Génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals

Clet Boudehenn

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

THÈSE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPÉRIEURE MINES-TÉLÉCOM ATLANTIQUE
BRETAGNE PAYS DE LA LOIRE - IMT ATLANTIQUE

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : INFORMATIQUE

Par

Clet BOUDEHENN

Génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals

Thèse présentée et soutenue à l'Ecole Navale, Lanvéoc, le 16/12/2022
Unité de recherche : Lab-STICC UMR CNRS 6285
Thèse financée et préparée au sein de la Chaire de Cyberdéfense des Systèmes Navals
Thèse N° : 2022IMTA0336

Rapporteurs avant soutenance :

Rapporteur :	Hichem SNOUSSI	Professeur des Universités, Université de Technologie de Troyes
Rapporteur :	Nabil TABBANE	Professeur (HdR), SupCom de Tunis

Composition du Jury :

Président du Jury :	Thierry CHONAVEL	Professeur (HdR), IMT-Atlantique
Examinateur :	Julien FRANCQ	Responsable Recherche & Innovation en Cybersécurité (Dr.), Naval Group
Examinateur :	Kavé SALAMATIAN	Professeur des Universités, Polytech Annecy-Chambery
Examinateur :	Hichem SNOUSSI	Professeur des Universités, Université de Technologie de Troyes
Examinateur :	Nabil TABBANE	Professeur (HdR), SupCom de Tunis

Directeur de thèse :	Abdel BOUDRAA	Professeur des Universités, Ecole Navale/ENSAM
Co-directeur de thèse :	Yvon KERMARREC	Professeur (HdR), IMT-Atlantique
Encadrant de thèse :	Jean-Christophe CEXUS	Enseignant-Chercheur, ENSTA-Bretagne

Invités

Laurent AUFRECHTER	Architecte en Cybersécurité, Thales
Marc PENNAMEN	Responsable développement des offres et projets cybersécurité, Thales

Table des matières

Table des figures

Liste des tableaux

Remerciements

Le travail, quand il nous tient à cœur, n'est jamais vraiment terminé, encore plus quand on travaille dans la recherche, mais je préfère tout de même y consacrer cette page de remerciement très imparfaite pour l'utiliser comme point d'honneur sur l'étendue de ces travaux et ainsi de tourner plus sereinement la page.

Je voudrais tout d'abord remercier mon directeur de thèse, Abdel BOUDRAA, Professeur des Universités à l'IRENav (Institut de Recherche de l'École Navale), mon encadrant académique, Jean-Christophe CEXUS (Ingénieur Divisionaire d'État et Enseignant-Chercheur à l'ENSTA-Bretagne) ainsi que mon encadrant industriel Laurent AUFRECHTER (Architectre en Cybersécurité à Thales GTX SAS Paris) qui m'ont tout les trois accompagné comme il se doit et grandement conseillé grâce à leur expérience respective académique et industrielle. Vous avez largement contribué à ce que cette thèse soit ce qu'elle est aujourd'hui et pour cela : MERCI.

Par ailleurs et de façon moins formelle (et sans aucune quelconque forme de retenue) je voudrais également et très sincèrement remercier toutes les personnes que j'ai pu côtoyer pendant toute la durée de ces travaux de recherches :

David, merci pour tout, pour ton accompagnement au quotidien, pour les opportunités dont tu nous as fait largement profiter, pour m'avoir laissé carte blanche sur mes expérimentations, de m'avoir accordé ta confiance pour toutes mes propositions, pour tes conseils et histoires au quotidien qui ont été plus que formateurs pendant toute la durée des travaux et sans oublier... LES BLAGUES ! beaucoup de choses ont été possibles grâce à toi. World's best boss mug is deserved.

Olivier, je pense que tu sais à quel point je suis reconnaissant de tout ce que tu as fait pour moi pendant ces travaux. Merci d'avoir su me guider comme tu l'as fait pendant ces quelques années, c'était un réel plaisir de travailler avec toi et tu as su donner une orientation vraiment pertinente de mes travaux de recherches de par ton expérience opérationnelle et surtout humaine.

Jean-Christophe, j'ai adoré travailler avec toi et t'avoir comme encadrant. Je sais que tu préfères que je sois concis, mais pour la dernière fois, je vais être redondant :). Sans toi ça n'aurait pas été la même tisane, tu as su instaurer un confort et une bienveillance qui n'a fait que m'aider à

surmonter les nombreux obstacles d'un tel projet. Sans parler du soutien moral de la dernière ligne droite. Au plaisir de retravailler ensemble dans d'autres contextes.

Même si ce n'est jamais facile de quitter une équipe dans laquelle on se sent bien, je voudrais également remercier tout le personnel de la Chaire : Maxence, mon partenaire d'escape game favori et acolyte des études depuis de longues années. Un grand merci pour tout le support technique et moral dont tu as fait preuve pendant ces quelques années passées à la Chaire ensemble et surtout pendant toutes ces années de travail collaboratif durant ces nombreuses années d'amitiés que l'on a au compteur. Un énorme merci aussi à Nicolas, Douraid, Paul, Mael pour leur bonne humeur quotidienne, c'était l'éclate de travailler avec vous pendant toutes ces années, si l'ambiance de travail était aussi bien, c'est grâce à vous (p'tit Warzone ?). Merci à Mickaël et Sebastien d'avoir assuré tous les besoins et supports techniques dont j'avais besoin pour mes recherches et pour les partages de connaissance et discussions tous domaines confondus.

Merci aussi aux plus anciens doctorants de la Chaire : Bastien, Etienne, Pedro pour tous vos retours et vos conseils plus avisés les uns que les autres. François, évidement, merci pour toutes ces discussions, pour ton soutien et pour ta vision des événements plus que clairvoyante. Erwan et Thomas, merci pour la confiance que vous m'avez accordée, pour tous ces échanges et opportunités.

Pour finir je voudrais également remercier toutes les personnes qui m'ont moralement soutenu pendant cet exercice : ma femme Sandra, à la fois ma meilleure amie et confidente du soir depuis plus de 10 ans, qui à largement su relever le défi de me soutenir et m'accompagner de façon la plus bienveillante possible pendant toute la durée de ce projet qui me suit et me soutient dans tous les autres (aussi ambitieux et chronophages qu'ils soient). Promis un jour je me calme, mais pas tout de suite :). Evidemment, ma mère, ma sœur et mon père sans qui je ne serais pas ce que je suis aujourd'hui, pour leur soutien et leur bienveillance inconditionnelle dans chacun de mes projets.

Ma dernière pensée va tout droit à mes amis, qui ont su me soutenir tout au long de ces 4 ans chacun à leur manière et n'ont jamais douté que j'allais y arriver. Apparemment vous connaissiez déjà la fin du film ? J'avoue avoir peut-être eu potentiellement quelques doutes sur le déroulé de l'intrigue... :).

Merci beaucoup à la DGA de m'avoir permis de finir cette thèse dans d'excellentes conditions et pour sa confiance dans les projets à venir.

Cette thèse est dédiée à toutes les personnes qui m'ont soutenu pendant cette épreuve à la fois humaine et professionnelle, mais également à ma nièce, Jamie.

Chapitre I

Introduction

Sommaire

I.1 Problématiques et motivations

En mars 2021 le monde essaye tant bien que mal de se remettre progressivement de la pandémie de Covid-19, qui a débutée environ un an plus tôt. Les économies du monde entier se sont fragilisées et le regain de croissance nécessite d'accroître les échanges internationaux afin de relancer les machines des industries et des plans financiers. Si le secteur aéronautique a été drastiquement impacté avec de nombreux avions cloués au sol pendant cette période de trouble, l'industrie maritime a, elle, connue une croissance considérable de ses échanges pour assurer le commerce international. Cependant, dans la nuit du 23 au 24 ars 2021, l'un des plus grands porte-conteneurs du monde, nommé *l'Ever Given* (400m de long, 20124 EVP [1]) de l'armateur *Evergreen Marine Corporation*, se déporte alors qu'il vient de franchir l'entrée sud du canal de Suez. Il s'enfonce profondément dans la berge avant d'entraver totalement le canal. Ainsi, c'est tout le trafic qui se trouve bloqué pendant près de 6 jours avec des centaines de navires de part et d'autre du canal. Chaque journée écoulée, c'est 9.6 milliards de dollars de marchandises qui sont retardées voire perdues. Au vu de l'ampleur que prenait l'incident au fil des jours, certaines compagnies préfèrent prendre la décision économiquement difficile de détourner leurs transporteurs de leur route initiale, au risque de générer des délais de livraison plus importants. Au final, cet incident impactera 10% du commerce de marchandise maritime mondial et aura fait perdre plus de 900 millions de dollars à l'armateur *EverGreen* ainsi qu'à l'Égypte, dont les sources de revenus générées par le canal représentent une

1. *EVP* : Equivalent Vingt Pieds, 1 EVP correspond à 1 conteneur de 20 pieds de long (environ 6 mètres).

part financière non négligeable pour l'économie nationale [2].

Les rapports de cet incident n'ont pas mis en cause une attaque intentionnelle ou malveillante, néanmoins il est tout fait possible d'envisager la possibilité qu'un acteur malveillant orchestre un incident similaire via par exemple l'utilisation de cyberattaques. L'hypothèse d'imaginer qu'un arrêt momentané, mais programmé, des systèmes de propulsion et la diffusion d'informations volontairement erronées sur les systèmes de navigation provoquant le même type d'incident ne paraît plus insensée. Ainsi, cet évènement illustre que la prise en compte de ces défis complexes exposés par des menaces et vulnérabilités de cybersécurité qui planent sur le monde maritime doivent devenir d'importantes préoccupations pour les décideurs tant sur les plans économiques que géopolitiques. Il n'est donc pas anodin de penser que des cyberattaquants pourraient tirer profit de ces vulnérabilités mettant en lumière les fragilités des économies mondialisées interdépendantes qui sont parfois prises en otage par les nouvelles technologies environnantes. De par sa numérisation croissante, le monde maritime n'est pas en reste en ce qui concerne les menaces de cybersécurité qui planent, ce qui fait de ce domaine un enjeu stratégique de premier plan.

Les révolutions technologiques de ces dernières années dans le domaine industriel ont permis d'améliorer considérablement les capacités de production, de rendement, d'administration et d'opérations de différents secteurs d'activités. Pour répondre aux besoins et aux évolutions de nos sociétés et économies modernes, de nouveaux moyens de communication s'imposent en mettant directement en lien les Technologies de l'Information (IT) et les Technologies Opérationnelles (OT). Mais cette révolution n'est pas sans risque. Les vulnérabilités associées aux systèmes informatiques peuvent maintenant avoir un impact direct sur ce type d'appareils que l'on peut considérer comme sensibles de par leur importance au sein de l'architecture globale des infrastructures sensibles. Faisant partie intégrante du réseau, ces systèmes, ne bénéficiant pas toujours de leur rempart technologique initial, sont devenus beaucoup plus facilement accessibles aux cybermenaces propres à ces domaines dont la surface d'attaque s'est considérablement étendue. Il est aujourd'hui possible qu'un acteur malveillant puisse en prendre le contrôle pour effectuer des actions ayant une incidence beaucoup plus importante comparée aux systèmes informatiques classiques. Ces risques encourus peuvent avoir des impacts sur la sécurité de vies humaines (centrale électrique, gare, aéroport, télécoms, port, barrage, etc.) mais aussi provoquer de graves dommages à l'environnement (centrales nucléaires, pipeline pétrolier, usine de produits chimiques, etc.).

La spécificité de ces systèmes avec leur composante et comportement physique ne doit pas être négligée. Comme tant d'autres vulnérabilités technologiques, les infrastructures de cybersécurité sont souvent issues d'une réflexion postérieure plutôt qu'une prestation assumée pendant les phases de conception, ce qui implique certaines fragilités. L'une des spécificités informatiques des systèmes navals étant l'intégration quasi systématique de systèmes de contrôle industriels (*Industrial Control*

2. www.bloomberg.com/news/features/2021-06-24/how-the-billion-dollar-ever-given-cargo-ship-got-stuck-in-the-suez-canal

Systems - ICS) et de systèmes de navigation. Ils ne sont pas non plus protégés et la prise en compte des menaces que peut faire face un navire dans sa globalité est trop souvent insoupçonnée.

De nos jours, le monde maritime englobe et transporte plus de 90% du trafic de fret mondial (en termes de volume) et 80% (en termes de valeur), représentant chaque seconde environ 290 tonnes de marchandises et fait de la mer le théâtre le plus important pour les échanges internationaux. Comme les autres secteurs, celui du maritime est confronté à cette évolution continue vers la numérisation technologique. Un navire construit au cours de la dernière décennie présente toutes les caractéristiques d'un système d'information complet combiné à des automates programmables, des capteurs numériques, des réseaux et ordinateurs pour assurer la navigation.

Parallèlement, les cybermenaces et autres menaces électroniques sont particulièrement importantes dans ce domaine et se sont développées au cours de la dernière décennie. Le nombre de cyberattaques visant ce type de système à bord augmente, notamment via l'émergence d'acteurs criminels (étatiques ou non) qui y trouvent un réel intérêt en profitant de ces déficiences. Le sabotage tactique et stratégique de ces systèmes devient presque monnaie courante et si peu coûteuse qu'il n'est plus si difficile pour un adversaire de réaliser ces actions malveillantes. Il est même hautement plausible que des régimes hostiles et des acteurs étatiques (bénéficiant d'un budget quasi illimité pour ce genre d'exactions) puissent se servir de ces faiblesses pour créer des situations dans des zones économiques sensibles et/ou stratégiques.

