible with the current program architecture.

In order to cover all the phases of the risk assessment process, the feedback from operational workers shall be taken into consideration, particularly in the parts of the information system where expert knowledge is required. Those parts shall be adaptable so they can fit as much as possible to the given user. In addition, validation of the program by users could enable this feedback and thus take part of a larger enhancement of the risk management process.

Publications

- Clément Iphar, Aldo Napoli, Cyril Ray, **A system for Alert Triggering based on Automatic Identification System (AIS) Data Integrity Analysis**, *Workshop on Decision Support and Risk Assessment for Operational Effectiveness*, 1 page, 2^{nd}-4^{th} October 2017, La Spezia, Italy

- Clément Iphar, Aldo Napoli, Cyril Ray, **Integrity Assessment of a Worldwide Maritime Tracking System for a Geospatial Risk Analysis at Sea**, 20^{th} *AGILE International Conference on Geographic Information Science (AGILE 2017)*, 4 pages, 9^{th}-12^{th} May 2017, Wageningen, the Netherlands

- Clément Iphar, Aldo Napoli, Cyril Ray, **On the interest of data mining for an integrity assessment of AIS messages**, 1^{st} *International ICDM Workshop on Maritime Domain Data Mining (MDDM 2016)*, 6 pages, 12^{th} December 2016, Barcelona, Spain

- Clément Iphar, Aldo Napoli, Cyril Ray, **Démarche d'analyse de l'intégrité d'un système de localisation de navires**, *SAGEO'16*, 4 pages, Poster, 6^{th}-9^{th} December 2016, Nice, France

- Clément Iphar, Aldo Napoli, Cyril Ray, Erwan Alincourt, David Brosset, **Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety**, *ESREL 2016*, 8 pages, 25^{th}–29^{th} September 2016, Glasgow, UK

- Clément Iphar, Aldo Napoli, Cyril Ray, **Falsification Discovery in AIS Messages**, *Workshop on Decision Support and Risk Assessment for Operational Effectiveness*, 1 page, 26^{th}–28^{th} July 2016, La Spezia, Italy

- Cyril Ray, Clément Iphar, Aldo Napoli, **Methodology for Real-Time Detection of AIS Falsification**, *Maritime Knowledge Discovery and Anomaly Detection Workshop*, pp 74-77, 5^{th}–6^{th} July 2016, Ispra, Italy

- Clément Iphar, Aldo Napoli, Cyril Ray, **A method for integrity assessment of information in a worldwide maritime localization system**, 19^{th} *AGILE International Conference on Geographic Information Science (AGILE 2016)*, 14^{th}–17^{th} June 2016, Helsinki, Finland

- Clément Iphar, Aldo Napoli, Cyril Ray, **Détection de messages falsifiés de localisation de navires**. *EGC 2016*, Poster, pp.557-558, 18^{th}–22^{nd} January 2016, Reims, France

- Clément Iphar, Aldo Napoli, Cyril Ray, **Detection of False AIS Messages for the Improvement of Maritime Situational Awareness**, *OCEANS'15* MTS/IEEE, 7 pages, 19^{th}–22^{nd} October 2015, Washington D.C., USA

- Clément Iphar, Aldo Napoli, Cyril Ray, **Data Quality Assessment For Maritime Situation Awareness**, 9^{th} *ISPRS International Symposium on Spatial Data Quality (ISSDQ 2015)*, Volume II-3/W5, pages 291-296, 29^{th}–30^{th} September 2015, La Grande Motte, France

- Cyril Ray, Clément Iphar, Aldo Napoli, Romain Gallen, Alain Bouju, **DeAIS project: Detection of AIS spoofing and Resulting Risks**, *OCEANS'15* MTS/IEEE, 6 pages, 18^{th}–21^{st} May 2015, Genova, Italy

- Cyril Ray, Clément Iphar, Aldo Napoli, Pierre-Yves Martin, Alain Bouju, **DeAIS project: Detection of faked AIS messages and Resulting Risks**, *IF&GI 2015*, 2 pages, 18^{th}–20^{th} May 2015, Grenoble, France

Bibliography

Aarsæther, Karl Gunnar and Torgeir Moan (2007). "Combined Maneuvering Analysis, AIS and Full-Mission Simulation". In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 1.1, pp. 31–36. ISSN: 2083-6473.

— (2010). "Computer Vision and Ship Traffic Analysis: Inferring Maneuver Patterns From the Automatic Identification System". In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 4.3, pp. 303–308. ISSN: 2083-6473.

Agumya, Aggrey and Gary J. Hunter (1998). "Fitness for use: reducing the impact of geographic information uncertainty". In: *Proceedings of the URISA 98 Conference.* (July 18–22, 1998). Charlotte, USA, pp. 245–254.

Alessandrini, A., M. Alvarez, H. Greidanus, V. Gammieri, F. Fernandez Arguedas, F. Mazzarella, C. Santamaria, M. Stasolla, D. Tarchi, and M. Vespe (2016). "Anomaly detection and knowledge discovery using vessel tracking data". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop.* (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 91–94.

Alessandrini, Alfredo, Pietro Argentieri, Marlene Alvarez Alvarez, Thomas Barbas, Conor Delaney, Virginia Fernandez Arguedas, Vincenzo Gammieri, Harm Greidanus, Fabio Mazzarella, Michele Vespe, and Ziemba Lukasz (2014). "Data Driven Contextual Knowledge from and for Maritime Situational Awareness". In: *Proceedings of the Context-Awareness in Geographic Information Services (CAGIS 2014) Conference.* GI-Science 2014. (Sept. 23, 2014). Ed. by Haosheng Huang, Jürgen Hahn, and Christophe Claramunt. Vienna, Austria.

Alincourt, Erwan, Cyril Ray, Pierre-Michel Ricordel, Delphine Dare-Emzivat, and Abdel Boudraa (2016). "Methodology for AIS signature identification through magnitude and temporal characterization". In: *Proceedings of the OCEANS 2016 SHANGHAI Conference.* (Apr. 10–13, 2016). Shanghai, China: Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/oceansap.2016.7485420.

Allen, Ainsley S. (2014). "The development of ships' routeing measures in the Bering Strait: Lessons learned from the North Atlantic right whale to protect local whale populations". en. In: *Marine Policy* 50, pp. 215–226. ISSN: 0308597X. DOI: 10.1016/j.marpol.2014.05.019.

Andrienko, Gennady, Natalia Andrienko, Christophe Claramunt, Georg Fuchs, and Cyril Ray (2016a). "Visual analysis of vessel traffic safety by extracting events and orchestrating interactive filters". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop.* (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 44–47.

Andrienko, Gennady, Natalia Andrienko, Christophe Claramunt, Georg Fuchs, and Cyril Ray (2016b). "Visual Analysis of Vessel Traffic Safety by Extracting Events and Orchestring Interactive Filters". In: *In proceedings of the Workshop on Visually-supported Computational Movement Analysis (VCMA'16)*. 19th AGILE International Conference on Geographic Information Science (AGILE 2016). (June 14–17, 2016). Helsinki, Finland, p. 7.

Balduzzi, Marco, Alessandro Pasta, and Kyle Wilhoit (2014). "A Security Evaluation of AIS Automated Identification System". In: *Proceedings of the 30th Annual Computer Security Applications Conference*. ACSAC'14. New Orleans, Louisiana, USA: ACM, pp. 436–445. ISBN: 978-1-4503-3005-3. DOI: 10.1145/2664243.2664257.

Balduzzi, Marco, Kyle Wilhoit, and Alessandro Pasta (2014). *A Security Evaluation of AIS*. Tech. rep. Trend Micro.

Bassett, Christopher, Brian Polagye, Marla Holt, and Jim Thomson (2012). "A vessel noise budget for Admiralty Inlet, Puget Sound, Washington (USA)". en. In: *The Journal of the Acoustical Society of America* 132.6, pp. 3706–3719. ISSN: 00014966. DOI: 10.1121/1.4763548.

Belfodil, Aimene, Mehdi Kaytoue, Céline Robardet, Marc Plantevit, and Julien Zarka (2016). "Une méthode de découverte de motifs contextualisés dans les traces de mobilité d'une personne". fr. In: *16ème Conférence Internationale Francophone sur l'Extraction et la Gestion des Connaissances*. (Jan. 18–22, 2016). Reims, France: RNTI.

Berder, Olivier, Philippe Rostaing, and Gilles Burel (2005). "Inter-channel interference rejection for maritime AIS system". In: *Proceedings of the 5th Int. Conf. on Intelligent Transportation Systems Telecomm.* Brest, France.

Berners-Lee, Tim (1998). *Why RDF model is different from the XML model*.

Blomqvist, Kirsimarja (1997). "The many faces of trust". In: *Scandinavian Journal of Management* 13.3, pp. 271–286. ISSN: 0956-5221. DOI: 10.1016/S0956-5221(97)84644-1.

Bošnjak, Rino, Ljupko Šimunović, and Zvonko Kavran (2012). "Automatic Identification System in Maritime Traffic and Error Analysis". In: *Transactions on Maritime Science* 01.02, pp. 77–84. DOI: 10.7225/toms.v01.n02.002.

Braca, Paolo and Enrica d'Afflisio (2017). "Abnormal behavior detection by means of the Ornstein-Uhlenbeck process". In: *Proceedings of the 2017 DeSRA Conference*. (Oct. 2–4, 2017). La Spezia, Italy.

Brodie, Michael L. (1980). "Data quality in information systems". In: *Information & Management* 3.6, pp. 245–258. ISSN: 0378-7206. DOI: 10.1016/0378-7206(80)90035-X.

Brusch, Stephan, Susanne Lehner, Thomas Fritz, Matteo Soccorsi, Alexander Soloviev, and Bart van Schie (2011). "Ship Surveillance With TerraSAR-X". In: *IEEE Transactions on Geoscience and Remote Sensing* 49.3, pp. 1092–1103. ISSN: 0196-2892, 1558-0644. DOI: 10.1109/TGRS.2010.2071879.

Ceolin, Davide, Willem Robert van Hage, Guus Schreiber, and Wan Fokkink (2013). "Assessing Trust for Determining the Reliability of Information". In: *Situation Awareness with Systems of Systems*. Ed. by Piërre van de Laar, Jan Tretmans, and Michael Borth. New York, USA: Springer New York, pp. 209–228. DOI: 10.1007/978-1-4614-6230-9_13.

Certu (2010). *La qualité des données géographiques : état des lieux pour un débat*. Tech. rep. Centre d'études sur les réseaux, les transports, l'urbanisme et les constructions publiques.

Cervera, Miguel A. and Alberto Ginesi (2008). "On the performance analysis of a satellite-based AIS system". In: *Proceedings of the 10th International Workshop on Signal Processing for Space Communications*. (Oct. 6–8, 2008). Rhodes, Greece: Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/SPSC.2008.4686715.

Cervera, Miguel A., Alberto Ginesi, and Knut Eckstein (2011). "Satellite-based vessel Automatic Identification System: A feasibility and performance analysis". en. In: *International Journal of Satellite Communications and Networking* 29.2, pp. 117–142. ISSN: 15420973. DOI: 10.1002/sat.957.

Chandola, Varun, Arindam Banerjee, and Vipin Kumar (2009). "Anomaly detection: A survey". In: *ACM Computing Surveys* 41.3. ISSN: 03600300. DOI: 10.1145/1541880.1541882.

Chang, Liu (2010). "Study of AIS communication protocol in VTS". In: *2nd International Conference on Signal Processing Systems*. (July 5–7, 2010). Dalian, China: IEEE, pp. V1–168–V1–171. ISBN: 978-1-4244-6892-8. DOI: 10.1109/ICSPS.2010.5555594.

Chen, Jinhai, Feng Lu, and Guojun Peng (2015). "A quantitative approach for delineating principal fairways of ship passages through a strait". en. In: *Ocean Engineering* 103, pp. 188–197. ISSN: 00298018. DOI: 10.1016/j.oceaneng.2015.04.077.

Chen, Min, Shiwen Mao, and Yunhao Liu (2014). "Big Data: A Survey". In: *Mobile Networks and Applications* 19 (2), pp. 171–209. ISSN: 1572-8153. DOI: 10.1007/s11036-013-0489-0.

Chen, Ming-Syan, Jiawei Han, and P.S. Yu (1996). "Data mining: an overview from a database perspective". In: *IEEE Transactions on Knowledge and Data Engineering* 8.6, pp. 866–883. ISSN: 10414347. DOI: 10.1109/69.553155.

Claramunt, Christophe, Cyril Ray, Elena Camossi, Anne-Laure Jousselme, Melita Hadzagic, Andrienko Gennady, Natalia Andrienko, Yannis Theodoridis, George Vouros, and Loïc Salmon (2017). "Maritime Data Integration and Analysis: Recent Progress and Research Challenges". In: *Proceedings of the 20th international conference on Extending Database Technology (EDBT)*. (Mar. 21–24, 2017). Venice, Italy. DOI: 10.5441/002/edbt.2017.18.

Clazzer, Federico and Andrea Munari (2015). "Analysis of capture and multi-packet reception on the AIS satellite system". In: *Proceedings of the OCEANS 2015 - Genova Conference*. (May 18–21, 2015). Genova, Italy: Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/OCEANS-Genova.2015.7271399.

Clazzer, Federico, Andrea Munari, Matteo Berioli, and Francisco Lazaro Blasco (2014). "On the characterization of AIS traffic at the satellite". In: *Proceedings of the OCEANS 2014 - TAIPEI Conference*. (Apr. 7–10, 2014). Taipei, China: Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/OCEANS-TAIPEI.2014.6964425.

Collin, Steven, Jean-Jacques Szkolnik, Abdel Boudraa, Delphine Daré-Emzivat, and Cyril Ray (2017). "Détection d'anomalies des signaux AIS à partir de la fréquence instantanée". In: *Proceedings of the 26ième Colloque GRETSI*. (Sept. 5–8, 2017). Juan-Les-Pins, France.

Corporation, Larus Technologies (2015). *High-Level Information Fusion of SAR and AIS to Enhance Maritime Surveillance*. Literature Survey Report. Report Number DRDC-RDDC-2016-C035 — Contract Report. Defence Research and Development Canada. 41 pp.

Costé, Benjamin, Cyril Ray, and Gouenou Coatrieux (2016). "Modèle et mesures de confiance pour la sécurité des systèmes d'informations". In: *Ingénierie des systèmes d'information* 2, pp. 1–24. DOI: 10.3166/ISI.22.2.1-24.

Costin, Andrei and Aurélien Francillon (2012). "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices". In: *Proceedings of the Blackhat USA 2012 Conference*. (July 21–26, 2012). Las Vegas, USA.

Davidson, Ian (2001). *Anomaly Detection, Explanation and Visualization*. By SGI.

Denize, Sara and Louise Young (2007). "Concerning trust and information". In: *Industrial Marketing Management* 36.7, pp. 968–982. ISSN: 0019-8501. DOI: 10.1016/j.indmarman.2007.06.004.

Devillers, Rodolphe (2004). "Conception d'un système multidimensionnel d'information sur la qualité des données géographiques". PhD thesis. Université Laval, Canada / Université de Marne-la-Vallée, France.

Diesch, J.-M., F. Drewnick, T. Klimach, and S. Borrmann (2013). "Investigation of gaseous and particulate emissions from various marine vessel types measured on the banks of the Elbe in Northern Germany". en. In: *Atmospheric Chemistry and Physics* 13.7, pp. 3603–3618. ISSN: 1680-7324. DOI: 10.5194/acp-13-3603-2013.

Dodge, Somayeh, Robert Weibel, and Anna-Katharina Lautenschütz (2008). "Towards a taxonomy of movement patterns". In: *Information Visualization* 7.3, pp. 240–252. ISSN: 1473-8716. DOI: 10.1057/palgrave.ivs.9500182.

Dragulanescu, Nicolae George (2003). "De nouveaux modèles pour les sciences de l'information ?" In: *Proceedings of the tenth Colloque bilatéral franco-roumain, CIFSIC*. (June 28–July 3, 2003). Bucharest, Romania.

EMSA (2013). *Vessel Tracking Globally. Understanding LRIT*. Report. European Maritime Safety Agency. 4 pp.

— (2015). *EMSA Facts and Figures 2015*. Report. European Maritime Safety Agency. 32 pp.

Erbe, Christine, Alec Duncan, and Matthew Koessler (2012). *Modelling Noise Exposure Statistics From Current And Projected Shipping Activity In Northern British Columbia*. Report. World Wildlife Fund Canada.

Erbe, Christine, Alexander MacGillivray, and Rob Williams (2012). "Mapping cumulative noise from shipping to inform marine spatial planning". en. In: *The Journal of the Acoustical Society of America* 132.5, pp. 423–428. ISSN: 00014966. DOI: 10.1121/1.4758779.

Erbe, Christine, Rob Williams, Doug Sandilands, and Erin Ashe (2014). "Identifying Modeled Ship Noise Hotspots for Marine Mammals of Canada's Pacific Region". en. In: *PLoS ONE* 9.11. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0114362.

Eriksen, Torkild, Gudrun Høye, Bjørn Narheim, and Bente Jensløkken Meland (2006). "Maritime traffic monitoring using a space-based AIS receiver". en. In: *Acta Astronautica* 58.10, pp. 537–549. ISSN: 00945765. DOI: 10.1016/j.actaastro.2005.12.016.

ESA (2012). *Space Station Keeps Watch on World's Sea Traffic*.

Etienne, Laurent (2011). "Motifs spatio-temporels de trajectoires d'objets mobiles, de l'extraction à la détection de comportements inhabituels. Application au trafic maritime." PhD thesis. Université de Bretagne Occidentale.

Etienne, Laurent, Thomas Devogele, and Alain Bouju (2010). "Spatio-temporal trajectory analysis of mobile objects following the same itinerary". In: *In Proceedings of the Joint International Conference on Theory, Data Handling and Modelling in GeoSpatial Information Science*. Hong Kong, China, pp. 86–91.

Etienne, Laurent, Thomas Devogele, Maike Buckin, and Gavin McArdle (2016). "Trajectory Box Plot: a new pattern to summarize movements". In: *International Journal of*

Geographical Information Science. Analysis of Movement Data 30.5, pp. 835–853. DOI: 10.1080/13658816.2015.1081205.

Faber, Jasper, Dagman Nelissen, Galen Hon, Haifend Wang, and Mikis Tsimplis (2012). *Regulated Slow Steaming in Maritime Transport. An Assessment of Options, Costs and Benefits*. Report. CE Delft. 117 pp.

Faragher, Ramsey, Peter F. MacDoran, and Michael B. Mathews (2014). "Spoofing Mitigation, Robust Collision Avoidance, and Opportunistic Receiver Localisation Using a New Signal Processing Scheme for ADS-B or AIS". In: *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2014)*. Tempa, Florida, USA, pp. 858–868.