I.2 Objectifs et Questions de Recherches

Les travaux de cette thèse (Fig. I.1) ont été réalisés dans le cadre de la Chaire de Cyberdéfense des Systèmes navals[3] avec comme problématique centrale **celle de la génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals. Question qui s'avère être au cœur de nos travaux**. Cette problématique comprend ; d'une part, la génération de jeux de données via l'élaboration d'une plate-forme de simulation réaliste et représentative des capacités fonctionnelles et opérationnelles d'un navire ; d'autre part, via des outils adaptés, la volonté de proposer des améliorations hybrides des systèmes de détection d'intrusion actuels permettant ainsi l'analyse et la détection d'anomalies dans les systèmes navals basées sur leurs comportements.

Ainsi, l'objectif principal de cette thèse est de proposer une méthodologie permettant de générer, d'analyser et de détecter les anomalies dans des systèmes spécifiques tels que les systèmes navals (Fig. I.1).
Pour ce faire, **une partie de cette thèse a consisté en un volet expérimental**. Nous avons

3. Cette chaire industrielle, créée en 2014, est le fruit de collaborations entre plusieurs organismes : des Écoles d'ingénieurs (École Navale, IMT-Atlantique, ENSTA-Bretagne) et aussi d'industriels de Défense (Naval Group et Thales). Elle bénéficie du soutien de la Région Bretagne.

activement participé à l'élaboration et au développement d'une plate-forme de simulation permettant de reproduire les principes de fonctionnement d'un navire. Cette plate-forme expérimentale [4], véritable champ de tir numérique et terrain de jeu virtuel, permet de reproduire les composantes fonctionnelles et opérationnelles que l'on peut retrouver sur un navire. La participation, très active à cette plate-forme et le temps consacré représentent sans conteste l'un des points centraux de nos travaux. Afin de pouvoir réaliser la détection d'anomalies dans ce type de systèmes, il est impératif d'avoir des données exploitables et relativement conséquentes. Or, pour des raisons évidentes de confidentialité industrielle, de telles données demeurent très peu disponibles ou accessibles, voire malheureusement inexistantes, dans la communauté scientifique.
Par la suite, nous avons mis en place un certain nombre de méthodologies pour l'extraction et l'analyse des données issues de cette plate-forme. Opérant dans plusieurs domaines d'applications, l'un des objectifs est de mettre en place des méthodologies de détection d'anomalies dans les ICS et les systèmes de navigation. De cette façon il est possible d'analyser, de détecter et de classifier les dysfonctionnements et les cyberattaques potentielles qui peuvent toucher et impacter ce genre de systèmes tout en proposant des prototypes de contre-mesures visant à limiter les incidents.

Pour répondre à cette problématique, trois Questions de Recherche ***QR*** et une Question de Développement ***QD*** ont été identifiées auxquelles nous allons tenter de répondre tout au long de ce manuscrit.

1. **QR1** : **comment générer des données crédibles et mener des attaques réalistes permettant de valider les travaux connexes ?** Le premier objectif de cette thèse est de générer des données réalistes et adaptées à nos problématiques cybernétiques. Pour ce faire, il sera question d'identifier quels sont les systèmes à mettre en place et à développer afin de correspondre à une architecture fiable et surtout proche de celle d'un navire disposant de systèmes de télécommunications spécifiques. Pour cela, il est nécessaire de participer à l'élaboration d'une plate-forme de simulation représentative d'un navire. Cela servira de base solide pour élaborer des scénarios crédibles d'incidents cyber, de collecter des données réalistes et exploitables, de proposer des solutions de cybersécurité, etc.
2. **QR2** : **quels sont les marqueurs significatifs des attaques générées ?** L'un des verrous scientifiques qui peut ressortir avec ce genre de plate-forme de simulation est de comprendre les incidents cyber qui ont eu lieu dans un contexte maritime et être capable de les reproduire via des scénarios réalistes. L'identification de marqueurs d'attaques réelles ou des menaces propres au domaine maritime peut donc permettre d'obtenir des scénarios aux services d'analyses futures. Les marqueurs ici représentent finalement les caractéristiques propres permettant de définir s'il s'agit d'un type d'attaque précise et de les classer.
3. **QR3** : **comment détecter les anomalies dans ce contexte maritime ?** De par leurs

4. Plate-forme financée par un Contrat de Plan État-Région (CPER).

systèmes vieillissants, beaucoup de navires utilisent des standards et protocoles parfois peu sécurisés à leur conception, qui ne sont pas voués à évoluer dans le temps et donc vulnérables à une multitude d'attaques. Dans ce contexte et au regard des données générées et des scénarios proposés par la plate-forme de simulation, le but ici est de proposer des méthodes de détection d'anomalie dédiées aux ICS et aux systèmes de navigation en se basant sur leurs protocoles respectif de communication.

4. **QD1 : en lien avec les Questions de Recherche, quels outils informatiques et matériels peuvent être développés pour faciliter la génération de données et de scénarios ainsi que la détection d'anomalies ?** De tels outils permettront d'automatiser la génération de données issues de contextes réalistes. L'automatisation d'injections de cyberattaques sera dédiée aux différents scénarios et facilitera la détection d'anomalies dans les systèmes cybernétiques navals.

La figure Fig. I.1 permet de schématiser les liens entre les différents thèmes de cette thèse et le tableau de la Fig. I.2 indique les correspondances entre les différentes questions de Recherches et les chapitres associés.

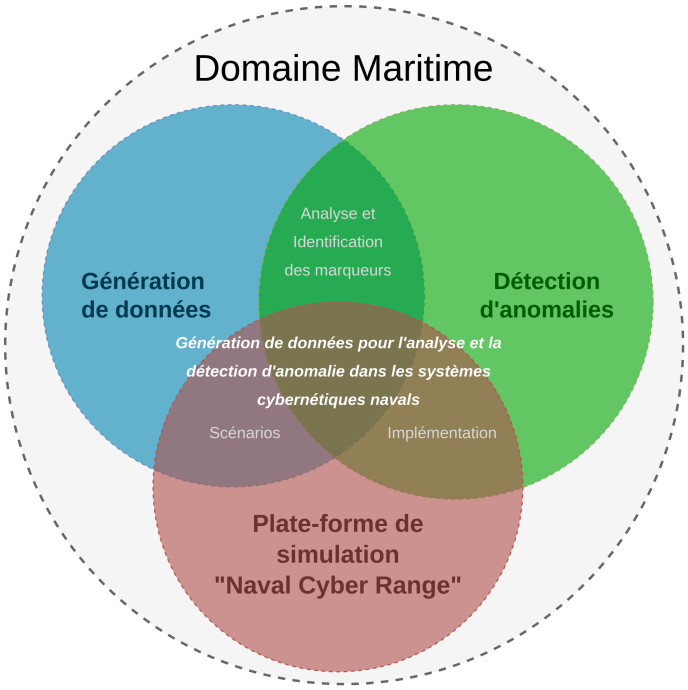


FIGURE I.1 – Domaines et problématiques étudiés dans cette thèse.

Ces travaux font suite, en particulier, de ceux de la thèse d'Olivier Jacq [62] réalisée au sein de la Chaire portant sur l'impact de la cyber dans le domaine maritime en instaurant le principe de *Maritime Cyber Situational Awareness*. Au cours de cette étude, O. Jacq a démontré qu'il était possible de proposer une modélisation numérique d'un navire en vue de problématiques cyber (dé-

Correspondance : Question de Recherche / Chapitre					
	Chap. II	Chap. III	Chap. IV	Chap. V	Chap. VI
QR I	■	■	■		
QR II			■	■	
QD I				■	
QR III		■			■

FIGURE I.2 – Tableau de correspondances entre les Questions de Recherche et les Chapitres.

fense, attaques, résiliences, etc.) pouvant amener à des situations dangereuses (piratage, échouage, pannes, etc.). Les situations mises en évidence étaient générées par la réponse d'un opérateur à une dérive dite « technique » (dérives de machines, matières premières, produits, déchets, etc.). Il s'agit dans cette thèse de poursuivre une partie de ces travaux afin de proposer d'autres solutions de cybersécurité spécifiques à l'environnement d'un navire.

Les contributions sont les suivantes :

1. nous avons développé et mis en œuvre une nouvelle stratégie pour générer des données des flux cybernétiques afin d'illustrer les vulnérabilités des systèmes maritimes via la mise en place de nouveaux capteurs. Pour commencer, de nouvelles sondes au sein de l'architecture de la plate-forme ont été mises en place. Ensuite, une méthode de détection d'anomalie basée sur l'opérateur d'énergie de *Teager-Kaiser* est développée pour détecter ces vulnérabilités en analysant les séries temporelles des données collectées. Des simulations de scénarios de cyberattaques sont proposées pour valider la nouvelle approche dans les systèmes navals. Les résultats obtenus montrent l'intérêt de la stratégie de détection d'anomalies basée sur la corrélation des données.
2. nous avons proposé un concept nouveau afin de visualiser et de détecter les cyberattaques de navigation avancées sur les systèmes maritimes en utilisant l'analyse contextuelle des données spécifiques aux systèmes de navigation. Une stratégie est élaborée pour améliorer la détection des attaques sur les systèmes de navigation (brouillage, leurrage, etc), évaluer les impacts physiques possibles à bord et permettre une aide à la décision pour les opérateurs. Stratégie d'ailleurs testée en condition réelle sur de vrais systèmes de navigation à bord d'un bateau pneumatique facilement manœuvrable pour ce type d'observation. Cette expérience apporte une preuve de concept sur la détection en temps réel de leurrage et de brouillage des systèmes de positionnement par satellites en se basant sur le flux des protocoles de communications NMEA des systèmes de navigation.
3. nous avons généré des données réalistes via le développement d'un prototype embarqué. Ce système autonome, placé sur un navire, est capable de collecter des données de navigation en temps réel sans utiliser de moyens propriétaires et restrictifs le rendant pleinement dédié à la

recherche scientifique. Dans notre cas, ce type de données, difficiles à collecter dans un contexte normal, alimente en continu la plate-forme cybernétique navale reproduisant les systèmes fonctionnels et opérationnels d'un navire. Ce prototype permet de reproduire la cinématique d'un navire dans différents contextes (manœuvres spécifiques,longue route, amarrage, etc.) afin d'établir des scénarios grâce à la génération et l'analyse de jeux de données réalistes. Comme tous les systèmes sont interconnectés et corrélés entre eux, cette plate-forme permet également de voir l'impact de différentes cyberattaques lorsque des composants à caractères cruciaux sont compromis ou endommagés. En complément de ce système embarqué dédié à la collection de données, des outils ont été développés. Le premier est dédié à la génération automatique de cyberattaques sur les données de navigation. Le second est une proposition automatisée de détection d'anomalies en temps réel pour aider la prise de décision des opérateurs.

4. nous avons développé un outil dédié à l'injection d'anomalies spécifiques aux protocoles utilisés dans les systèmes de navigation en exploitant leurs vulnérabilités. Ces protocoles n'étant pas protégés contre les cyberattaques, il est en effet aisé de forger soit même de fausses données pour leurrer les systèmes de navigation sans qu'aucune alerte ne soit renseignée. L'outil développé permet de générer des jeux de données (ou datasets) suivant des scénarios d'attaques basés sur les données précédemment collectées par notre système d'acquisition. Ces datasets, composés de cyberattaques et destinés à être rendus public au profit de la communauté scientifique, peuvent être utilisées pour tester et améliorer les systèmes de détection d'intrusion classiques, actuellement non exploités sur les systèmes de navigation au même titre que les réseaux informatiques traditionnels. Nous proposons ainsi une méthode de détection d'anomalie en utilisant des approches d'apprentissage automatique exploitant des caractéristiques nouvelles (spécifiques aux systèmes de navigation) définies grâce aux données générées.

l'ensemble des travaux ont permis la publication de trois articles dans des conférences internationales avec actes et comité de lecture, un article dans une revue à comité de lecture en cours de révision ainsi que l'encadrement de stages (1 PFE et 1 Master II) :

[RI1] **C. Boudehenn**, J.C. Cexus and A.O. Boudraa, "Realistic datasets generation and anomaly detection in navigation Systems : A naval case study," *Expert Systems with Applications*, en révision.

[CI1] **C. Boudehenn**, J.C. Cexus and A.O. Boudraa, "A data extraction method in naval systems," *Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1-4, 2020.

[CI2] **C. Boudehenn**, O. Jacq, M. Lannuzel, J.C Cexus and A.O. Boudraa, "Navigation anomaly detection : An added value for cybersituationnal awareness", *Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1-4, 2021.

[CI3] **C. Boudehenn**, J.C Cexus, M. Lannuzel, O. Jacq, D. Brosset and A.O. Boudraa, "Hollistic approach of integrated navigation equipment for cybersecurity at sea", *Int. Conf. Cyber Situational*

Awareness, Data Analytics and Assessment (CyberSA), pp. 1-4, 2022.

[P1] **Ramla Ben Abdelkader** - Master recherche II (ENSTA Bretagne) : Acquisition et analyse de falsification de signaux GNSS, 60 pages, 2021

[P2] **EV1 Guillaume** et **EV1 Théophile** - PFE (Ecole Navale) : Détection temps-réel d'anomalies et de cyberattaques sur des réseaux NMEA (GNSS) par l'utilisation de techniques d'apprentissage automatique, 50 pages, 2020

I.3 Plan du manuscrit

Pour répondre à la problématique **de génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals**, le manuscrit de cette thèse est composé d'une introduction, de cinq chapitres et d'une conclusion générale suivie de perspectives (Fig. I.1).