Fernandez Arguedas, Virginia, Giuliana Pallotta, and Michele Vespe (2014a). "Automatic generation of geographical networks for maritime traffic surveillance". In: *Proceedings of the 17th International Conference on Information Fusion*. Salamanca, Spain: IEEE. ISBN: 978-84-9012-355-3.

— (2014b). "Unsupervised Maritime Pattern Analysis to Enhance Contextual Awareness". In: *Proceedings of the Context-Awareness in Geographic Information Services (CAGIS 2014) Conference*. GIScience 2014. (Sept. 23, 2014). Ed. by Haosheng Huang, Jürgen Hahn, and Christophe Claramunt. Vienna, Austria.

Finke, Cindy, Jonathan Butts, and Robert Mills (2013). "ADS-B encryption: confidentiality in the friendly skies". In: *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13*. (Jan. 8–10, 2013). Oak Ridge, TN, USA: ACM Press, p. 1. ISBN: 978-1-4503-1687-3. DOI: 10.1145/2459976.2459986.

Fisher, Craig W. and Bruce R. Kingma (2001). "Criticality of Data Quality As Exemplified in Two Disasters". In: *Information and Management* 39.2, pp. 109–116. ISSN: 0378-7206. DOI: 10.1016/S0378-7206(01)00083-0.

Fondin, Hubert (2005). "La science de l'information ou le poids de l'histoire". In: *Les enjeux de l'information et de la communication*. GRESEC, pp. 35–54.

Fox, Christopher, Anany Levitin, and Thomas Redman (1994). "The Notion of Data and Its Quality Dimensions". In: *Information Processing and Management* 30.1, pp. 9–19. ISSN: 0306-4573. DOI: 10.1016/0306-4573(94)90020-5.

Franke, Beate, Jean-François Plante, Ribana Roscher, Annie Lee, Cathal Smyth, Armin Hatefi, Fuqi Chen, Einat Gil, Alexander Schwing, Alessandro Selvitella, Michael M. Hoffman, Roger Grosse, Dieter Hendricks, and Nancy Reid (2015). *Statistical Inference, Learning and Models in Big Data*. In Thematic Program on Statistical Inference, Learning, and Models for Big Data, by Fields Institute; 23 pages.

Frewer, L. J., C. Howard, D. Hedderley, and R. Shepherd (1996). "What determines Trust in Information About Food-Related Risks? Underlying Psychological Constructs". In: *Risk Analysis* 16.4, pp. 473–485.

Gaffiot, Félix (1934). *Dictionnary Latin-French*.

Gaspar, Philippe, Rémy Lopez, Marza Marzuki, Ronan Fablet, Philippe Gros, Jean-Michel Zigna, and Gaetan Fabritius (2016). "Analysis of vessel trajectories for maritime surveillance and fisheries management". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 22–23.

gCaptain (2012). *Reuters: Iran Falsifying AIS Data to Conceal Ship Movements*. by Jessica Donati and Daniel Fineren.

Gervais, Marc (2003). "Pertinence d'un manuel d'instructions au sein d'une stratégie de gestion du risque juridique découlant de la fourniture de données géographiques numériques". PhD thesis. Université de Marne-la-Vallée, France.

Giannotti, Fosca, Mirco Nanni, Fabio Pinelli, and Dino Pedreschi (2007). "Trajectory Pattern Mining". In: *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '07*. (Aug. 12–15, 2007). San José, CA, USA: ACM Press. ISBN: 978-1-59593-609-7. DOI: 10.1145/1281192.1281230.

Gilberg, A., E. Kleiven, and R.J. Bye (2016). "Marine navigation accidents and influencing conditions: An exploratory statistical analysis using AIS data and accident databases". In: *Proceedings of the ESREL 2016 Conference*. (Sept. 25–29, 2016). Ed. by Lesley Walls, Matthew Revie, and Tim Bedford. Glasgow, United Kingdom: Taylor & Francis, pp. 97–104. ISBN: 978-1-138-02997-2.

Glandrup, Maurice (2013). "Improving Situation Awareness in the Maritime Domain". In: *Situation Awareness with Systems of Systems*. Ed. by Piërre van de Laar, Jan Tretmans, and Michael Borth. New York, USA: Springer New York, pp. 21–38. DOI: 10.1007/978-1-4614-6230-9_2.

Goerlandt, Floris and Pentti Kujala (2011). "Traffic simulation based ship collision probability modeling". en. In: *Reliability Engineering & System Safety* 96.1, pp. 91–107. ISSN: 09518320. DOI: 10.1016/j.ress.2010.09.003.

Goldsworthy, Laurie and Brett Goldsworthy (2015). "Modelling of ship engine exhaust emissions in ports and extensive coastal waters based on terrestrial AIS data – An Australian case study". en. In: *Environmental Modelling & Software* 63, pp. 45–60. ISSN: 13648152. DOI: 10.1016/j.envsoft.2014.09.009.

Gómez-Pérez, Asunción (1999). *Ontological Engineering: A State Of The Art*. Facultad de Informatica, Universidad Politecnica de Madrid.

Goshtasby, A. Ardeshir (2012). "Similarity and Dissimilarity Measures". In: *Image Registration*. London, UK: Springer London, pp. 7–66. ISBN: 978-1-4471-2457-3 978-1-4471-2458-0.

Guarino, N. (1998). *Formal Ontology in Information Systems: Proceedings of the 1st International Conference June 6-8, 1998, Trento, Italy*. 1st. Amsterdam, The Netherlands, The Netherlands: IOS Press. ISBN: 9051993994.

Gucma, Maciej (2008). "Combination of Processing Methods for Various Simulation Data Sets". In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 2.1, pp. 11–15. ISSN: 2083-6473.

Guichoux, Yann, Marc Lennon, and Nicolas Thomas (2016). "Sea surface currents calculation using vessel tracking data". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 31–35.

Habtemariam, B., R. Tharmarasa, M. McDonald, and T. Kirubarajan (2015). "Measurement level AIS/radar fusion". en. In: *Signal Processing* 106, pp. 348–357. ISSN: 01651684. DOI: 10.1016/j.sigpro.2014.07.029.

Hadzagic, Melita and Anne-Laure Jousselme (2016). "Contextual anomalous destination detection for maritime surveillance". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 62–65.

Hammond, Tim, Mark McIntyre, David M. F. Chapman, and Anna-Liesa S. Lapinski (2006). *The Implications of Self-Reporting Systems for Maritime Domain Awareness*.

Report. Technical Memorandum - DRDC Atlantic TM 2006-232 - December 2006. Defence Research and Development Canada.

Harati-Mokhtari, Abbas, Alan Wall, Philip Brooks, and Jin Wang (2007). "Automatic Identification System (AIS): A Human Factors Approach". In: *Journal of Navigation*. Cambridge University Press.

Hartmann, Stephan and Luc Bovens (2001). "A Probabilistic Theory of the Coherence of an Information Set". In: *Argument & Analysis: Proceedings of the 4th International Congress of the Society for Analytical Philosophy*. Ed. by Ansgar Beckermann. Bielefeld, Germany, pp. 195–206.

Hassanin, Ahmed, Francisco Lazaro, and Simon Plass (2015). "An advanced AIS receiver using a priori information". In: *OCEANS 2015 - Genova*. (May 18–21, 2015). Genova, Italy: Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/OCEANS-Genova.2015.7271475.

Hatch, Leila, Christopher Clark, Richard Merrick, Sofie Van Parijs, Dimitri Ponirakis, Kurt Schwehr, Michael Thompson, and David Wiley (2008). "Characterizing the Relative Contributions of Large Vessels to Total Ocean Noise Fields: A Case Study Using the Gerry E. Studds Stellwagen Bank National Marine Sanctuary". In: *Environmental Management* 42.5, pp. 735–752. ISSN: 0364-152X, 1432-1009. DOI: 10.1007/s00267-008-9169-4.

Hepp, Martin (2007). *Ontologies: State of the Art, business, potential, and grand challenges*. Digital Enterprise Research Institute, University of Innsbruck.

Hertzum, Morten, Hans H.K Andersen, Verner Andersen, and Camilla B Hansen (2002). "Trust in information sources: seeking information from people, documents, and virtual agents". In: *Interacting with Computers* 14.5, pp. 575–599. ISSN: 0953-5438. DOI: 10.1016/S0953-5438(02)00023-1.

St-Hilaire, Marie-Odette (2010). *Determining the Consistency of Information between Multiple Subsystems used in Maritime Domain Awareness*. Report. Contract Report DRDC Atlantic CR 2010-025. July 2010. Defence Research and Development Canada.

Holst, Anders, Peter Ryman, and Anders Linse (2016). "Statistical anomaly detection for maritime surveillance and monitoring". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 7–9.

Horn, Steven, Cheryl Eisler, Peter Dobias, and Joe Collins (2016). "Data requirements for anomaly detection". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 52–56.

Høye, Gudrun K., Torkild Eriksen, Bente J. Meland, and Bjørn T. Narheim (2008). "Space-based AIS for global maritime traffic monitoring". en. In: *Acta Astronautica* 62.2-3, pp. 240–245. ISSN: 00945765. DOI: 10.1016/j.actaastro.2007.07.001.

Hu, Baifan, Xiang Jiang, Erico de Souza, Ronald Pelot, and Stan Matwin (2016). "Identifying fishing activities from AIS data with Conditional Random Fields". In: *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*. (Sept. 11–14, 2016). Gdansk, Poland: IEEE.

Huh, Y. U., F. R. Keller, T. C. Redman, and A. R. Watkins (1990). "Data Quality". In: *Information and Software Technology* 32.8, pp. 559–565. ISSN: 0950-5849. DOI: 10.1016/0950-5849(90)90146-I.

Huntington, Henry P., Raychelle Daniel, Andrew Hartsig, Kevin Harun, Marilyn Heiman, Rosa Meehan, George Noongwook, Leslie Pearson, Melissa Prior-Parks, Martin Ro-

bards, and George Stetson (2015). "Vessels, risks, and rules: Planning for safe shipping in Bering Strait". In: *Marine Policy* 51, pp. 119–127. ISSN: 0308597X. DOI: 10.1016/j.marpol.2014.07.027.

Idiri, Bilal (2013). "Méthodologie d'extraction de connaissances spatio-temporelles par fouille de données pour l'analyse de comportements à risques - Application à la surveillance maritime". PhD thesis. MINES ParisTech.

Ilarri, Sergio, Dragan Stojanovic, and Cyril Ray (2015). "Semantic management of moving objects: A vision towards smart mobility". In: *Expert Systems with Applications* 42.3, pp. 1418–1435. ISSN: 0957-4174. DOI: 10.1016/j.eswa.2014.08.057.

IMO (1987). *IMO ship identification number scheme. Resolution A.600(15)*. Resolution. International Maritime Organization.

— (1995). *Definition of Sea Areas A1, A2, A3 and A4 from IMO resolution A801(19)*. Report. International Maritime Organization.

— (2004). *International Convention for the Safety of Life at Sea*. Tech. rep. IMO.

— (2009). *COLREGS - International Regulations for Preventing Collisions at Sea*. Tech. rep. International Maritime Organization. 74 pp.

— (2013). *IMO ship identification number scheme. Resolution A.1078(28)*. Resolution. International Maritime Organization.

IOM (2017). *Arrivées de migrants en Europe par la Méditerranée : 114 287 ; décès en mer : 2 385*. International Organization for Migrations.

Iphar, Clément, Aldo Napoli, and Cyril Ray (2016). "On the interest of data mining for an integrity assessment of AIS messages". In: *Proceedings of the 1st International ICDM Workshop on Maritime Domain Data Mining (MDDM 2016)*. (Dec. 12, 2016). Barcelona, Spain: Institute of Electrical and Electronics Engineers - IEEE, pp. 368–373. DOI: 10.1109/ICDMW.2016.72.

Iphar, Clément, Aldo Napoli, Cyril Ray, Erwan Alincourt, and David Brosset (2016). "Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety". In: *Proceedings of the ESREL 2016 Conference*. (Sept. 25–29, 2016). Ed. by Tim Bedford Lesley Walls Matthew Revie. Glasgow, United Kingdom: Taylor & Francis, pp. 606–613. ISBN: 978-1-138-02997-2.

ITU (2012). *Recommendation ITU-R M.1084-5 (03/2012) – Interim solutions for improved efficiency in the use of the band 156-174 MHz by stations in the maritime mobile service*. Recommendation. March 2012. International Telecommunication Union.

— (2015). *Recommendation ITU-R M.585-7 (03/2015) – Assignment and use of identities in the maritime mobile service. M Series. Mobile, radiodetermination, amateur and related satellite services*. Recommendation. March 2015. International Telecommunication Union.

Jagadish, H. V., Johannes Gehrke, Alexandros Labrinidis, Yannis Papakonstantinou, Jignesh M. Patel, Raghu Ramakrishnan, and Cyrus Shahabi (2014). "Big Data and Its Technical Challenges". In: *Commun. ACM* 57 (7), pp. 86–94. ISSN: 0001-0782. DOI: 10.1145/2611567.

Jalkanen, J.-P., A. Brink, J. Kalli, H. Pettersson, J. Kukkonen, and T. Stipa (2009). "A modelling system for the exhaust emissions of marine traffic and its application in the Baltic Sea area". In: *Atmospheric Chemistry and Physics* 9.23, pp. 9209–9223. DOI: 10.5194/acp-9-9209-2009.

Jalkanen, J.-P., L. Johansson, J. Kukkonen, A. Brink, J. Kalli, and T. Stipa (2012). "Extension of an assessment model of ship traffic exhaust emissions for particulate matter

and carbon monoxide". en. In: *Atmospheric Chemistry and Physics* 12.5, pp. 2641–2659. ISSN: 1680-7324. DOI: 10.5194/acp-12-2641-2012.

Jalkanen, Jukka-Pekka, Lasse Johansson, and Jaakko Kukkonen (2014). "A Comprehensive Inventory of the Ship Traffic Exhaust Emissions in the Baltic Sea from 2006 to 2009". In: *AMBIO* 43.3, pp. 311–324. ISSN: 0044-7447, 1654-7209. DOI: 10.1007/s13280-013-0389-3.

Jousselme, A.-L., E. Camossi, M. Hadzagic, C. Ray, C. Claramunt, E. Reardon, K. Bryan, and M. Ilteris (2016). "A fishing monitoring use case in support to collaborative research". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 57–61.

Jousselme, Anne-Laure and Giuliana Pallotta (2015). "Dissecting uncertainty-based fusion techniques for maritime anomaly detection". In: *Proceedings of the 18th International Conference on Information Fusion*. (July 6–9, 2015). Washington, DC, USA: IEEE.

Kao, Sheng-Long, Kuo-Tien Lee, Ki-Yin Chang, and Min-Der Ko (2007). "A Fuzzy Logic Method for Collision Avoidance in Vessel Traffic Service". en. In: *Journal of Navigation* 60.1, p. 17. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463307003980.

Karadáis, Basil (2013). "Atomicity, coherence of information, and point-free structures". In: *Annals of Pure and Applied Logic* 167.9. Fourth Workshop on Formal Topology (4WFTop), pp. 753–769. DOI: 10.1016/j.apal.2016.04.012.

Katal, Avita, Mohammad Wazid, and R. H. Goudar (2013). "Big data: Issues, challenges, tools and Good practices". In: *Proceedings of the 2013 Sixth International Conference on Contemporary Computing (IC3)*. (Aug. 8–10, 2013). Noida, India. DOI: 10.1109/IC3.2013.6612229.

Katsilieris, Fotios, Paolo Braca, and Stefano Coraluppi (2013). "Detection of malicious AIS position spoofing by exploiting radar information". In: *Proceedings of the 16th International Conference on Information Fusion*. Istambul, Turkey.

Kelton, Kari, Kenneth R. Fleischmann, and William A. Wallace (2008). "Trust in Digital Information". In: *Journal of the American Society for Information Science and Technology* 59.3, pp. 363–374. ISSN: 1532-2882. DOI: 10.1002/asi.v59:3.

Kotovirta, Ville, Risto Jalonen, Lars Axell, Kaj Riska, and Robin Berglund (2009). "A system for route optimization in ice-covered waters". In: *Cold Regions Science and Technology* 55.1, pp. 52–62. ISSN: 0165232X. DOI: 10.1016/j.coldregions.2008.07.003.

Koufakou, Anna, Jimmy Secretan, and Michael Georgiopoulos (2011). "Non-derivable itemsets for fast outlier detection in large high-dimensional categorical data". In: *Knowledge and Information Systems* 29.3, pp. 697–725. ISSN: 0219-1377, 0219-3116. DOI: 10.1007/s10115-010-0343-7.

Kumar, Vipin and Sonajharia Minz (2014). "Feature Selection: A literature Review". In: *The Smart Computing Review* 4.3. ISSN: 22344624. DOI: 10.6029/smartcr.2014.03.007.

Langford, Chad, Tao Cheng, and Michele Vespe (2016). "Data driven identification of migrant vessel at sea". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 69–73.

Last, Philipp, Christian Bahlke, Martin Hering-Bertram, and Lars Linsen (2014). "Comprehensive Analysis of Automatic Identification System (AIS) Data in Regard to Vessel

Movement Prediction". In: *Journal of Navigation* 67.05, pp. 791–809. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463314000253.

Last, Philipp, Martin Hering-Bertram, and Lars Linsen (2015). "How automatic identification system (AIS) antenna setup affects AIS signal quality". In: *Ocean Engineering* 100, pp. 83–89. ISSN: 00298018. DOI: 10.1016/j.oceaneng.2015.03.017.

Lautier, Irène (2007). *Expression - Communication*. Lesson to Licence GAAS - Faculté des Sciences du Sport et de l'EP - University of Lille 2.

Lavigne, Valerie, Denis Gouin, and Michael Davenport (2011). "Visual analytics for maritime domain awareness". In: *Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST)*. (Nov. 15–17, 2011). Waltham, USA: IEEE, pp. 49–54. DOI: 10.1109/THS.2011.6107846.

Lecornu, Laurent, Julien Montagner, and John Puentes (2013). "Reliability evaluation of incomplete AIS trajectories". In: *Proceedings of the COST MOVE Workshop on Moving Objects at Sea*. (June 27–28, 2013). Brest, France.

Lee, H.S., S.M. Lee, and H.H. Lee (2007). "The Realization of the Performance Estimation System on AIS SOTDMA Algorithm". In: *2007 5th IEEE International Conference on Industrial Informatics*. (June 23–27, 2007). Vienna, Austria: IEEE, pp. 405–410. ISBN: 978-1-4244-0850-4 978-1-4244-0851-1. DOI: 10.1109/INDIN.2007.4384791.