Le **deuxième chapitre** présente le contexte de l'étude ainsi que la problématique. Une présentation sur le contexte et les enjeux du secteur maritime avec une description détaillée des particularités des systèmes cybernétiques navals est réalisée. Dans ce contexte, nous détaillons également les enjeux de la numérisation du secteur maritime en discutant notamment du fonctionnement du transport maritime dans sa globalité et en précisant les vulnérabilités potentielles d'un point de vue numérique et cybernétique.

Le **troisième chapitre** propose une description sur les spécificités des systèmes de navigation et des ICS en décrivant les problématiques de cybersécurité qui en découlent. Il est décrit en quoi ces systèmes sont particulièrement vulnérables aux cyberattaques. Pour cela, nous énumérons quelques cyberattaques et incidents de cybersécurité propres à ces systèmes et plus particulièrement dans le contexte maritime. Enfin, une vue d'ensemble des méthodes de détection d'anomalies et de nouveautés est présentée en insistant notamment sur les approches par apprentissage automatique qui ont déjà fait leurs preuves et qui sont mises en œuvre dans le chapitre VI de cette thèse.

Le **quatrième chapitre** présente la plate-forme de simulation en réalisant une description détaillée de tous les systèmes mis en place pour reproduire aux plus proches de la réalité les fonctions opérationnelles d'un navire. Durant cette thèse, nous avons activement participé lors de son élaboration, ce qui nous a permis par la suite de maîtriser les systèmes employés et de pouvoir les exploiter lors des différentes phases d'expérimentation.

Dans le **cinquième chapitre**, nous décrivons notamment les outils et les méthodes mises en œuvre afin de collecter et de générer les données (falsifiées ou non) sur la plate-forme navale que ce soit des données réalistes liées aux ICS mais aussi aux systèmes de navigation. Dans cette optique de génération de données, nous détaillons la conception d'un système embarqué spécifiquement dédié à

la collection de données maritimes développé durant cette thèse. De plus, pour faciliter l'élaboration de scénarios d'attaques et de génération de données, des outils informatiques ont été développés dont les principes de fonctionnement seront détaillés au cours de ce même chapitre.

Le **sixième chapitre**, quant à lui, présente plusieurs cas d'études dans lesquels nous avons mis en application les méthodes de détections d'anomalies avec les données précédemment générées. Ces cas d'études mettent également en œuvre des scénarios plausibles et réalistes de cyberattaques sur les systèmes cybernétiques navals basés sur des rapports d'incidents réels qui ont eu lieu dans ce domaine. Ainsi, des scénarios d'attaques sont présentés dans différents contextes. Pour finir, nous décrivons et analysons les résultats des différents scénarios et quelques recommandations d'un point de vue cybersécurité sont faites.

Enfin, ce manuscrit se termine par une **conclusion** pour rappeler les différents objectifs et problématiques, les contributions et propositions de solutions apportées dans ces travaux répondant aux questions de recherches sous-jacentes. Différentes perspectives possibles sont également détaillées au regard des travaux réalisés.

Chapitre II

La Numérisation du Monde Maritime

Sommaire

II.1 Introduction

Dans ce chapitre nous détaillons les rouages du transport maritime, qui est d'une importance stratégique au niveau mondial, avec une vue d'ensemble sur tous les sous-systèmes qui y sont reliés et dont les vulnérabilités représentent des vecteurs d'attaques majeurs. Ensuite, il est question d'esquisser en quoi la transformation numérique dans ce secteur joue un rôle majeur dans notre problématique en s'intéressant tout particulièrement aux différents systèmes concernés qu'ils soient issus de technologies informationnelles ou opérationnelles. Pour finir, la sécurité numérique à bord d'un navire est abordée sous le prisme de la nécessité d'une réelle prise de conscience des différents protagonistes face aux cybermenaces.

Ce chapitre permet de répondre à la première partie de la **QR1**, comme le montre la figure (II.1).

Correspondance : Question de Recherche / Chapitre					
	Chap. II	Chap. III	Chap. IV	Chap. V	Chap. VI
QR I					
QR II					
QD I					
QR III					

FIGURE II.1 – Tableau de correspondances entre les Questions de Recherche et les Chapitres.

II.2 Le secteur maritime

Indéniablement, le transport maritime fait partie intégrante des secteurs de transport à l'instar d'autres secteurs connexes comme le transport routier, ferroviaire ou encore aérien, mais si on le compare à ses concurrents, le transport maritime est le grand gagnant de la mondialisation [45]. Il est généralement admis que sans transport maritime [139], la mondialisation telle qu'on la connaît aujourd'hui n'aurait pas été possible. Au lendemain de la Seconde Guerre mondiale, en 1950, il était question de 500 millions de tonnes de marchandises transportées par voies maritimes, aujourd'hui, c'est plus de 10 milliards de tonnes qui transitent chaque année par la mer. De nos jours, le terme d'« *économie dématérialisée* » arrive sur le devant de la scène avec le développement du E-commerce et des nouvelles méthodes de transactions informatiques. Mais jamais l'économie internationale n'a autant reposé sur des flux physiques et biens matériels acheminés par le secteur maritime [124, 2, 50]. À lui seul, ce secteur supporte 90% de ces flux en volume [48]. Cela repose sur une très grande spécialisation des navires qui s'est mise en place progressivement, mais qui a connu un développement considérable à partir de la période d'après-guerre via l'émergence des transporteurs de tout type de marchandises (pétrole, charbon, céréales, et autres biens de consommation). Ainsi, les navires civils et militaires sillonnent les différents océans et mers et contribuent dans une très large mesure à l'échange de biens dans le commerce international et à la mobilité des voyageurs par ferries et par les navires de croisière géants, qui peuvent naviguer avec parfois plus de 6000 passagers (Fig. II.2). À l'image de l'organisation très structurée de l'espace mondial et des zones économiques, l'organisation du transport maritime est extrêmement hiérarchisée[114].

L'élément que nous avons tendance à associer le plus au secteur maritime est le navire en lui-même, avec l'image du porte-conteneurs en égérie. Les navires marchands ne génèrent pas d'argent lorsqu'ils sont immobiles, ils doivent par conséquent être le plus souvent possibles en déplacement vu les investissements réalisés. Si tous les pays ayant un littoral et un port peuvent se considérer comme une nation maritime, la plupart des pays même ceux sans littoral dépendent en grande partie du transport maritime principalement pour leur économie.

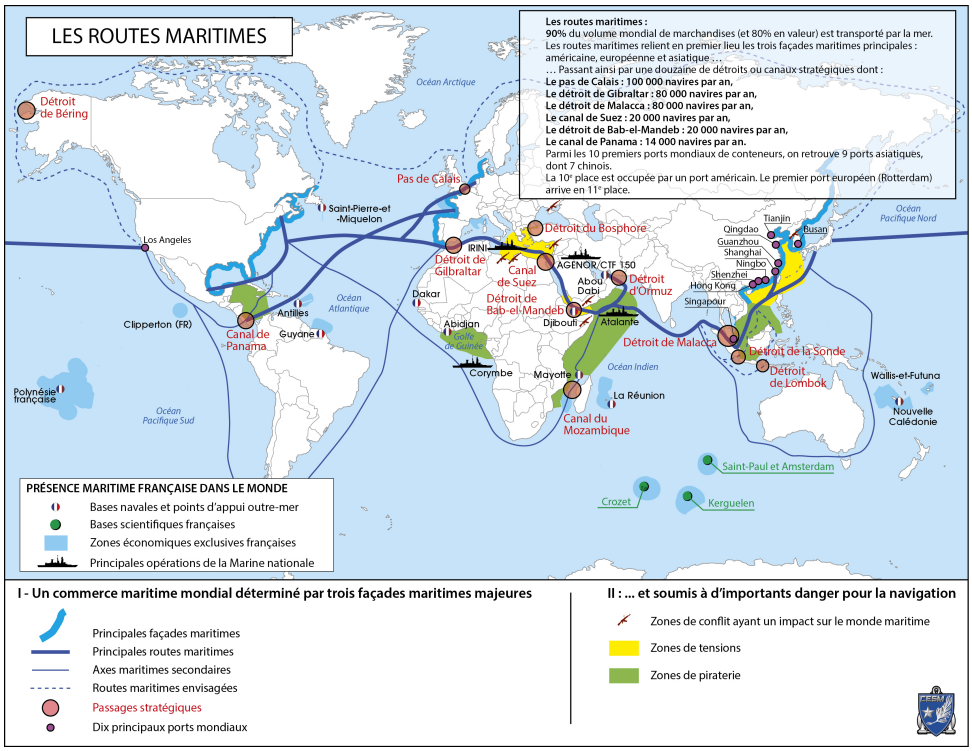


FIGURE II.2 – Les principales voies et façades maritimes française (Ministère des armées, Octobre 2021)

II.3 Organisation du secteur maritime et ses vulnérabilités

Du point de vue organisationnel, le transport maritime peut être vu comme un système composé de sous-systèmes hétérogènes qui sont interconnectés (II.3). Ces interconnexions montrent les dépendances potentielles de chaque secteur d'activité et permettent de restituer le contexte dans lequel se place notre étude. Chaque sous-système peut être vulnérable aux attaques (maillon faible ou vecteur d'attaques) et la multiplication des interconnexions va affecter l'ensemble du système. Pour se rendre compte de ce problème de vulnérabilité, nous rappelons d'abord les opérations relatives à chaque sous-système :

1. Le système *"Navire"* : les navires modernes sont des réseaux flottants, impliquant des réseaux opérationnels contrôlant les systèmes des navires, des réseaux reliant les systèmes de sécurité et de gestion des cargaisons, et des systèmes de pont pour la navigation et la communication ;
2. Le système *"Armateurs"* : les compagnies maritimes disposent de réseaux complexes tournés vers l'extérieur ainsi que de nombreux réseaux internes. Généralement, le site Web ouvert d'une société maritime est directement relié à l'Internet public donnant l'accès à des portails de connexions dédiés aux clients et aux partenaires, des capacités de commerce électronique, des systèmes de réservation, des systèmes de suivi des navires et des cargaisons, etc. Les réseaux

FIGURE II.3 – Vue d'ensemble des secteurs d'activité participant au transport maritime.

internes gèrent par exemple les communications avec les navires, le suivi des passagers et des marchandises, la gestion de la logistique et de l'approvisionnement ou la gestion des itinéraires ;

3. Le système *"Portuaire"* : les ports ont également leur propre présence sur le Web, des systèmes de vente et de marketing, des systèmes de suivi des navires et des cargaisons, des portails pour les clients, les locataires et les partenaires de la chaîne d'approvisionnement. Les systèmes de sécurité physique des ports, tels que les caméras, les automates industriels et les capteurs, sont aussi généralement gérés directement via le réseau informatique. Les communications sont essentielles entre le siège de l'armateur et le terminal, la gestion du trafic des navires, les navires entrants et sortants du port, les autorités légales et les douanes et les compagnies maritimes ;
4. Le système *"Gestion du fret (cargaison et transport)"* : les réseaux liés à la cargaison assurent la connexion avec les douanes, les partenaires commerciaux et les propriétaires de la cargaison qui est temporairement stockée dans le port. La sécurité du fret est contrôlée par des ordinateurs, ainsi que le transfert vers et depuis les transporteurs connexes, faisant directement la liaison avec les transporteurs ferroviaires, routiers et aériens ;
5. Le système *"Contrôle du trafic maritime"* : la gestion du flux de navires nécessite des communications radio fiables, des systèmes de Positionnement, de Navigation et de Temps (PNT), tels que le Système de Positionnement Global (GPS). Il y a également les réseaux de connaissance de la situation, tels que le Système d'Identification automatique (AIS), des cartes et des avis aux navigateurs actualisés, ainsi que d'autres fonctions permettant de maintenir un mouvement sûr et efficace des navires, des marchandises et des personnes comme le CROSS (Centre

Régional Opérationnel de Surveillance et de Sauvetage Maritime) (Fig. II.4). Chacun de ces systèmes constitue un vecteur potentiel de cyberattaques dans des zones géographiques qui peuvent tolérer une faible marge d'erreur ;

6. Particularité du système *"Véhicule autonome"* : des véhicules autonomes commencent à se développer pour une meilleure préservation du personnel, d'impératifs économiques et d'autres facteurs de performance et d'efficacité en fonction des situations (recherche sous-marine, déminage, etc.). Ces véhicules vont des systèmes télécommandés aux navires entièrement autonomes, aux remorqueurs ou aux installations d'amarrage. S'ils ne sont pas correctement sécurisés, chacun d'entre eux peut être détourné pour être au mieux non fonctionnel, ou au pire transformé en arme physique ;

Les éléments ci-dessus ne visent qu'à donner un aperçu de la complexité et du nombre de systèmes nécessaires au fonctionnement dans l'ensemble du secteur maritime et, par conséquent, une liste non exhaustive de cibles potentielles et des menaces possibles.

FIGURE II.4 – Le trafic maritime mondial en temps réel du 24 mai 2022 à 12h00 - Marine Trafic. Vert : Tanker, Rouge : Navire cargo, Bleu : Transporteur de passagers.

II.4 La numérisation du monde maritime

Un navire peut être considéré comme une usine flottante du fait de sa complexité technique et de ses déplacements. Il est très proche des usines concernant les processus industriels complexes soumis à des contraintes spécifiques (environnement marin, aléas météorologiques, etc.). Mais si l'on prend en compte d'autres aspects comme les passagers et la vie à bord, le navire peut presque plus facilement s'apparenter à une petite ville flottante mélangeant zones de conduite, zone d'opérations

industrielles et zones de vie. Les avancées technologiques permettent de construire des navires plus grands, plus rapides et plus puissants, qui peuvent transporter des milliers de conteneurs et passagers à travers le monde. Si la sécurité a toujours été une préoccupation dans l'industrie navale, il concerne en premier lieu la sûreté en assurant la sécurité des équipages, mais aussi le transport à bonne destination des marchandises sans en perdre une partie. Faute à la conclusion courante entre sécurité [1] et sûreté [2], il est difficile, du moins en français, d'être d'une clarté absolue. Pour éviter cet écueil et parce que les questions de sécurité comme de sûreté sont souvent entremêlées, il ne sera fait référence qu'à la sécurité comme impliquant les deux notions.