Lee, Seoung-Hyeon, Yong-Kyun Kim, Jong-Wook Han, and Deok-Gyu Lee (2014). "Protection Method for Data Communication between ADS-B Sensor and Next-Generation Air Traffic Control Systems". en. In: *Information* 5.4, pp. 622–633. ISSN: 2078-2489. DOI: 10.3390/info5040622.

Lefrançois, Maxime (2016). *Logiques de description, et ontologies en logiques de description*. Lecture. MINES Saint-Etienne.

Lessing, P., L. Bernard, B. Tetreault, and J. Chaffin (2006). "Use of the Automatic Identification System (AIS) on Autonomous Weather Buoys for Maritime Domain Awareness Applications". In: *Proceedings of the OCEANS 2006 Boston Conference*. (Sept. 18–21, 2006). Boston, USA: IEEE, pp. 1–6. ISBN: 978-1-4244-0114-7 978-1-4244-0115-4. DOI: 10.1109/OCEANS.2006.307023.

Lindstrom, Tedric R. (2014). "Using Automatic Identification System technology to improve maritime border security". MA thesis. Monterey Naval Postgraduate School.

Liping, Li and Ma Shexiang (2012). "Analysis and Simulation of Slot Collision and Reception Performance of AIS". In: *Advances in Electric and Electronics*. Ed. by Wensong Hu. Vol. 155. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 661–669. ISBN: 978-3-642-28743-5 978-3-642-28744-2.

Liu, Changqing and Xiaoqian Chen (2013). "Inference of Single Vessel Behaviour with Incomplete Satellite-based AIS Data". In: *Journal of Navigation* 66.06, pp. 813–823. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463313000374.

Lloyd's List (2013). *Can AIS be trusted?*

Lundkvist, Markus, Lars Jakobsson, and René Modigh (2008). "Automatic Identification System (AIS) and Risk-Based Planning of Hydrographic Surveys in Swedish Waters". In: *Proceedings of the FIG Working Week 2008*. (June 14–19, 2008). Stockholm, Sweden.

Madnick, Stuart and Hongwei Zhu (2006). "Improving Data Quality Through Effective Use of Data Semantics". In: *Data Knowl. Eng.* 59.2, pp. 460–475. ISSN: 0169-023X. DOI: 10.1016/j.datak.2005.10.001.

Maggi, Fabrizio M., Arjan J. Mooij, and Wil M. P. van der Aalst (2013). "Analyzing Vessel Behavior Using Process Mining". In: *Situation Awareness with Systems of Systems*.

Ed. by Piërre van de Laar, Jan Tretmans, and Michael Borth. New York, USA: Springer New York, pp. 133–148. DOI: 10.1007/978-1-4614-6230-9_9.

Marin, Le (2014). *Comment le port d'Anvers a été piraté par un cartel de la drogue*. Le Marin, 25th July 2014, page number 10, by Robin Geoffroy.

Martineau, Etienne and Jean Roy (2011). *Maritime Anomaly Detection: Domain Introduction and Review of Selected Literature*. Tech. rep. Technical Memorandum - DRDC Valcartier TM 2010-460 - October 2011. Defence Research and Development Canada. 66 pp.

Mazzarella, Fabio, Alfredo Alessandrini, Harm Greianus, Marlene Alvarez Alvarez, Pietro Argentieri, Domenico Nappo, and Ziemba Lukasz (2013). "Data Fusion for Wide-Area Maritime Surveillance". In: *Proceedings of the COST MOVE Workshop on Moving Objects at Sea*. (June 27–28, 2013). Brest, France.

Mazzarella, Fabio, Virginia Fernandez Arguedas, and Michele Vespe (2015). "Knowledge-based vessel position prediction using historical AIS data". In: *2015 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*. Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/sdf.2015.7347707.

Mazzarella, Fabio, Michele Vespe, Dimitrios Damalas, and Giacomo Osio (2014). "Discovering vessel activities at sea using AIS data: Mapping of fishing footprints". In: *Proceedings of the 17th International Conference on Information Fusion*. (July 7–10, 2014). Salamanca, Spain.

Mazzarella, Fabio, Michele Vespe, and Carlos Santamaria (2015). "SAR Ship Detection and Self-Reporting Data Fusion Based on Traffic Knowledge". In: *IEEE Geoscience and Remote Sensing Letters* 12.8, pp. 1685–1689. ISSN: 1545-598X, 1558-0571. DOI: 10.1109/LGRS.2015.2419371.

Mazzarella, Fabio, Michele Vespe, Dario Tarchi, Giuseppe Aulicino, and Antonio Vollero (2016). "AIS reception characterisation for AIS on/off anomaly detection". In: *Proceedings of the 19th International Conference on Information Fusion*. (July 5–8, 2016). Heidelberg, Germany: IEEE.

McAfee, A. and E. Brynjolfsson (2012). "Big data: the management revolution." In: *Harvard Business Review* 90 (10), pp. 60–66.

McCauley, D. J., P. Woods, B. Sullivan, B. Bergman, C. Jablonicky, A. Roan, M. Hirshfield, K. Boerder, and B. Worm (2016). "Ending hide and seek at sea". In: *Science* 351.6278, pp. 1148–1150. DOI: 10.1126/science.aad5686.

McGillivary, Philip A., Kurt D. Schwehr, and Kevin Fall (2009). "Enhancing AIS to improve whale-ship collision avoidance and maritime security". In: *Proceedings of the OCEANS 2009 Biloxi Conference*. (Oct. 26–29, 2009). Biloxi, USA: IEEE.

McKenna, Megan F., Donald Ross, Sean M. Wiggins, and John A. Hildebrand (2012). "Underwater radiated noise from modern commercial ships". In: *The Journal of the Acoustical Society of America* 131.1, pp. 92–103. ISSN: 00014966. DOI: 10.1121/1.3664100.

McKnight, Harrison (2005). "Trust in Information Technology". In: *The Blackwell Encyclopedia of Management*. Management Information Systems 7. Ed. by G.B. Davis, pp. 329–331.

Merchant, Nathan D., Enrico Pirotta, Tim R. Barton, and Paul M. Thompson (2014). "Monitoring ship noise to assess the impact of coastal developments on marine mammals". In: *Marine Pollution Bulletin* 78.1-2, pp. 85–95. ISSN: 0025326X. DOI: 10.1016/j.marpolbul.2013.10.058.

Merchant, Nathan D., Matthew J. Witt, Philippe Blondel, Brendan J. Godley, and George H. Smith (2012). "Assessing sound exposure from shipping in coastal waters using a single hydrophone and Automatic Identification System (AIS) data". In: *Marine Pollution Bulletin* 64.7, pp. 1320–1329. ISSN: 0025326X. DOI: 10.1016/j.marpolbul.2012.05.004.

Millefiori, Leonardo M., Luca Cazzanti, Dimitris Zissis, and Gianfranco Arcieri (2016). "Scalable estimation of port areas from AIS data". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 48–51.

Millefiori, Leonardo M., Dimitrios Zissis, Luca Cazzanti, and Gianfranco Arcieri (2016). "Scalable and distributed sea port operational areas estimation from AIS data". In: *Proceedings of the 1st International ICDM Workshop on Maritime Domain Data Mining (MDDM 2016)*. (Dec. 12, 2016). Barcelona, Spain: Institute of Electrical and Electronics Engineers - IEEE, pp. 374–381. DOI: 10.1109/ICDMW.2016.27.

Millefiori, Leonardo, Paolo Braca, Karna Bryan, and Peter Willett (2016). "Long-Term Vessel Kinematics Prediction Exploiting Mean-Reverting Processes". In: *Proceedings of the 19th International Conference on Information Fusion*. (July 5–8, 2016). Heidelberg, Germany: IEEE.

Miola, Apollonia and Biagio Ciuffo (2011). "Estimating air emissions from ships: Meta-analysis of modelling approaches and available data sources". en. In: *Atmospheric Environment* 45.13, pp. 2242–2251. ISSN: 13522310. DOI: 10.1016/j.atmosenv.2011.01.046.

Montewka, Jakub, Tomasz Hinz, Pentti Kujala, and Jerzy Matusiak (2010). "Probability modelling of vessel collisions". In: *Reliability Engineering & System Safety* 95.5, pp. 573–589. ISSN: 09518320. DOI: 10.1016/j.ress.2010.01.009.

Morel, Michel, Aldo Napoli, Anne Littaye, Marie-Pierre Gleizes, Valérie Bazin, Bernard Alhadef, Christian Scapel, Bruno Leroy, Jacques Lebrevelec, and Daniel Dejardin (2009). "Surveillance et contrôle des activités des navires en mer". In: *La sécurité globale : enjeux et perspectives*. Ed. by J. Roujansky. CNRS Editions.

Mou, Jun Min, Cees van der Tak, and Han Ligteringen (2010). "Study on collision avoidance in busy waterways by using AIS data". en. In: *Ocean Engineering* 37.5-6, pp. 483–490. ISSN: 00298018. DOI: 10.1016/j.oceaneng.2010.01.012.

Napoli, Amedeo (1997). *Une introduction aux logiques de descriptions*. Research Report. INRIA. 72 pp.

Natale, Fabrizio, Maurizio Gibin, Alfredo Alessandrini, Michele Vespe, and Anton Paulrud (2015). "Mapping Fishing Effort through AIS Data". In: *PLOS ONE* 10.6. Ed. by George Tserpes. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0130746.