II.4.1 Les réseaux à bord des navires

Bien que plusieurs organisations du domaine de la sécurité publient des conseils sur la gestion de la cybersécurité, aucune d'elles n'est responsable des systèmes informatiques qui permettent de faire fonctionner le transport maritime dans son ensemble. D'autant plus que la plupart des organisations ne sont pas entièrement propriétaires ou exploitantes de leur infrastructure informatique.

II.4.1.1 Une grande variabilité dans les réseaux fortement interconnectés

Les navires disposent généralement de plusieurs réseaux spécifiques à bord. Le réseau interne du navire contrôle les fonctions de bord, telles que la propulsion, l'alimentation, la surveillance de l'état global des actionneurs et les ballastes. Le navire est également susceptible d'être connecté à Internet pour les communications avec l'équipage, les passagers et les divertissements, ainsi que pour les communications de l'entreprise et permet également de communiquer avec la Terre. Le GPS, l'AIS et autres communications radio (*Very High Frequency* - VHF) utilisent également des canaux radio publics. Les armateurs, quant à eux, utilisent une combinaison de réseaux privés pour les communications internes, de réseaux publics pour la navigation et les communications avec notamment les autres industries de transport pour l'approvisionnement et la gestion des marchandises et des passagers.

Murrison *et al.* [99] montrent que l'industrie maritime est de plus en plus impactée par l'Internet des Objets (*Internet of Things* - IoT [3]). L'IoT se manifeste sur les navires et les ports par une automatisation accrue des différents processus, une maintenance automatique croissante, une

1. La sécurité désigne normalement les moyens - humains, techniques et organisationnels - de prévention et d'intervention contre les risques à caractère accidentel : catastrophe naturelle, accident industriel, incendie, fuite d'eau, ...

2. La sûreté désigne l'ensemble des moyens dédiés à la prévention des actes de malveillance. Ces actes, par définition volontaires, ont pour finalité le profit et/ou l'intention de nuire : vols, sabotage, attentat, etc.

3. L'Internet des Objets (IoT) est le fonctionnement "Internet" d'appareils physiques, de véhicules, de bâtiments et d'autres éléments - intégrés à l'électronique, aux logiciels, aux capteurs, aux actionneurs et à la collectivité réseau qui permettent à ces objets de collecter et d'échanger des données [137]. Souvent ces appareils sont également appelés « appareils connectés » ou « appareils intelligents ».

aide à la gouvernance ou encore joue un rôle croissant dans les systèmes de surveillance [60, 43]. Ainsi les systèmes sur un navire sont devenus fortement interdépendants [125]. Par exemple, l'AIS est connecté à plusieurs systèmes qui sont tous dépendant comme le Radar ou le traceur de cartes [98]. Le navire est devenu un système éminemment complexe avec énormément de systèmes informatiques interconnectés. Il doit opérer dans un milieu hostile, corrosif et imprévisible et les nouvelles technologies permettent justement de réduire l'impact de ces contraintes pour que le navire puisse s'adapter plus facilement à cet environnement rude. A noter que les technologies numériques sont de plus en plus indispensables du fait des exigences de réduction des coûts et des effectifs des personnes naviguants [43]. De plus, certaines tâches peuvent être particulièrement dangereuses et il convient de les remplacer par des dispositifs automatisés et de les contrôler depuis la passerelle du navire. Pour cela, les systèmes à base d'automate industriel et des Systèmes de Contrôle Industriels (ICS) et en particulier à base de SCADA (Systèmes de Contrôle, de Supervision et d'Acquisition de données) sont utilisés, par exemple pour piloter des vannes, à ouvrir des portes, ou actionner ou non la ligne de barre et le gouvernail. Ces systèmes sont programmables et opérables à distance et même directement par Internet, et par conséquent ils sont vulnérables aux attaques.

II.4.1.2 Les spécificités des réseaux de communications dans un navire

Il existe une grande variété de réseaux de communication associés aux diverses opérations d'un navire. Certains réseaux externes sont privés, relativement sûrs, et peuvent ou non être chiffrés. Les réseaux publics sont totalement ouverts à toute personne possédant un récepteur. Ces réseaux de communication externes sont imagés dans la figure (II.5) et comprennent :

1. la radio VHF est présente sur tous les navires avec un canal dédié aux communications traditionnelles, et peut être utilisée pour les appels de détresse ;
2. les systèmes de surveillance des navires (*Vessel Monitoring System* - VMS) permettent aux organismes de réglementation de l'environnement de suivre et de surveiller les activités des navires de pêche ;
3. les systèmes d'identification à longue distance et de suivi (*Long-Range Identification and Tracking* - LRIT) permettent de signaler leur position sur une période précise ;
4. les VPN permettent des communications privées et sécurisées avec le navire pour pouvoir échanger ou accéder à des données via Internet ;
5. les systèmes de positionnement par Satellite (*Global Navigation Satellite Systems* - GNSS) et l'AIS sont conçus pour la position, la navigation, la synchronisation et la bonne compréhension de la situation environnante ;
6. les systèmes VSAT (*Very Small Aperture Terminal*) permettent une communication bidirectionnelle avec des stations terrestres via des constellations de satellites, généralement pour les transmissions de données, mais qui disposent d'un débit très limité.

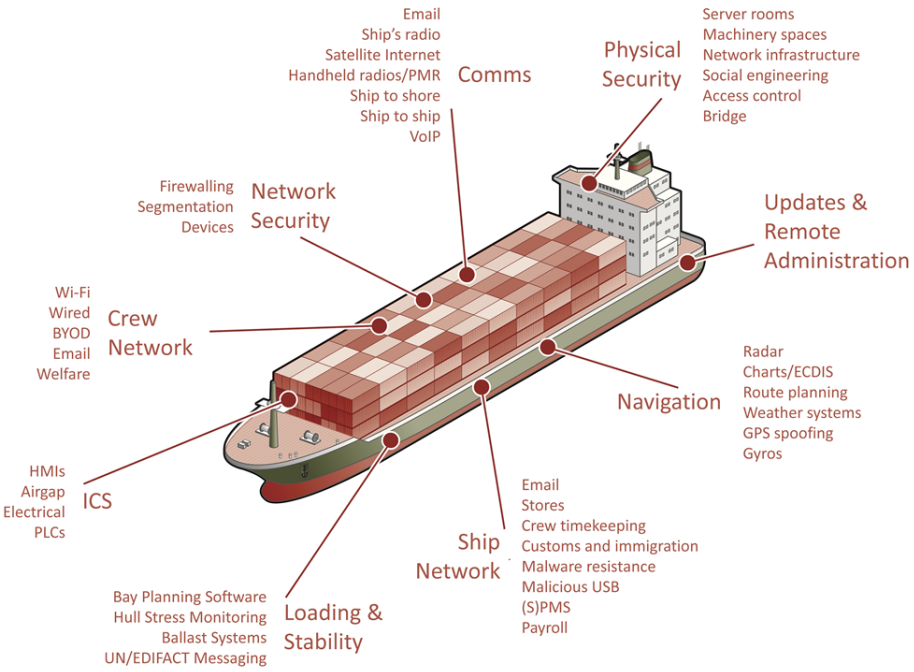


FIGURE II.5 – Vue globale des systèmes cybernétiques à bord d'un navire (Source : Pen Test Partners https ://www.pentestpartners.com/content/uploads/2018/03/MaritimeMVWeb.png.)

Concernant les réseaux internes et leurs systèmes, on peut d'ailleurs énoncer (Fig. II.5) :

- ✓ les réseaux des systèmes mécaniques, tels que le moteur principal, le moteur auxiliaire, le contrôle de la direction et la gestion des ballasts ;
- ✓ les réseaux des systèmes de surveillance et de sécurité du navire, tels que le système d'alerte de sécurité du navire, les systèmes de contrôle d'accès ou les interphones d'alarme générale ;
- ✓ les réseaux des systèmes de manutention de la cargaison, tels que les commandes à distance des vannes, les systèmes de surveillance du niveau et de la pression, la planification des baies, la surveillance des contraintes ou l'échange de données électroniques pour l'administration.

Les navires spécialisés ont également leurs propres réseaux spécifiques, tels que les systèmes de divertissement sur les navires de passagers ou les VMS sur les bateaux de pêche commerciale. Les dispositifs de ces réseaux sont interconnectés à l'aide de protocoles de réseau standard tels que le bus CAN (*Controller Area Network*), Ethernet ou les liaisons série, qui présentent chacun leurs propres vulnérabilités en matière de sécurité. En outre, les différents réseaux de bord sont interconnectés de manière peu étanche. Il est donc possible de se déplacer latéralement d'un réseau à l'autre, y compris depuis l'extérieur du navire.

II.4.2 Le système de navigation intégré et ses vulnérabilités

Les systèmes de navigation à bord des navires ont radicalement évolué depuis l'introduction des systèmes électroniques. Cette partie se concentre sur les systèmes de navigation du navire ainsi que leurs vulnérabilités associées. On propose de faire une synthèse sur les systèmes les plus exploités dans le monde, à savoir le GNSS, et en particulier le GPS et l'AIS. À bord d'un navire, le centre du commandement est souvent la passerelle, c'est-à-dire l'endroit où sont coordonnées la surveillance et la gestion de tous les systèmes de contrôle du navire. On appelle Système de Navigation Intégré, ou *Integrated Navigation System* (INS), le matériel de passerelle qui regroupe sur une ou plusieurs consoles toutes les fonctions logicielles et systèmes liés à la navigation et à la sécurité. Un INS intègre les données provenant par exemple de l'ECDIS, l'AIS, le GPS, ou Radar ainsi que de différents capteurs (gouvernail, salinité, température de l'eau, capteurs météorologiques, etc.) comme le montre la figure (II.6).

La navigation et l'élaboration d'une route sont relativement complexes puisqu'il est nécessaire de prendre en compte de nombreux paramètres (courants marins, données météorologiques, zones de piraterie, etc.) tout en optimisant la trajectoire pour réduire la consommation de carburant et de maximiser le rendement économique. Pour cela, les outils informatiques présents en passerelle (INS) sont devenus incontournables et jouent un rôle majeur dans la navigation. Les données et cartes maritimes sont désormais numériques et les informations sur l'environnement du navire sont directement renseignées à partir de différents capteurs [81, 107].

Du fait de sa forte interconnexion, un INS est une cible de choix pour subir des cyberattaques via des vecteurs différents comme des modules de communication ou encore des protocoles réseau peu sécurisés. Lund *et al.* [86] montrent comment en branchant une clé USB, contenant un script malveillant, à un des appareils connectés sur l'INS on peut infecter l'ensemble du système. Ainsi, le logiciel malveillant a infecté l'ECDIS et les signaux GPS ont été manipulés en usurpant le protocole de messages GPS utilisé entre les appareils connectés sur l'INS. Cette attaque a permis de rendre inopérant le poste d'opérateur, rendant le navire aveugle (la navigation devenant impossible).

II.4.2.1 Les systèmes de positionnement par satellites (GNSS)

On utilise le terme générique GNSS pour désigner les quatre systèmes de navigation par satellite à couverture mondiale, à savoir le GPS (États-Unis), BeiDou (République populaire Chine), Galileo (Union européenne) et enfin GLONASS (Fédération de Russie). Le principe de fonctionnement est relativement simple. Un récepteur GNSS détermine sa position sur la surface de la Terre à l'aide d'un processus appelé *trilatération* (Fig. II.7). Plus exactement, un récepteur reçoit des informations d'une collection de satellites, dans le cas minimal 4 satellites et 6 satellites dans le cas optimal. Chaque satellite émet une onde électromagnétique de vitesse connue. Cette onde porteuse

FIGURE II.6 – Exemple de Systèmes de Navigations Intégrés (INS) en passerelle du navire. (Source wikipédia : https ://en.wikipedia.org/wiki/Navigation)

d'un code est émise à un temps bien déterminé. Le récepteur estime ensuite le temps de transmission qui est le temps nécessaire pour que son signal, porteur du même code, soit en phase avec le signal émis par la satellite. En multipliant ce temps par la vitesse, on obtient donc la distance qui le sépare du satellite. En répétant cette procédure avec un deuxième satellite, il peut à nouveau se situer sur une deuxième sphère centrée sur le deuxième satellite. En réitérant l'opération une troisième fois et en cherchant la zone d'intersection entre ces trois cercles, on obtient la position sur terre. Le quatrième satellite permet de déterminer le décalage entre l'heure du récepteur et l'heure exacte fournie par les satellites, afin d'affiner la position. La précision de position augmente donc en fonction du nombre de satellites.

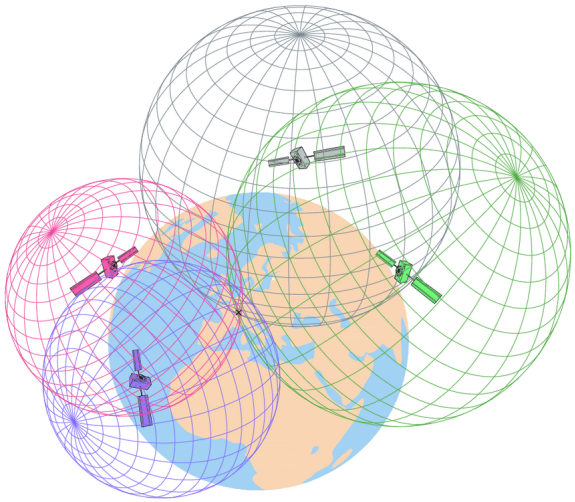


FIGURE II.7 – Principe de la trilatération des systèmes de positionnement par satellites [106].

II.4.2.2 Les vulnérabilités des systèmes de positionnement par satellites (GNSS)

De très nombreux systèmes allant des téléphones portables et véhicules autonomes jusqu'aux avions en passant par les navires exploitent de plus en plus les systèmes GNSS afin de déterminer leurs positions permettant la géolocalisation et une navigation d'une précision extrême. Si l'on considère tous les endroits dans le monde où est utilisé le GNSS pour faire transiter des navires de plus en plus grands dans des canaux de navigation étroits comme le détroit du Bosphore (Turquie), d'Ormuz (Golf Persique), de Kill Van Kull (États-Unis), le canal de Suez (Égypte) ou encore le canal de Panama, il apparaît clairement que les systèmes GNSS sont devenus incontournables. Ainsi, on comprend facilement en quoi ces systèmes peuvent être tout à fait critiques lorsqu'ils sont soumis à des cyberattaques [35]. Deux attaques du GNSS sont exploitées dans les travaux de cette thèse à savoir : le brouillage et le leurrage.

Le brouillage GNSS (*GNSS Jamming*)

Le brouillage consiste à interférer délibérément avec un signal GNSS, généralement en distordant ou en surchargeant le signal original de sorte que le récepteur ne puisse pas obtenir sa position. Bien que leur détention et leur utilisation soient illégales, les brouilleurs de GNSS peuvent être achetés à bas prix sur Internet [64]. Le brouillage GNSS, qui est un mécanisme peu coûteux de piratage des systèmes de positionnement, peut avoir de graves conséquences et a fait émerger de nombreux travaux de recherches [51, 58]. Ainsi on peut par exemple citer le cas de ce conducteur de poids lourd dans le New Jersey utilisant un brouilleur GPS afin de cacher où il se trouvait pendant ses pauses. Et par inadvertance, il a brouillé le système GPS de l'aéroport Newark Liberty pendant les essais des systèmes d'atterrissage automatique [54].

Le leurrage GNSS (*GNSS Spoofing*)

Le leurrage (ou falsification de signaux GNSS) désigne la transmission délibérée de faux signaux de positionnement afin qu'un récepteur GNSS calcule mal sa position [115]. Le leurrage est une forme d'attaque beaucoup plus insidieuse que le brouillage dans la mesure où il consiste à imiter délibérément une constellation GNSS, en faisant croire au récepteur qu'il a reçu des informations cohérentes, pertinentes et autorisées. Dans sa forme la plus simple, le leurrage GPS consiste à envoyer de fausses informations de localisation au récepteur GNSS (un navire dans un port d'escale pourrait voir sa position comme étant en mer). Dans ces circonstances, le leurrage fonctionne essentiellement comme une forme plus intelligente de brouillage. Il convient de noter que tous les navires se trouvant à proximité peuvent également être victimes de cette perturbation et les données GNSS transitant par les données AIS seront également falsifiées. Les incidents d'usurpation de signaux GPS ont augmenté si rapidement au cours des dernières années que ces techniques sont devenues une arme de conflit et une menace majeure pour la navigation commerciale [4] [141, 12]. À titre d'exemple, on peut citer la première expérience civile de leurrage GPS très médiatisée en mer Méditerranée en

4. https ://www.c4reports.org/aboveusonlystars.

2013. Elle a été réalisée par des chercheurs de l'Université du Texas à Austin qui ont amené le yacht le *White Rose of Drachs* de 213 pieds (65m) à modifier sa route et son cap à l'insu de l'équipage. Pour cela, l'équipe a utilisé des produits du commerce pour construire le dispositif d'usurpation. L'événement a commencé par la diffusion de signaux GPS de très faible puissance. La puissance du signal a été lentement augmentée jusqu'à ce que le récepteur du navire accepte le nouveau signal et abandonne le signal légitime. Les signaux transmis à l'équipage ont donné l'impression que le yacht avait dérivé de trois degrés vers la gauche. Une dérive si légère que l'équipage a supposé qu'elle était due au vent et aux conditions météorologiques. L'équipage a compensé cette dérive en faisant glisser le navire vers la droite, ce qui a fini par le faire dévier d'environ 1 km.

Depuis le début de l'invasion de l'Ukraine [80, 91], l'armée russe n'hésite pas à mettre en œuvre des méthodes de brouillage et de leurrage des signaux GNSS, pour perturber les systèmes de géolocalisation de type GPS ou Galileo, utilisés par les avions de ligne. Ces brouillages ne se limitent pas à la zone de conflit en Ukraine. D'après un bulletin d'alerte publié le 17 mars 2022 par l'Agence Européenne de la Sécurité Aérienne (AESA), les forces russes auraient ainsi brouillé les signaux GNSS dans les pays Baltes, la Pologne et la mer Baltique, l'est de la Finlande, la mer Noire, ainsi que l'Est de la Méditerranée entre Chypre, la Syrie, l'Israël, le Liban, le nord de l'Irak et une partie de la Turquie. La zone des perturbations se serait considérablement étendue et aurait touché à plusieurs reprises l'espace aérien et maritime de l'Union Européenne, d'après la Direction Générale de l'Aviation Civile (DGAC). [5]

II.4.2.3 Le Système d'Identification Automatique (AIS)

L'AIS est un système radio qui fonctionne dans un rayon de 10 à 20 milles nautiques (nm). Il permet aux équipages en mer de connaître la présence des autres navires (éviter les collisions), de s'identifier auprès des autorités maritimes qui surveillent les navires et leurs cargaisons dans leur zone de responsabilité. Cela permet aussi aux navires et aux stations côtières d'échanger des informations météorologiques, de sécurité et d'autres informations jugées importantes pour la navigation. L'AIS a été conçu dans les années 1990 et adopté au niveau international lors de la Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS) de 2002. Les transpondeurs AIS de classe B (dédiées aux particuliers) sont par exemple utilisés sur les yachts, les petits bateaux de pêche et autres plaisanciers. Les appareils de classe A (dédiés aux professionnels) transmettent généralement des informations plus détaillées avec une meilleure puissance d'émission que les appareils de classe B, notamment le numéro d'immatriculation du navire (*Maritime Mobile Service Identity* - MMSI), le numéro de l'Organisation Maritime Internationale (OMI), les dimensions, la latitude, la longitude, la route, le cap, la vitesse de giration, la destination, le type de cargaison et le statut opérationnel.

5. https ://www.lesechos.fr/industrie-services/air-defense/comment-la-russie-perturbe-le-trafic-aerien-en-europe-en-brouillant-les-signaux-gps-1395673.

Les dispositifs AIS obtiennent des informations de localisation à partir des données GNSS du navire et sont donc dépendants de l'intégrité du système de positionnement. L'AIS est également utilisé par les ports, les services de gestion du trafic maritime et les agences de surveillance côtière. Le schéma de la figure II.8 montre le fonctionnement de l'AIS. Parmi les utilisateurs de ce système, on retrouve, les navires de recherche et de sauvetage (*Search And Rescue* - SAR), les avions, les stations de base AIS, les satellites, les répéteurs et les aides à la navigation spécialement équipées. Les autres stations mobiles compatibles AIS comprennent les transpondeurs SAR (AIS-SART), les émetteurs d'homme à la mer (MOB) et les radiobalises de localisation des sinistres (EPIRB). Les GNSS ne sont pas des composants de l'AIS, mais ils fournissent des informations sur la position géographique essentielles au fonctionnement de l'AIS.

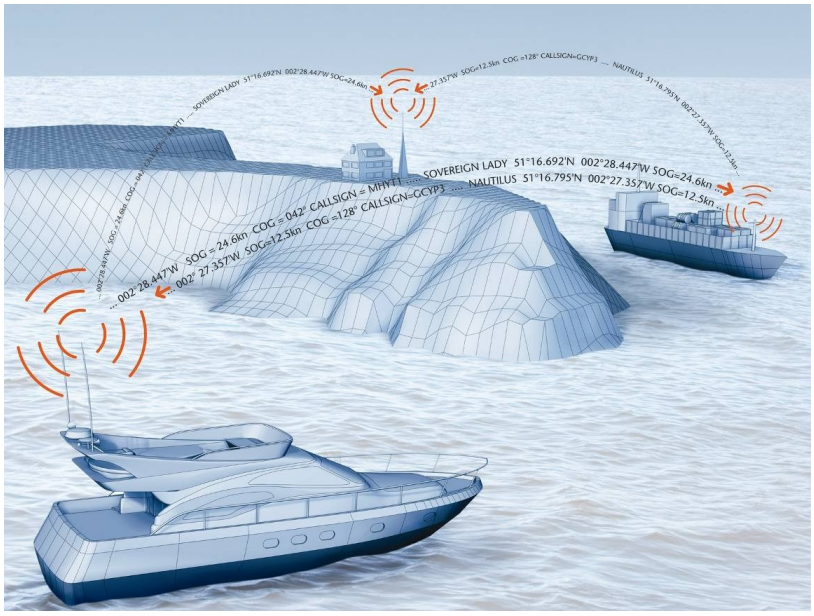


FIGURE II.8 – Principe de fonctionnement de l'AIS (Source : Digital Yacht - https ://digitalyacht.fr/blog/2018/07/transmission-ais/).

II.4.2.4 Les vulnérabilités du Système d'Identification Automatique (AIS)

L'AIS n'a pas été développé pour faire face à des attaques actives allant à l'encontre de son fonctionnement lorsqu'il a été conçu. C'est pourquoi, un grand nombre de vulnérabilités ont été identifiées dans les protocoles AIS :

- ✓ Absence de validation géographique : il est possible qu'un appareil transmette un message AIS d'un endroit donné tout en prétendant être dans un autre endroit.
- ✓ Absence d'information sur l'horodatage : un individu malintentionné peut enregistrer des messages AIS valides pour faire croire qu'un navire était présent à un autre moment.

- ✓ Absence d'authentification des messages : aucun mécanisme d'authentification de l'expéditeur d'un message, toute personne capable de trafiquer un paquet AIS peut usurper l'identité d'un autre appareil et donc d'un autre navire.
- ✓ Absence d'intégrité du message : comme les messages AIS ne contiennent pas de vérification de l'intégrité du message, un adversaire peut intercepter et/ou modifier les transmissions avant de les envoyer au récepteur.

Ces vulnérabilités permettent à quiconque de créer intentionnellement de faux messages pour usurper l'identité d'un navire existant ou se faire passer pour un navire fantôme, de rejouer des AIS antérieurs, de déclencher de fausses alertes SAR ou d'envoyer de fausses informations météorologiques comme de navigation. Chacun de ces cas de figure peut amener un autre navire à modifier sa trajectoire. Étant donné que tous les émetteurs-récepteurs AIS émettent sur la fréquence VHF publique, n'importe qui peut écouter le trafic radio. Un individu peut brouiller les signaux AIS, entraînant la mise hors service d'une petite zone du réseau AIS. Ces attaques sont rendues possibles par des outils logiciels capables de générer et d'intercepter des messages AIS. Ils sont même couramment disponibles sur Internet [13].

II.4.3 Les Systèmes de Contrôle Industriels (ICS)

Depuis des dizaines d'années, le déploiement des ICS s'est fortement accéléré de façon universelle (usines, centrales électriques, centrales nucléaires, pipelines, etc.). Le domaine des transports connaît aussi les mêmes mutations technologiques comme les gares ou les aéroports en passant par les ports et les navires eux-mêmes. Il est nécessaire de définir les systèmes de Technologie de l'Information (*Information Technology* - IT) et les systèmes de Technologie Opérationnelle (*Operational Technology* - OT) :

Définition IT : La Technologie de l'Information [103, 53] comprend le bon fonctionnement de tous les outils de communication et d'information de l'entité. Elle inclut tous les services, équipements, systèmes ou sous-systèmes d'équipements interconnectés qui sont utilisés pour différentes tâches. Ces tâches regroupent l'acquisition, du stockage, l'analyse, l'évaluation, la manipulation, la gestion, le contrôle, l'affichage, la transmission ou la réception automatique de données et d'informations par l'entité concernée. Le tout peut être représenté par le réseau informatique, filaire ou sans-fil, la téléphonie fixe, le parc informatique, la maintenance des logiciels, la stratégie de protection, etc.

Définition OT : La Technologie Opérationnelle [53] englobe les systèmes ou dispositifs programmables qui interagissent avec l'environnement physique (ou qui gèrent les dispositifs interagissant avec l'environnement physique). Ces systèmes surveillent et contrôlent des dispositifs, des processus ou des événements. La finalité de l'OT est d'assurer la pérennité du fonctionnement d'un outil de production ou de biens matériels pendant les opérations.

Afin d'appréhender les spécificités des ICS dans le domaine maritime, il est intéressant de décrire les différences entre les ICS et les systèmes informatiques selon trois grands axes :

- ✓ Les fonctionnalités et les spécificités attendues ;
- ✓ Les technologies utilisées ainsi que les cycles de vie des entités ;
- ✓ Les différences majeures dans les politiques de sécurité.