Naus, Krzysztof, Artur Makar, and Jaroslaw Apanowicz (2007). "Usage AIS Data for Analyzing Ship's Motion Intensity". In: *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation* 1.3, pp. 237–242. ISSN: 2083-6473.

Nepal, Sandeep (2014). "A study of Maritime Refugees And Illegal Immigrants Via Sea". MA thesis. Novia University of applied science. 32 pp.

Ng, Simon K.W., Christine Loh, Chubin Lin, Veronica Booth, Jimmy W.M. Chan, Agnes C.K. Yip, Ying Li, and Alexis K.H. Lau (2013). "Policy change driven by an AIS-assisted marine emission inventory in Hong Kong and the Pearl River Delta". In: *Atmospheric Environment* 76, pp. 102–112. ISSN: 13522310. DOI: 10.1016/j.atmosenv.2012.07.070.

Numano, M., H. Itoh, J. Futuko, and Y. Niwa (2003). *Simulation Study on Sea Traffic Control at an Intersection Utilizing Information Sharing with Automatic Identification System (AIS)*.

Oo, Kyay Mone Soe, Chaojian Shi, Hu Qinyou, and Adam Weintrit (2010). "Clustering Analysis and Identification of Marine Traffic Congested Zones at Wusongkou, Shanghai". In: *Zeszyty Naukowe Akademii Morskiej w Gdyni* 67, pp. 101–113.

Oxford (1989). *Oxford advanced learner's dictionary of current English*.

Pallotta, Giuliana, Steven Horn, Paolo Braca, and Karna Bryan (2014). "Context-enhanced vessel prediction based on Ornstein-Uhlenbeck processes using historical AIS traffic patterns: Real-world experimental results". In: *Proceedings of the 17th International Conference on Information Fusion*. Salamanca, Spain: IEEE. ISBN: 978-84-9012-355-3.

Pallotta, Giuliana and Anne-Laure Jousselme (2015). "Data-driven Detection and Context-based Classification of Maritime Anomalies". In: *Proceedings of the 18th International Conference on Information Fusion*. (July 6–9, 2015). Washington, DC, USA: IEEE.

Pallotta, Giuliana, Michele Vespe, and Karna Bryan (2013a). "Traffic Knowledge Discovery from AIS Data". In: *Proceedings of the 16th International Conference on Information Fusion*. (July 9–12, 2013). Istambul, Turkey.

— (2013b). "Traffic Route Extraction and Anomaly Detection from AIS Data". In: *Proceedings of the COST MOVE Workshop on Moving Objects at Sea*. Brest, France.

— (2013c). "Vessel Pattern Knowledge Discovery from AIS Data: A Framework for Anomaly Detection and Route Prediction". In: *Entropy* 15.6, pp. 2218–2245. ISSN: 1099-4300. DOI: 10.3390/e15062218.

Pan, Lee-Yun and Jyh-Shen Chiou (2011). "How Much Can You Trust Online Information? Cues for Perceived Trustworthiness of Consumer-generated Online Information". In: *Journal of Interactive Marketing* 25.2, pp. 67–74. ISSN: 1094-9968. DOI: 10.1016/j.intmar.2011.01.002.

Parent, Christine, Stefano Spaccapietra, Chiara Renso, Gennady Andrienko, Natalia Andrienko, Vania Bogorny, Maria Luisa Damiani, Aris Gkoulalas-Divanis, Jose Macedo, Nikos Pelekis, Yannis Theodoridis, and Zhixian Yan (2013). "Semantic Trajectories Modeling and Analysis". In: *ACM Comput. Surv.* 45.4. ISSN: 0360-0300. DOI: 10.1145/2501654.2501656.

Perez, Heather M., Roger Chang, Richard Billings, and Theodore L. Kosub (2009). *Automatic Identification Systems (AIS) Data Use in Marine Vessel Emission Estimation*.

Perkovic, Marko, Lucjan Gucma, Marcin Przywarty, Maciej Gucma, Stojan Petelin, and Peter Vidmar (2012). "Nautical Risk Assessment for LNG Operations at the Port of Koper". In: *Strojniški vestnik – Journal of Mechanical Engineering* 58.10, pp. 607–613. ISSN: 00392480. DOI: 10.5545/sv-jme.2010.265.

Pierkot, Christelle (2010). "Vers un usage éclairé de la donnée géographique". In: *Proceedings of the 10th Conférence Internationale Francophone sur l'Extraction et la Gestion de Connaissances (EGC)*. Revue des Nouvelles Technologies de l'Information. Hammamet, Tunisia.

Pierkot, Christelle, Esteban Zimányi, Yuan Lin, and Thérèse Libourel (2011). "Advocacy for External Quality in GIS". In: *Proceedings of the 4th International Conference on GeoSpatial Semantics*. GeoS'11. Brest, France: Springer-Verlag, pp. 151–165. ISBN: 978-3-642-20629-0.

Pinto, Hugo José P. B. Paulino (2016). "Generating and evaluating long-term complex maritime traffic relationships for risk assessment and mission planning via near-real-time big-data analytics". In: *Proceedings of the Maritime Knowledge Discovery and*

Anomaly Detection Workshop. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 28–30.

Plass, Simon and Romain Hermenier (2014). "Study on Worldwide Detection of AIS Signals via Airliners". In: *Proceedings of the OCEANS 2014 - TAIPEI Conference*. (Apr. 7–10, 2014). Taipei, China: Institute of Electrical and Electronics Engineers (IEEE).

Plass, Simon, Robert Poehlmann, Romain Hermenier, and Armin Dammann (2015). "Global Maritime Surveillance by Airliner-Based AIS Detection: Preliminary Analysis". In: *Journal of Navigation* 68.06, pp. 1195–1209. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463315000314.

Qu, Xiaobo, Qiang Meng, and Li Suyi (2011). "Ship collision risk assessment for the Singapore Strait". en. In: *Accident Analysis & Prevention* 43.6, pp. 2030–2036. ISSN: 00014575. DOI: 10.1016/j.aap.2011.05.022.

Ray, Cyril, Clément Iphar, Aldo Napoli, Romain Gallen, and Alain Bouju (2015). "DeAIS project: Detection of AIS Spoofing and Resulting Risks". In: *Proceedings of the OCEANS 2015 Genova Conferece*. (May 18–21, 2015). Genova, Italy: IEEE. DOI: 10.1109/OCEANS-Genova.2015.7271729.

Raymond, Eric S. (2016). *AIVDM/AIVDO protocol decoding*.

Redoutey, Martin, Eric Scotti, Christian Jensen, Cyril Ray, and Christophe Claramunt (2008). "Efficient Vessel Tracking with Accuracy Guarantees". In: *Proceedings of the W2GIS 2008 Conference: Web and Wireless Geographical Information Systems*. Ed. by Michela Bertolotto, Cyril Ray, and Xiang Li. Vol. 5373. Shanghai, China: Springer Berlin Heidelberg, pp. 140–151. ISBN: 978-3-540-89902-0 978-3-540-89903-7. DOI: 10.1007/978-3-540-89903-7_13.

Riveiro, Maria and Göran Falkman (2011). "The role of visualization and interaction in maritime anomaly detection". In: 7868. Ed. by Pak Chung Wong, Jinah Park, Ming C. Hao, Chaomei Chen, Katy Börner, David L. Kao, and Jonathan C. Roberts. DOI: 10.1117/12.871801.

Riveiro, Maria, Göran Falkman, Tom Ziemke, and Håkan Warston (2009). "VISAD: an interactive and visual analytical tool for the detection of behavioral anomalies in maritime traffic data". In: *SPIE Proceedings, Visual Analytics for Homeland Defense and Security*. Ed. by William J. Tolone and William Ribarsky. Vol. 7346. Orlando, USA. DOI: 10.1117/12.817819.

Roussey, Catherine, François Pinet, and Michel Schneider (2013). "Representations of Topological Relations Between Simple Regions in Description Logics: From Formalization to Consistency Checking". In: *International Journal of Agricultural and Environmental Information Systems (IJAEIS)* 4.2, pp. 50–69.

Roy, Jean (2008). "Anomaly detection in the maritime domain". In: *Optics and Photonics in Global Homeland Security IV*. Ed. by Craig S. Halvorson, Daniel Lehrfeld, and Theodore T. Saito. Vol. 6945. SPIE Proceedings. DOI: 10.1117/12.776230.

Roy, Jean and Michael Davenport (2009). "Categorization of Maritime Anomalies for Notification and Alerting Purpose". In: *Proceedings of the NATO Workshop on Data Fusion and Anomaly Detection for Maritime Situational Awareness*. (Sept. 15–17, 2009). La Spezia, Italy.

— (2010). "Exploitation of maritime domain ontologies for anomaly detection and threat analysis". In: *Proceedings of the 2010 International Waterside Security Conference (WSS)*. (Nov. 3–5, 2010). Carrara, Italy: IEEE. ISBN: 978-1-4244-8894-0. DOI: 10.1109/WSSC.2010.5730278.

Sagiroglu, Seref and Duygu Sinanc (2013). "Big data: A review". In: *Proceedings of the 2013 International Conference on Collaboration Technologies and Systems (CTS)*. (May 20–24, 2013). San Diego, CA, USA. DOI: 10.1109/CTS.2013.6567202.