II.4.3.1 Différences de fonctionnalités entre ICS et Systèmes Informatiques

Ainsi à partir des définitions précédentes, il est possible d'aborder les principales différences entre les ICS et les systèmes informatiques classiques. La figure II.9 schématise une vue d'ensemble des systèmes industriels. Rappelons que les exigences de performance, de fiabilité et de sécurité des logiciels et du matériel industriel sont différentes de celles des systèmes informatiques traditionnels.

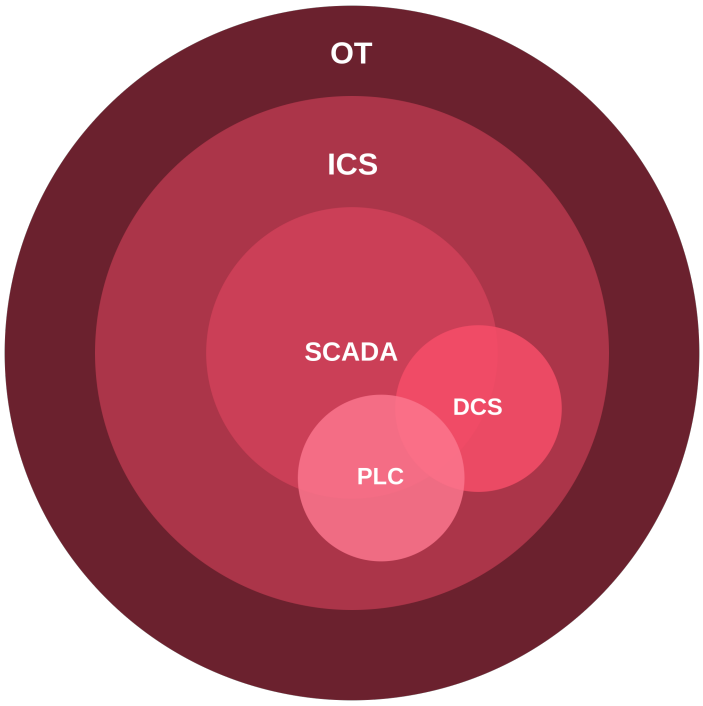


FIGURE II.9 – Vue d'ensemble des systèmes industriels.

L'OT comprend les nombreuses technologies et méthodes qui permettent de réunir les mondes virtuels et physiques. Dans les systèmes OT, les automates assurent directement la surveillance et le contrôle de dispositifs physiques tels que les vannes, les pompes, les barrages, les chaînes de montage ou les réseaux électriques. Les ICS constituent ainsi le plus grand segment des dispositifs OT. Quand on parle d'ICS, il est généralement fait référence aux systèmes informatiques qui gèrent les opérations industrielles et d'autres applications de Systèmes Cyber-Physiques (*Cyber Physical System* - CPS). L Ainsi, ils contrôlent les équipements dans le monde physique. Les systèmes IT

gèrent généralement les opérations et les données administratives.

L'une des particularités est que les ICS gèrent principalement des environnements opérationnels en permanence (24h/24, 7j/7 et 365j/an). Sur les ICS, les contrôles nécessitent une gestion en temps réel, une communication sans délai, un matériel et un logiciel à haute disponibilité. Ainsi, les conséquences d'une panne du ICS, due à une défaillance du dispositif ou à des cyberattaques, peuvent être désastreuses, non seulement pour le dispositif lui-même, mais aussi pour l'environnement opérationnel et la sécurité des personnes à proximité. Cependant cela peut-être aussi le cas pour de l'IT lorsque par exemple des systèmes informatiques de banques doivent gérer des transactions avec un haut niveau de disponibilité. Les ICS comprennent une variété de sous-systèmes de contrôle : un contrôleur logique programmable (*Programmable Logic Controller* - PLC) qui est un système informatique spécialisé qui contrôle les dispositifs matériels dans un environnement d'automatisation industrielle. C'est à dire une combinaison entre un automate qui reçoit des données de capteurs et d'autres dispositifs d'entrée permettant de traiter les données et d'envoyer des commandes de contrôle au matériel géré via des interfaces homme-machine.

Un système de commande distribué (*Distributed Control System* - DCS) gère des processus qui comportent de nombreuses boucles d'alimentation et sont répartis entre différents contrôleurs. Un DCS, par exemple, peut être vu comme un grand nombre de PLC mis en réseau, chacun fonctionnant indépendamment les uns des autres, mais tous reliés à un poste de commande central. Dans ce cas, c'est le DCS qui fournit la logique du système distribué pour le faire apparaître comme un seul système et les PLC mettent en œuvre la fonction de contrôle. Un exemple pourrait être le système de propulsion d'un navire, où la surveillance et la gestion des moteurs, des arbres d'entraînement et des hélices peuvent se faire à partir d'une console centrale, qui est informée de l'état des différents composants par des capteurs.

Les systèmes de contrôle de surveillance et d'acquisition de données SCADA fournissent un environnement de gestion centrale de haut niveau dans lequel les opérateurs peuvent conserver une connaissance de la situation et gérer un ICS distribué. Les systèmes SCADA intègrent des communications réseau, une interface graphique pour l'utilisateur et de multiples capacités d'acquisition de données de sorte qu'un opérateur humain puisse surveiller l'état d'un système, détecter une activité anormale ou l'état du système en temps-réel et ajuster le processus si nécessaire. Finalement du côté des fonctionnalités attendues, les ICS sont généralement conçus pour appliquer des tâches spécifiques, optimisés pour une faible consommation d'énergie avec un coût minimal. Les caractéristiques essentielles d'un ICS sont :

✓ Le pilotage d'un processus physique selon le mode opératoire prévu, mais aussi d'assurer des

fonctions de sécurité en cas de fonctionnement anormal [44].

✓ Un ICS doit être constamment en fonctionnement ou alors fonctionnel par intermittence selon les besoins opérationnels.

II.4.3.2 Différences dans la politique sécuritaire

D'un point de vue sécuritaire, les ICS et les systèmes informatiques diffèrent, et les mécanismes mis en œuvre ne sont pas identiques. Ceci est dû à la différence des technologies utilisées :

✓ Objectif de sécurité : l'une des plus grandes différences entre la sécurité informatique des ICS et des systèmes informatiques est l'objectif principal de chacune en matière de sécurité. Les systèmes informatiques classiques ont pour finalité de sécuriser principalement la confidentialité des données : c'est à dire, s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé. Parallèlement, bien que la protection de l'information soit importante pour un ICS, son objectif est l'intégrité de son processus de fonctionnement et de la disponibilité des composants [101]. Pour un ICS, la confidentialité est rarement au premier plan ;

✓ Niveau de gravité en cas d'attaque : Les systèmes informatiques gèrent des informations souvent importantes, ainsi une attaque dans ces systèmes peut produire des problèmes importants (blocage des informations, pertes financières, etc.), mais non nécessairement vitaux. A contrario, une attaque dans un ICS peut être catastrophique, car qu'il gère des systèmes physiques et des infrastructures critiques. Les effets peuvent aller de la simple dégradation de production à des problèmes d'intégrité système, pouvant entraîner de graves problèmes de sécurité pouvant mettre en péril la santé des personnes [128] [6] ;

✓ Mise à jour des logiciels et des systèmes d'exploitation : les systèmes informatiques sont conçus pour être utilisés avec des systèmes d'exploitation typiques. Leurs mises à jour sont dans la mesure du possible simplifié avec la disponibilité d'outils de déploiement automatisés. En revanche, les ICS utilisent des systèmes d'exploitation différents et souvent propriétaires. Les modifications et les mises à jour des logiciels peuvent impliquer des modifications importantes du matériel, mais aussi des logiciels.

Ainsi pour les ICS, les risques portent par exemple sur l'ensemble de leurs réseaux, la gestion des capteurs et actionneurs, les SCADA, l'ensemble des serveurs et les applications de l'ICS afin de superviser le procédé industriel dans son ensemble. À bord du navire, les ICS sont amenés à gérer la plate-forme navire (propulsion, énergie, etc.) comme la conduite du navire, les systèmes du navire, les systèmes de sécurité ou encore l'exploitation et la gestion de la cargaison.

6. https ://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels/

II.4.3.3 Les vulnérabilités des Systèmes de Contrôle Industriels (ICS)

L'introduction des capacités informatiques sur ces systèmes a causé l'émergence d'un grand nombre de vulnérabilités [142, 85]. Cependant, les systèmes informatiques et les ICS possèdent des caractéristiques différentes, qui nécessitent des mécanismes de sécurité et de supervision différents, mais complémentaires du fait de leurs fortes interconnexions.

La problématique de la gestion de la sécurité des ICS réside essentiellement dans la différence de durée de vie entre les outils des SCADA (cycle de vie court, entre 3 à 5 ans) et les réseaux industriels (cycle de vie long, 15-20 voire 30 ans) [128]. On peut considérer que ces derniers sont figés dans le bateau et difficiles à faire évoluer. Il est possible de regrouper les vulnérabilités de ces systèmes en 5 grands thèmes :

- ✓ un faible niveau de protection des accès : contrôle d'accès avec une gestion de l'utilisateur et du mot de passe trop faibles, absence d'antivirus sur les postes de travail et serveurs, des utilisateurs disposant de privilèges administrateurs ;
- ✓ la non-mise à jour et la faiblesse des protocoles de gestion courants (FTP, Telnet, VNC, SNMP, etc.) utilisés sans chiffrement qui ouvrent l'accès à la récupération de login/mot de passe, à des connexions illégitimes aux serveurs ;
- ✓ l'absence de cloisonnement entre les systèmes de gestion et les systèmes industriels non sécurisés (absence de pare-feu ou mauvaise configuration de sécurité). Cela permet de s'introduire facilement, via le système de gestion informatique, dans le réseau industriel. Cette méthode d'accès permet à la fois de recueillir des informations, mais aussi de saboter les différents systèmes. Cette faiblesse est la cible de nombreuses attaques récentes [9] ;
- ✓ l'utilisation croissante de systèmes informatiques standards : ces produits sur étagères permettent une réduction des coûts et d'interopérabilité. Ces systèmes sont par conséquent la proie de logiciels malveillants ;
- ✓ l'absence de contrôle des intervenants sur les systèmes industriels : la surveillance des sous-traitants reste bien souvent insuffisante. Les conséquences de cette non-gestion peuvent être la perte de données et l'absence de supervision du système en cas de comportements anormaux.

Même si les ICS et les systèmes informatiques présentent des vulnérabilités partagées, ils ont des conséquences différentes. Par exemple, l'attaque de Déni de Service (DoS) sur un système informatique rend le service indisponible impactant fortement l'infrastructure dans laquelle ils sont utilisés [55]. Malgré leur convergence d'interconnexion, un ICS présente de nombreuses caractéristiques qui diffèrent des systèmes informatiques traditionnels. Les ICS ont des exigences de performances et de fiabilités différentes, et utilisent souvent des applications qui peuvent être considérées comme non conventionnelles dans un environnement de réseau informatique plus classique. Certains d'entre eux peuvent ainsi provoquer des dommages importants à l'environnement, voire impacter la sécurité et la santé des êtres humains. C'est pourquoi des protections de sécurité doivent êtres mises en œuvre

de manière à maintenir l'intégrité du système pendant les opérations normales ainsi que pendant les périodes de cyberattaques. Cette partie sera développée plus en détail dans le prochain chapitre (Chap. III).

II.5 La sécurité à bord des navires

II.5.1 Quelques faiblesses des systèmes de sécurité sur un navire

Nous avons décrit les différents réseaux qui peuvent coexister à bord en plus des systèmes de navigation et des ICS en précisant pour certains leurs vulnérabilités, mais quand est-il véritablement du point de vue de la sécurité à bord d'un navire ?

Les systèmes de passerelle
Tous les systèmes embarqués sont réunis sur la passerelle, ce qui permet aux opérateurs de bord ou à l'équipage d'avoir une vision globale des aspects pertinents pour la conduite du navire. Ces systèmes restent vulnérables au piratage, principalement en raison de la faible sécurité des protocoles de communication et de la conception du réseau du navire, comme les terminaux de communication par satellite exposés à Internet, les interfaces administratives accessibles par des protocoles non sécurisés (Telnet et HTTP). Les réseaux de bord n'utilisent généralement pas l'authentification et le chiffrement des messages. Cette situation peut être encore plus aggravée par une mauvaise hygiène de sécurité de la part des utilisateurs qui utilisent trop souvent des identifiants de connexion par défaut, faciles à pirater, ainsi qu'une mauvaise gestion des mots de passe.

Les systèmes de commande
Les systèmes de contrôle des moteurs supervisent et contrôlent les systèmes de propulsion des navires. Il s'est avéré qu'un système de contrôle de moteur largement utilisé présentait des défauts de conception majeurs en matière de sécurité. Plus précisément, l'utilisation d'informations d'identification codées en dur qui ne pouvaient pas être modifiées par les utilisateurs, l'incapacité d'authentifier le dispositif d'envoi et la transmission en clair d'informations sensibles. Ces failles pourraient permettre à un attaquant d'accéder aux unités et de contrôler les moteurs connectés, de déterminer quels capteurs sont présents et en service, de lire ou de modifier les informations de configuration d'autres paramètres comme transmettre des informations falsifiées aux unités de contrôle.

Les systèmes de vidéosurveillance
Les systèmes de vidéosurveillance à bord des navires n'ont pas été largement pointés du doigt comme étant vulnérables aux cyberattaques, ils n'en sont pas moins concernés. En 2017, une compagnie maritime basée en Louisiane a signalé que les caméras d'un quart de sa petite flotte de bateaux avaient été compromises. Les pirates ont exploité une faiblesse dans les procédures d'authentification de la caméra et y ont accédé à distance via Internet. Il s'est avéré que les hackers avaient changé les

paramètres de contraste rendant les caméras aveugles. Comme tous les appareils inhérents à l'IoT, ces caméras sont accessibles facilement et disposent d'une très faible politique de sécurité. À l'image des caméras embarquées dans les voitures de la police Ukrainienne, qui avait été rendue accessibles via Internet afin de suivre le conflit Russo-Ukrainien début 2022 [7].