Salmon, Loic, Cyril Ray, and Christophe Claramunt (2016). "Continuous detection of black holes for moving objects at sea". en. In: *Proceedings of the 7th ACM SIGSPATIAL International Workshop on GeoStreaming - IWGS '16*. (Oct. 31–Nov. 3, 2016). San Francisco, CA, USA: ACM Press, pp. 1–10. ISBN: 978-1-4503-4579-8. DOI: 10.1145/3003421.3003423.

Schäfer, Matthias, Vincent Lenders, and Ivan Martinovic (2013). "Experimental Analysis of Attacks on Next Generation Air Traffic Communication". In: *Applied Cryptography and Network Security*. Ed. by David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y. Vardi, Gerhard Weikum, Michael Jacobson, Michael Locasto, Payman Mohassel, and Reihaneh Safavi-Naini. Vol. 7954. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 253–271. ISBN: 978-3-642-38979-5 978-3-642-38980-1.

Schwehr, Kurt (2011). "Vessel Tracking Using the Automatic Identification System (AIS) During Emergency Response: Lessons from the Deepwater Horizon Incident". In: *Proceedings of the 13th U.S. Hydro Conference*. Tempa, Fl, USA.

Schwehr, Kurt D. and Philip A. McGillivary (2007). "Marine Ship Automatic Identification System (AIS) for Enhanced Coastal Security Capabilities: An Oil Spill Tracking Application". In: *Proceedings of the OCEANS Vancouver 2007 Conference*. (Sept. 29–Oct. 4, 2007). Vancouver, Canada: IEEE. DOI: 10.1109/OCEANS.2007.4449285.

Scott, Dana S. (1982). "Domains for denotational semantics". In: *Proceedings of the Ninth Colloquium on Automata, Languages and Programming*. (July 12–16, 1982). Ed. by Mogens Nielsen and Erik Meineche Schmidt. Aarhus, Denmark: Springer Berlin Heidelberg, pp. 577–610. ISBN: 978-3-540-39308-5. DOI: 10.1007/BFb0012801.

Serafim, Pedro (2016). "Portuguese navy perspective in maritime situational awareness – the anomaly detection". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 10–11.

Serry, Arnaud and Laurent Lévêque (2015). "Le système d'identification automatique (AIS)". In: *Netcom* 29.1/2, pp. 177–202. DOI: 10.4000/netcom.1943.

Shannon, Claude E. (1948). "A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3, pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

Shelmerdine, Richard L. (2015). "Teasing out the detail: How our understanding of marine AIS data can better inform industries, developments, and planning". en. In: *Marine Policy* 54, pp. 17–25. ISSN: 0308597X. DOI: 10.1016/j.marpol.2014.12.010.

Shibatani, Masayoshi and Theodora Bynon (1999). *Approaches to Language Theory*. Oxford University Press. 400 pp. ISBN: 978-0198238669.

SHOM (2016). *Symboles, abbréviations et termes utilisés sur les cartes marines. Symbols, abbreviations and terms used on charts*. fr. Tech. rep. Ouvrage 1D. Version 6. Service Hydrographique et Océanographique de la Marine. 124 pp.

Shu, Y., W. Daamen, H. Ligteringen, and S.P. Hoogendoorn (2013). "AIS-data analysis for vessel behavior during strong currents and during encounters in the Botlek Area in the Port of Rotterdam". In: *In Proceedings of IWNTM13: International Workshop*

on Nautical Traffic Models. (July 5–7, 2013). Delft, The Netherlands: Delft University of Technology.

Shucksmith, Rachel, Lorraine Gray, Christina Kelly, and Jacqueline F. Tweddle (2014). "Regional marine spatial planning – The data collection and mapping process". en. In: *Marine Policy* 50, pp. 1–9. ISSN: 0308597X. DOI: 10.1016/j.marpol.2014.05.012.

Siegert, Gregor, Paweł Banyś, and Frank Heymann (2016). "Improving the maritime trafffic situation assessment for a single target in a multisensor environment". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 78–82.

Silveira, P.A.M., A.P. Teixeira, and C. Guedes Soares (2013). "Use of AIS Data to Characterise Marine Traffic Patterns and Ship Collision Risk off the Coast of Portugal". In: *Journal of Navigation* 66.06, pp. 879–898. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463313000519.

Song, Su (2014). "Ship emissions inventory, social cost and eco-efficiency in Shanghai Yangshan port". In: *Atmospheric Environment* 82, pp. 288–297. ISSN: 13522310. DOI: 10.1016/j.atmosenv.2013.10.006.

Souza, Erico N. de, Kristina Boerder, Stan Matwin, and Boris Worm (2016). "Improving Fishing Pattern Detection from Satellite AIS Using Data Mining and Machine Learning". In: *PLOS ONE* 11.7. Ed. by Athanassios C. Tsikliras. ISSN: 1932-6203. DOI: 10.1371/journal.pone.0158248.

Stitt, I. P. A. (2004). "AIS and Collision Avoidance a Sense of Déjà Vu". In: *Journal of Navigation* 57.2, pp. 167–180. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463304002760.

Stoddard, M A, L Etienne, M Fournier, R Pelot, and L Beveridge (2016). "Making sense of Arctic maritime traffic using the Polar Operational Limits Assessment Risk Indexing System (POLARIS)". In: *IOP Conference Series: Earth and Environmental Science* 34.1, p. 012034. DOI: 10.1088/1755-1315/34/1/012034.

Strohmeier, Martin, Vincent Lenders, and Ivan Martinovic (2015). "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol". In: *IEEE Communications Surveys & Tutorials* 17.2, pp. 1066–1087. ISSN: 1553-877X. DOI: 10.1109/COMST.2014.2365951.

Studer, Rudi, V. Richard Benjamins, and Dieter Fensel (1998). "Knowledge Engineering: Principles and Methods". In: *Data Knowl. Eng.* 25.1-2, pp. 161–197. ISSN: 0169-023X. DOI: 10.1016/S0169-023X(97)00056-6.

Su, Chien-Min, Ki-Yin Chang, and Chih-Yung Cheng (2012). "Fuzzy Decision on Optimal Collision Avoidance Measures for Ships in Vessel Traffic Service". In: *Journal of Marine Science and Technology* 20.1, pp. 38–48.

Télégramme, Le (2011). *Coquiliers. Surveillés par satellite !* Le Télégramme Online, 30th September 2011.

Tetreault, B.J. (2005). "Use of the Automatic Identification System (AIS) for Maritime Domain Awareness (MDA)". In: *Proceedings of OCEANS 2005 MTS/IEEE*. (Sept. 17–23, 2005). Washington, DC, USA: IEEE. ISBN: 978-0-933957-34-3. DOI: 10.1109/OCEANS.2005.1639983.

The Maritime Executive (2012a). *Coast Guard Responds to Ship Collision in Caribbean Sea*. The Maritime Executive Online, 12th March 2012.

— (2012b). *Iran, Tanzania and Falsifying AIS signals to Trade with Syria*.

The Maritime Executive (2015). *SE Asia Tanker Hijacks Rose, Global Piracy Drops*. The Maritime Executive Online, 14th January 2015.

The Telegraph (2012). *Costa Concordia: will it sink the cruise industry?* The Telegraph Online, 16th January 2012, by Jane Archer.

Tsou, Ming-Cheng and Chao-Kuang Hsueh (2010). "The study of ship collision avoidance route planning by ant colony algorithm". In: *Journal of Marine Science and Technology* 18.5, pp. 746–756.

Tunaley, James K.E. (2013). "Utility of Various AIS Messages for Maritime Awareness". In: *8th ASAR Workshop*. Longueuil, Canada.

United Nations (1958). *Convention on the High Seas*.

UNODC (1988). *United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances*. Tech. rep. United Nations Office on Drugs and Crime. 31 pp.

— (2005). *2005 World Drug Report*. Tech. rep. United Nations Office on Drugs and Crime. 182 pp.

— (2013). *The Illicit Trafficking of Counterfeit Goods and Transnational Organized Crime*. Tech. rep. United Nations Office on Drugs and Crime. 10 pp.

USCG (2010). *Caution to AIS users. Marine Safety Alert*. United States Coast Guards.

Vanneschi, Leonardo, Mauro Castelli, Ernesto Costa, Alessandro Re, Henrique Vaz, Victor Lobo, and Paulo Urbano (2015). "Improving Maritime Awareness with Semantic Genetic Programming and Linear Scaling: Prediction of Vessels Position Based on AIS Data". In: *Applications of Evolutionary Computation*. Ed. by Antonio M. Mora and Giovanni Squillero. Vol. 9028. Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 732–744. ISBN: 978-3-319-16548-6 978-3-319-16549-3. DOI: 10.1007/978-3-319-16549-3_59.

Vasseur, Bérangère, Robert Jeansoulin, Rodolphe Devillers, and A. U. Frank (2005). "Evaluation de la qualité externe de l'information géographique : une approche ontologique". In: *Qualité de l'information géographique : traité IGAT*. Ed. by Rodolphe Devillers and Robert Jeansoulin. Hermès Science, pp. 285–301.

Vespe, Michele, Harm Greidanus, and Marlene Alvarez Alvarez (2015). "The declining impact of piracy on maritime transport in the Indian Ocean: Statistical analysis of 5-year vessel tracking data". In: *Marine Policy* 59, pp. 9–15. ISSN: 0308597X. DOI: 10.1016/j.marpol.2015.04.018.

Vodas, Marios, Nikos Pelekis, Yannis Theodoridis, Cyril Ray, Vangelis Karkaletsis, Sergios Petridis, and Anastasia Miliou (2013). "Efficient AIS Data Processing for Environmentally Safe Shipping". In: *SPOUDAI - Journal of Economics and Business* 63.3-4, pp. 181–190.

Voinov, Sergey, Egbert Schwarz, and Detmar Krause (2016). "Automated Processing system for SAR target detection and identification in near real time applications for maritime situational awareness". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 66–68.

Vu Trong, Thu, Tri Dinh Quoc, Thang Dao Van, Hung Pham Quang, and Hugo Nguyen (2011). "Constellation of small quick-launch and self-deorbiting nano-satellites with AIS receivers for global ship traffic monitoring". In: *Proceedings of the 2nd Nano-Satellite Symposium*. (Mar. 14–16, 2011). Tokyo, Japan.

Wahl, Terje, Gudrun K. Høye, Aleksander Lyngvi, and Bjørn T. Narheim (2005). "New possible roles of small satellites in maritime surveillance". In: *Acta Astronautica* 56.1-2, pp. 273–277. ISSN: 00945765. DOI: 10.1016/j.actaastro.2004.09.025.

Wang, Richard Y., M.P. Reddy, and Henry B. Kon (1995). "Toward quality data: An attribute-based approach". In: *Decision Support Systems* 13.3–4. Information technologies and systems, pp. 349–372. ISSN: 0167-9236. DOI: 10.1016/0167-9236(93)E0050-N.

Wang, Richard Y. and Diane M. Strong (1996). "Beyond Accuracy: What Data Quality Means to Data Consumers". In: *Journal of Management Information Systems* 12.4, pp. 5–33. ISSN: 0742-1222. DOI: 10.1080/07421222.1996.11518099.

Wang, Ting, Mark Bebbington, and David Harte (2010). "A comparative study of coherence, mutual information and cross-intensity models". In: *International Journal of Information and Systems Sciences* 6.1, pp. 49–60.

Wang, Yang, Jinfen Zhang, Xianqiao Chen, Xiumin Chu, and Xinping Yan (2013). "A spatial–temporal forensic analysis for inland–water ship collisions using AIS data". In: *Safety Science* 57, pp. 187–202. ISSN: 09257535. DOI: 10.1016/j.ssci.2013.02.006.

Weng, Jinxian, Qiang Meng, and Xiaobo Qu (2012). "Vessel Collision Frequency Estimation in the Singapore Strait". In: *Journal of Navigation* 65.02, pp. 207–221. ISSN: 0373-4633, 1469-7785. DOI: 10.1017/S0373463311000683.

Wiley, David N., Michael Thompson, Richard M. Pace, and Jake Levenson (2011). "Modeling speed restrictions to mitigate lethal collisions between ships and whales in the Stellwagen Bank National Marine Sanctuary, USA". In: *Biological Conservation* 144.9, pp. 2377–2381. ISSN: 00063207. DOI: 10.1016/j.biocon.2011.05.007.

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

Winther, Morten, Jesper H. Christensen, Marlene S. Plejdrup, Erik S. Ravn, Ómar F. Eriksson, and Hans Otto Kristensen (2014). "Emission inventories for ships in the arctic based on satellite sampled AIS data". In: *Atmospheric Environment* 91. ISSN: 13522310. DOI: 10.1016/j.atmosenv.2014.03.006.

Wolton, Dominique (2004). "Information et communication : Dix chantiers scientifiques, culturels et politiques". In: *Hermès* 38. ISSN: 1963-1006, 0767-9513. DOI: 10.4267/2042/9445.

Xiao, Fangliang, Han Ligteringen, Coen van Gulijk, and Ben Ale (2015). "Comparison study on AIS data of ship traffic behavior". In: *Ocean Engineering* 95, pp. 84–93. ISSN: 0029-8018. DOI: 10.1016/j.oceaneng.2014.11.020.

Xiao, Fanglinag, Han Ligteringen, Coen van Gulijk, and Ben Ale (2012). "AIS Data Analysis for Realistic Ship Traffic Simulation Model". In: *Proceedings of IWNTM'2012*. Shanghai, China.

Yaghoubi Shahir, Hamed, Uwe Glasser, Narek Nalbandyan, and Hans Wehn (2014). "Maritime Situation Analysis: A Multi-vessel Interaction and Anomaly Detection Framework". In: *Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference*. (Sept. 24–26, 2014). The Hague, The Netherlands: IEEE, pp. 192–199. ISBN: 978-1-4799-6364-5 978-1-4799-6363-8. DOI: 10.1109/JISIC.2014.36.

Yan, Zhixian, Jose Macedo, Christine Parent, and Stefano Spaccapietra (2008). "Trajectory Ontologies and Queries". In: *Transactions in GIS* 12, pp. 75–91. ISSN: 13611682, 14679671. DOI: 10.1111/j.1467-9671.2008.01137.x.

Yau, P.S., S.C. Lee, James J. Corbett, Chengfeng Wang, Y. Cheng, and K.F. Ho (2012). "Estimation of exhaust emission from ocean-going vessels in Hong Kong". en. In: *Science of The Total Environment* 431, pp. 299–306. ISSN: 00489697. DOI: 10.1016/j.scitotenv.2012.03.092.

Zhang, Weibin, Floris Goerlandt, Jakub Montewka, and Pentti Kujala (2015). "A method for detecting possible near miss ship collisions from AIS data". In: *Ocean Engineering* 107, pp. 60–69. ISSN: 00298018. DOI: 10.1016/j.oceaneng.2015.07.046.

Zheng, Bin, Jinbiao Chen, Shaosheng Xia, and Yongxing Jin (2008). "Data Analysis of Vessel Traffic Flow Using Clustering Algorithms". In: *Proceedings of the 2008 International Conference on Intelligent Computation Technology and Automation (ICICTA)*. (Oct. 20–22, 2008). Changsa, China: Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/ICICTA.2008.127.

Zissis, Dimitrios (2016). "Detecting anomalies in streams of AIS vessel data". In: *Proceedings of the Maritime Knowledge Discovery and Anomaly Detection Workshop*. (July 5–6, 2016). Ed. by Michele Vespe and Fabio Mazzarella. JRC Conference and Workshop Reports. Ispra, Italy, pp. 36–38.

Zouaoui-Elloumi, S. (2012). "Reconnaissance de comportements de navires dans une zone portuaire sensible par approches probabiliste et événementielle : Application au Grand Port Maritime de Marseille". PhD thesis. Mines ParisTech.

Résumé

Il existe différents systèmes de localisation de navires en mer qui favorisent une aide à la navigation et une sécurisation du trafic maritime. Ces systèmes sont également utilisés en tant qu'outils de surveillance et d'aide à la décision par les centres de surveillance basés à terre. Le Système d'Identification Automatique (AIS) déployé par l'Organisation Maritime Internationale, bien qu'étant le système de localisation de navires le plus utilisé de nos jours, est faiblement sécurisé. Cette vulnérabilité est illustrée par des cas réels et détectés tels que des usurpations d'identité ou des disparitions volontaires de navires qui sont sources de risques pour les navires, les infrastructures offshores et côtières et l'environnement.

Nous proposons dans cette thèse une démarche méthodologique d'analyse et d'évaluation des messages AIS fondée sur les dimensions de la qualité de la donnée, dont l'intégrité considérée comme la plus importante de ces dimensions. Du fait de la structure complexe de l'AIS, une liste d'indicateurs a été établie, afin d'évaluer l'intégrité de la donnée, sa conformité avec les spécifications techniques du système et la cohérence des champs des messages entre eux et au sein d'un seul ou plusieurs messages. Notre démarche repose également sur l'usage d'informations additionnelles telles que des données géographiques ou des registres de navires afin d'évaluer la véracité et l'authenticité d'un message AIS et de son expéditeur.

Enfin, une évaluation des risques associés est proposée, permettant une meilleure compréhension de la situation maritime ainsi que l'établissement de liens de causalité entre les vulnérabilités du système et les risques relevant de la sécurité et sûreté de la navigation maritime.

Mots Clés

Système de géolocalisation, Système d'identification Automatique, évaluation de l'intégrité, risques maritimes, falsification de données, système d'aide à la décision

Abstract

At sea, various localisation systems enable vessels to be aware of their environment, fostering aid to navigation and the securing of maritime traffic. Those systems are also used as surveillance and decision support tools by coastal authorities. The Automatic Identification System (AIS), created by the International Maritime Organisation, albeit being the most used system for vessel localisation, is weakly secured. This vulnerability is illustrated by real and detected cases of identity theft or voluntary vessel disappearances, which are a threat to the vessels, the offshore and coastal infrastructures and the environment.

In this thesis, we propose a methodological approach for the analysis and assessment of AIS messages based on data quality dimensions, including integrity which has been discriminated as the most important of those dimensions in our study. As the structure of AIS data is complex, a list of integrity items have been established, their purpose being to assess the consistency of the data within the data fields with the technical specifications of the system and the consistency of the data fields within themselves in a message and between the different messages. Our method also relies on the use of additional data (such as geographical data or fleet registers), providing additional information to assess the truthfulness and the genuineness of an AIS message and its sender.

Last, an assessment of associated risks is proposed, allowing a better comprehension of the maritime situation and the establishment of links between the vulnerabilities caused by the weaknesses of the system and the maritime risks related to the safety and security of maritime navigation.

Keywords

Geolocation system, Automatic Identification System, integrity assessment, maritime risks, data falsification, decision support system