L'enregistreur de données de voyage (VDR)

Le VDR (*Voyage Data Recorder*) saisit et enregistre les données dynamiques liées à la navigation du navire. Cela concerne par exemple les conversations sur la passerelle, les signaux audio VHF, le Radar, les informations GNSS, la vitesse ou le cap. Bien que ce système soit parfois comparé à la boîte noire des avions, de nombreuses études ont montré que les VDR peuvent être trafiqués et modifiés par l'équipage du navire ou par un pirate informatique. En 2015, le VDR VR-3000 de Furuno a été le premier à montrer qu'il était susceptible de faire l'objet d'un accès non autorisé, d'une modification ou d'une suppression de données.

II.5.2 Problématique de la cybersécurité maritime

Sur un navire des incidents peuvent être causés par le ciblage des réseaux informatiques à bord mais aussi des systèmes de navigation et des ICS souvent accessibles par Internet [134]. Les vulnérabilités en matière de cybersécurité peuvent ainsi être exploitées par des agents hostiles et ont pour conséquences par exemple l'arrêt des navires ou la fermeture de canaux de navigation [134]. Compte tenu de la fréquence croissante des cyberattaques dans le domaine maritime, les CPS à protéger englobent en premier lieu [90] :

- ✓ les systèmes de communication et les trafics numériques critiques ;
- ✓ les informations et les bases de données critiques ;
- ✓ les systèmes automatisés des terminaux et des navires ;
- ✓ les infrastructures critiques.

Le tableau Tab. II.1 résume les principaux risques associés aux différents systèmes navals (identifiés dans la thèse de Perdo Merino-Laso [97]).

Bien que les actifs de l'industrie maritime soient en grande partie mécaniques avec comme principale menace l'environnement maritime, elle n'est pas à l'abri de perturbations en lien avec les technologies numériques (communications, ordinateurs, Internet, ICS, etc.) [43]. D'après plusieurs rapports officiels, il apparaît que la communauté maritime n'est pas véritablement résiliente du point de vue de la cybersécurité et n'a pas véritablement de directives, de protocoles ou de réponses spécifiques pour dissuader ou empêcher des cyberattaques majeures [56]. Direnzot *et al.* [38] ont attiré l'attention sur la gravité des cyberattaques dans le secteur maritime et sur le fait que les vulnérabilités ne sont que peu ou pas connues. En 2016, Van Niekerk [133] montre ainsi que le secteur

7. https ://reflets.info/articles/reflets-s-invite-par-hasard-dans-les-voitures-de-police-ukrainiennes.

TABLE II.1 – Les risques associés aux différents systèmes navals.

Systèmes	**Exemples de sous-Systèmes**	**Risques associés**
Position	GPS, GLONASS, Galileo, Beidou, IRNSS, QZSS, NAVSAT, LORAN.	Détournement du navire, risques élevés de leurrage et brouillage GNSS.
Navigation	Gyro Compass, Lock, Speedometer, Echo Sondeur.	Détournement du navire, mauvaises prises de décisions.
Cartographie.	ECS, ECDIS.	Détournement des routes et des informations affichées sur les systèmes cartographiques.
Capteurs météorologiques.	Centrale Météo, prédictions.	Calcul de routes non optimales et potentiellement dangereuses.
Environnement.	AIS, Radar, Sonar.	Falsification d'information, leurrage, détournement des données reçues, collisions.
Communication.	Radio VHF, téléphonie, réseau, Internet.	Espionnage, sabotage, isolement.
Manoeuvrabilité, Contrôle.	Propulsion, gouvernail ou barre.	Perte de contrôle, détournement, sabotage.
Systèmes informatiques.	Serveurs et ordinateurs de bord (pilote automatique, calcul de routes, etc.).	Calcul de routes potentiellement dangereuses.
Supervision.	Pression de fluides, niveau des cuves (ultrasonique, ondes sonores, sondes), température, tachymètre, flux de fioul, détection de flamme.	Dissimulation de sabotages et pannes, prise de mauvaises décisions.
Sécurité et surveillance du navire.	CCTV (Caméras de surveillance), capteurs incendies, voies d'eau, indicateur de MOB (homme à la mer).	Fausses alertes, non-détection de danger.
Surveillance extérieure	Hélicoptère, drone aérien (UAV : Unmanned Aerial Vehicle), drone de surface, drone subaquatique (ROV : Remotely Operated Vehicle).	Perte de signal, perte de systèmes, leurrage ou brouillage, détournement pour saboter une installation.
Supervision secondaire.	Indicateur d'état de portes, contrôles de lumières, alarmes chambre froide.	Problèmes d'habitabilité et de santé.

maritime est l'un des plus touchés de tous les modes de transport en nombres d'incidents signalés. Néanmoins il est à noter que les principaux impacts dans le secteur maritime sont principalement liés à la perturbation des opérations et à la perte de confidentialité des données. Mais rien ne garantit, dans un avenir proche, que cela ne puisse évoluer vers des impacts plus dramatiques aussi bien économiques qu'environnementaux (marées noires, blocages portuaires, détournement de marchandises, etc.). On peut pour exemple citer l'accident d'une plate-forme pétrolière au large des côtes africaines qui a basculé suite à l'arrêt d'un des systèmes de contrôles lors de son déplacement lié à une infection par un logiciel malveillant [35].

Une analyse rétrospective des incidents de cybersécurité maritime, allant de la période 2010 à 2021, a été récemment conduite par Meland *et al.* [96]. Chaque incident est lié à une taxonomie de points d'attaque liés à des systèmes embarqués ou débarqués. Les auteurs montrent sur la base de sources ouvertes, que même si le secteur maritime n'a pas connu le plus grand nombre d'attaques, comparé par exemple au secteur bancaire, l'impact des cyberattaques est très important. Plus exactement les incidents sont à faible fréquence, mais à fort impact, ce qui les rend difficiles à prévoir et à préparer. Il ressort de cette analyse que la surface d'attaque numérique a sensiblement augmenté [96]. Jensen montre par une analyse détaillée que le secteur maritime ne dispose pas d'une approche normalisée de la cybersécurité [63]. Il fait remarquer qu'une approche nationale serait contre-productive et une norme internationale obligatoire, bien que nécessaire, serait longue à mettre en œuvre. Pour établir des recommandations, l'auteur propose à la communauté du domaine d'examiner en détail les caractéristiques spécifiques du secteur maritime en matière de cybersécurité, et de recenser les vulnérabilités existantes et de cyberattaques signalées [63]. Burton [27] montre que cette approche communautaire peut être en réalité un réel avantage dans le cadre de la cyberrésilience maritime, car cela permet une redondance dans les informations. Ce regroupement des installations permet de bénéficier d'une assistance technique mutuelle plus proactive. Nagurney et Shukla [100] confirment l'intérêt pour ce type de modèle de coopération massive dans un cadre de cybersécurité. Toujours selon les auteurs, cette approche communautaire est un très bon moyen de lutter efficacement contre la menace des logiciels malveillants [35]. Le principe étant de ne pas avoir de maillon faible dans la chaîne pouvant stopper la chaîne tout entière.

II.5.3 Vers une prise de conscience des vulnérabilités

La mise en œuvre des systèmes automatisés dans les infrastructures maritimes critiques (automatisation des terminaux) et sur les navires (automatisation des navires) est en constante augmentation et par conséquent, la possibilité d'augmenter les cyberattaques [136, 43]. Il est important de noter que la mise à niveau des composants critiques de communication, de navigation et d'exploitation des infrastructures est souvent bien plus lente dans le domaine maritime que dans d'autres secteurs industriels en prenant en compte la durée de vie des navires. Finalement, les mêmes ex-

perts notent que la sensibilisation à la cybersécurité dans le secteur maritime est plus faible que dans d'autres secteurs des transports alors que l'automatisation est tout aussi importante [50]. Par ailleurs un navire en mer dispose rarement d'un expert cyber dans son équipage. La liaison du navire est reliée avec la terre par des liaisons satellites, mais les bandes passantes sont étroites et onéreuses, limitant la possibilité de surveillance et d'intervention à distance. Le navire navigue dans un cyberespace mondialisé constitué de réseaux fortement interdépendants [110]. Le cyberespace et son infrastructure sous-jacente sont vulnérables à un large éventail de risques résultats à la fois de menaces et de dangers physiques et cybernétiques. Enfin, rappelons que l'une des raisons majeures du transport maritime est la chaîne d'approvisionnement des biens et des services. La cybersécurité de celle-ci est de plus en plus importante [109]. Ainsi, Khan et Estay [71] ont identifié que les cyberrisques des flux maritimes sont des sujets relativement nouveaux. L'une de leurs principales conclusions est qu'il n'existe pas véritablement de réglementations spécifiques pour traiter les problèmes de résilience de cybersécurité de la chaîne d'approvisionnement. Newberry propose de regrouper les menaces potentielles sur les infrastructures maritimes en cinq grandes catégories [102] :

- ✓ les pirates informations ou "hacktivistes" (hackers politiquement actifs) ;
- ✓ les organisations criminelles ;
- ✓ les terroristes ;
- ✓ l'industrie par l'espionnage industriel ;
- ✓ les gouvernements nationaux.

Il est intéressant de noter que les cyberattaques sont des problématiques nouvelles au regard des actes de piraterie et de brigandage plus classiques (abordages et prises d'otages). La sûreté maritime a mis l'accent sur le terrorisme et la piraterie. Issus des enquêtes et rapports sur les accidents, les aspects de sécurité se concentrent essentiellement sur l'infrastructure pour la prévention de la pollution de l'environnement et l'atténuation des accidents. Cela concerne aussi les collisions et la capacité de survie des navires, mais trop souvent cela prime sur la cybersécurité des systèmes informatiques [90]. Ainsi, l'accent mis sur l'aspect de cybersécurité est plus récent. À noter que les atteintes à la cybersécurité dans l'industrie maritime couvrent souvent d'autres actes malveillants plus classiques tels que les trafics de drogues [73].

Pour lutter contre ces cyberattaques, de nombreuses réglementations et recommandations ont fait leurs apparitions pour guider l'industrie maritime sans parler des politiques spécifiques à chaque pays [46]. Plusieurs organismes sont d'ailleurs à l'origine de ces recommandations. Parmi eux, l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), en collaboration avec la Direction des Affaires maritimes (Ministère de la Transition écologique et de la Cohésion des territoires et ministère de la Transition énergétique), propose notamment en 2016 un "*Guide des bonnes pratiques de sécurité informatique à bords des navires*" pour la prévention des incidents et

des attaques informatiques à bord. Cette recommandation fait d'ailleurs suite au précédent "*Guide des bonnes pratiques de l'informatique (CGPME - ANSSI mars 2015)*",[8] mais cette fois en s'adaptant aux contraintes et spécificités du transport maritime grâce à la contribution des compagnies maritimes françaises. De son côté, l'OMI a publié en 2017 des "*Directives sur la Gestion des cyberrisques maritimes*"[9] visant à mieux appréhender les cyberrisques. Cela permet aux compagnies maritimes de prendre conscience des vulnérabilités auxquelles elles sont potentiellement soumises afin d'améliorer la sûreté et la sécurité du transport maritime qui se doivent d'être dorénavant plus résilientes face à ces nouveaux risques (Fig. II.10).

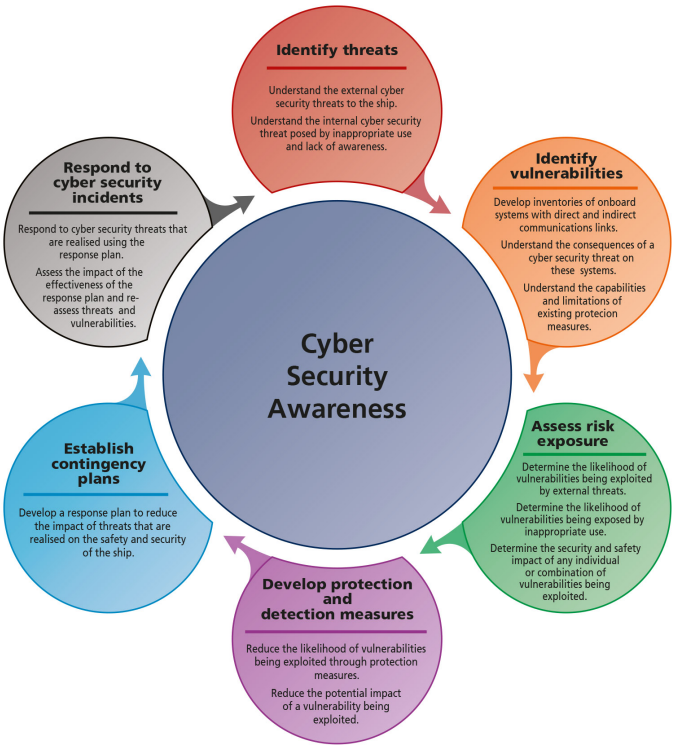


FIGURE II.10 – Vue d'ensemble de la cybersécurité du point de vue de la connaissance de la situation (*Cyber Security Awareness*).

En France, la question est prise très au sérieux avec l'émergence de nouvelles associations ayant pour but de mieux protéger le monde maritime face aux cybermenaces. L'une d'entres-elles, *France Cyber Maritime* en est un très bon exemple. Lancée en 2020, cette association, dont le siège social est idéalement placé à Brest (nommée en 2022 Capitale européenne de la mer), a été créée pour faire face aux enjeux de la numérisation du monde maritime au niveau national. En collaboration directe avec les armateurs et les industriels concernés, elle bénéficie du soutien de l'ANSSI et développe progressivement une M-CERT (*Maritime Computer Emergency Response Team*) assurant un lien direct avec des analystes cyber lorsque survient un incident dans le domaine.

8. https ://www.ssi.gouv.fr/actualite/guide-des-bonnes-pratiques-de-securite-informatique-a-bord-des-navires/
9. https ://www.imo.org/fr/OurWork/Security/Pages/Cyber-security.aspx

II.6 Conclusions

La numérisation des activités du domaine maritime est une tendance marquée et qui est solidement établie. Un possible retour en arrière n'est clairement pas envisageable. L'ensemble des innovations (informatiques, télécommunications, systèmes autonomes, énergies vertes, etc.) sont synonymes de performance et d'innovation et de fortes transformations de la « Supply Chain » maritime ainsi que l'amélioration des systèmes avec de véritables ruptures technologiques (navires autonomes, assistance à la navigation, optimisation de la consommation, etc.). Il y a donc un véritable enjeu pour le transport maritime et les constructeurs de navires. Malheureusement, le manque de préparation de l'industrie et des infrastructures face aux cybermenaces suscite de nombreuses consternations et interrogations. Certains analystes notent que l'industrie maritime a entre 10 et 20 ans de retard [29] par rapport à d'autres secteurs industriels (aviations, nucléaires, etc.). Les défis de la cybersécurité maritime sont colossaux et incluent des problématiques extrêmement vastes allant de la sécurisation des navires en mer (navigation, propulsion, communication, ICS, etc.) à celle des infrastructures portuaires (manutention et circulation des marchandises, stockage des cargaisons, ICS, etc.) [66]. Dans ce chapitre nous avons détaillé et énuméré les spécificités propres aux systèmes navals ainsi que leurs vulnérabilités associées permettant de répondre en partie à la Question de Recherche **QR1**.

Le chapitre suivant portera dans un premier temps sur des incidents de cybersécurité ayant eu lieu dans le monde maritime. Dans un second temps, quelques solutions pour lutter contre ces menaces seront proposées avant de discuter des principes de la détection d'anomalie appliquée à ce domaine relativement spécifique qu'est le monde maritime.

Chapitre III

De la Cyberattaque à la Cybersécurité dans le Domaine Maritime

Sommaire

III.1 Introduction

Les prises de décision par un marin en pleine mer concernant sa mission et les bonnes opérations des systèmes se font à partir de données qui sont en général non vulnérables, car jusqu'à récemment les navires étaient hors de portées d'éventuelles cyberattaques qui peuvent se produire. Avec l'avènement d'Internet et le déploiement à grande échelle des réseaux de communications à bord d'un navire, ce dernier devient vulnérable à cause des cyberattaques et le marin voit alors la

sécurité et la sûreté remises en question et ceci, quelle que soit la localisation du navire. En effet, les ICS et les systèmes de navigation à bord des navires se trouvent de plus en plus vulnérables aux cyberattaques.

Dans ce chapitre, des incidents de cybersécurité ayant eu lieu dans le secteur maritime, ou dans d'autres secteurs connexes sont énumérés à titre d'exemple. Ce chapitre propose d'énumérer quelques approches de solutions en matière de détection d'anomalies en fonction des systèmes considérés sur un navire. Le principe de détection d'anomalie est discuté en précisant leurs limitations spécifiques et un état de l'art des techniques existantes est réalisé. Comme le montre la figure III.1, ce chapitre permet également de répondre à la **QR1**.

Correspondance : Question de Recherche / Chapitre					
	Chap. II	**Chap. III**	Chap. IV	Chap. V	Chap. VI
QR I					
QR II					
QD I					
QR III					

FIGURE III.1 – Tableau de correspondances entre les Questions de Recherche et les Chapitres.

III.2 Cyberattaques du monde industriel vers le monde maritime

L'objectif de cette section est de présenter une synthèse de quelques exemples d'attaques spécifiques et significatives, qui mettent en lumière les véritables enjeux des cyberattaques et de la-cybersécurité aussi bien dans le domaine industriel (nucléaire, métallurgie, etc.) que dans le domaine maritime (navires, ports, etc.) [72, 116, 131].

III.2.1 Exemples de malware/ransomware

Si le ransomware (ou rançongiciel [1]) n'est plus à présenter, il est important de connaître la finalité d'une telle attaque. L'objectif est de chiffrer les données (prendre en otage) des fichiers d'un ordinateur jusqu'à ce qu'une rançon soit payée [104]. La facilité d'une telle attaque repose sur le fait que ce type de logiciel, permettant de déclencher une attaque rançonnée, peut être facilement acheté et personnalisé (on parle notamment de Ransomware "As a Service" [2]), ce qui est très attrayant

1. Le malware est un programme malveillant développé dans le but de nuire à un système informatique sans le consentement de l'utilisateur alors que le ransomware a la particularité de prendre en otage les données d'un utilisateur contre une rançon

2. https ://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

aussi bien pour les cybercriminels professionnels que pour les novices [59]. Parmi l'ensemble des malwares/ransomwares existants, quelques-uns sont très connus comme par exemple Petya, cette famille de logiciels malveillants de chiffrement découverts pour la première fois en 2016 [16]. Ce malware cible les systèmes basés sur Microsoft Windows, infectant l'enregistrement de démarrage principal pour exécuter une charge utile qui chiffre la table du système de fichiers d'un disque dur et empêche le système d'exploitation de démarrer. Le malware Petya aurait ainsi infecté des millions de systèmes au cours de sa première année de sortie. Des industriels comme Saint-Gobain, les laboratoires Merck ou l'armateur Maersk ont été impactés par ce ransomware.

Les navires marchands peuvent très bien être affectés par un malware/ransomware, soit directement, soit à distance via les systèmes et services utilisés par les armateurs. Le rapport 2020 du BIMCO intitulé *"Guidelines on Cyber Security Onboard Ships - Version 4"*[3] détaille ainsi plusieurs cas d'infections par ransomware survenus dans le secteur maritime [3, 126].

III.2.2 Cyberattaques de compagnies maritimes

En septembre 2020, la compagnie maritime française CMA-CGM a confirmé avoir été victime de cyberattaques par le ransomware Ragner Locker, qui a impacté les serveurs périphériques, un grand nombre de systèmes d'information et les sites web ont été inaccessibles pendant presque toute une journée[4]. En septembre 2020, c'est l'entreprise CMA-CGM qui été frappé une deuxième fois par un autre ransomware[5]. L'entreprise a informé ses clients qu'elle avait subi une fuite de données sur des informations client limitées impliquant le nom et le prénom, l'employeur, la fonction, l'adresse e-mail et le numéro de téléphone. Les entreprises MSC et COSCO, ont aussi été victimes de piratages cybernétiques ces dernières années, entraînant des pertes massives [4, 75, 126]. Enfin, déjà fortement impactés par la pandémie, les secteurs maritime et portuaire ont vu ces diverses attaques s'ajouter à la vingtaine de cyberattaques (connue publiquement) en 2020 selon France Cyber Maritime.

III.2.3 Cyberattaques des ICS

La gestion de la sécurité des systèmes d'information sur un navire repose principalement sur deux points réellement problématiques :

1. les systèmes SCADA ont classiquement des cycles de vie courts entre 3-5 ans alors que les réseaux industriels (le navire) sont plutôt sur des cycles de 25-30 ans voir même 40 ans. Cela rend difficile la mise à niveau cybernétique de l'ensemble des systèmes fixes.

3. https ://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships
4. https ://splash247.com/cma-cgm-confirms-cyber-attack-alliance-partner-coscos-site-suffers-brief-outage/
5. https ://splash247.com/cma-cgm-hit-by-another-cyber-attack/

2. la culture de programmation (développements informatiques, mises à jour, etc.) de ces équipements ne va pas, traditionnellement, dans le sens d'une approche sécuritaire [135]. D'autant plus que les systèmes informatiques sur un navire reposent, de plus en plus, sur la mise en œuvre de produits standards non durcis (« présents sur étagères ») multipliant les possibilités d'attaques cyber.

Il est indéniable que les ICS présentent de nombreuses vulnérabilités d'un point de vue cybersécurité [120]. Les causes de ces vulnérabilités peuvent provenir, par exemple, d'installations défectueuses (pare-feu mal configurés, etc.), de failles logicielles (absence ou faible niveau d'authentification, etc.) ou encore l'utilisation de protocoles peu sécurisés (Modbus et DNP3 sur TCP/IP, etc.) [122]. Dans [94], Laughlin *et al.* regroupent les vulnérabilités ICS en cinq couches : matériel, firmware, logiciel, réseau et processus ICS. Une discussion des caractéristiques de chaque couche, des attaques, des menaces et des vulnérabilités possibles sont expliquées en détail dans [70]. Dans cette partie, nous avons décidé de nous focaliser essentiellement sur des attaques basées sur la propagation de logiciels malveillants via les réseaux industriels.

En 2007, BlackEnergy Malware [41] [6] est un virus de type "Cheval de Troie" [7] a permis de prendre à distance le contrôle d'un ordinateur. Initialement, il réalise des attaques par déni de service distribué (DDoS) [8]. L'attaque est généralement diffusée via une pièce jointe dans un e-mail. En 2010 puis en 2014 et encore aujourd'hui, différentes versions (BlackEnergy2, BlackEnergy3) apparaissent couramment, offrant des capacités d'attaques accrues [138].

En 2010, Stuxnet [9] a permis de saboter furtivement le programme nucléaire de l'Iran. Ce virus informatique vise les systèmes SCADA et les PLC mis au point par Siemens sous environnement Windows, et plus spécifiquement les centrifugeuses [26, 30, 4]. L'origine de l'infection provient de l'utilisation d'une clé USB à partir de laquelle le ver s'est propagé à travers les équipements du réseau à la recherche des machines en charge de contrôler les automates industriels des centrifugeuses. Une fois trouvé, le vers Stuxnet a reprogrammé le SCADA afin de saboter l'installation.

En septembre 2013, Havex [10] un virus aussi de type "Cheval de Troie" d'accès à distance, est utilisé dans le cadre d'une campagne d'espionnage internationale ciblant les ICS et des outils de supervision SCADA de plusieurs secteurs industriels situés en Europe et aux États-Unis [11].

Le 17 décembre 2016, un framework de logiciels dénommé Industroyer [22, 36] provoque un « black-out » électrique dans la capitale ukrainienne, Kiev, durant environ une heure. Il s'avère que ce malware très sophistiqué a été développé, tout comme Stuxnet, spécifiquement pour interférer

6. https ://en.wikipedia.org/wiki/BlackEnergy
7. https ://fr.wikipedia.org/wiki/Cheval$_{d}e_{T}roie_{(}informatique)$
8. https ://en.wikipedia.org/wiki/Denial-of-service$_{a}ttackDistributed_{a}ttack$
9. https ://securelist.com/stuxnet-zero-victims/67483/
10. https ://securid.novaclic.com/cyber-securite-industrielle/havex-dragonfly-russe.html
11. https ://www.lemondeinformatique.fr/actualites/lire-des-variantes-du-malware-havex-ciblent-les-utilisateurs-des-systemes-scada-57915.html

avec les ICS [12]. Dans le cas présent, il cible les réseaux électriques et plus spécifiquement les stations de distribution (relais et coupe-circuits).

Ainsi, les menaces persistantes avancées (*Advanced Persistent Threat* - APT) de type Titan Rain (en 2003 - un des premiers APT [13]), BlackEnergy (en 2007), Stuxnet (en 2009), ou Industroyer (en 2016) ont montré leurs capacités à cibler furtivement des entités spécifiques dans le domaine de l'industrie comme le nucléaire, les réseaux électriques ou les usines de traitement des eaux [105, 4, 76].
Ce type de système présente de nombreuses failles, telles que l'absence de développement sécurisé et le faible niveau de protection des accès, des systèmes de contrôle et industriels non sécurisés, les systèmes d'information de gestion qui ne sont pas hermétiques, la non-actualisation et les faiblesses des protocoles de gestion actuels et la supervision des anomalies du système qui est presque inexistante [92, 79]. Par conséquent, les ICS utilisés dans ce type d'infrastructures critiques sont sujets à des cyberattaques et malheureusement un navire est équipé du même type de matériel et notamment de nombreux PLC. Or, là encore, les firmwares (micrologiciels) des PLC sont vulnérables à un nombre d'attaques comme l'arrêt et le démarrage du CPU, les attaques par force brute (*Bruteforce Attack*), l'injection de fausses commandes et réponses, le déni de service (DDoS) ou la lecture et l'écriture de la mémoire.

Dans le domaine maritime, les mise en œuvre de CPS présentent les mêmes problèmes de sécurité que tous les systèmes informatiques ou IoT. Paradoxalement, dans le monde maritime, il existe peu d'attaques documentées (peut être pour des raisons de sécurité ou encore la volonté de ne pas entacher les crédibilités ou réputations des acteurs et sociétés du domaine).

III.3 Cyberattaques spécifiques du secteur maritime

Le secteur maritime est devenu un écosystème complexe, réunissant des acteurs et des organisations de tailles, de maturité, de complexité et de portée opérationnelle différentes. La connectivité accrue et la convergence des systèmes IT et OT exposent les opérations maritimes à de nouvelles menaces qui peuvent avoir de graves répercutions économiques et de réputation. Le M-CERT de l'association France Cyber Maritime alimente en continu une base de données publique répertoriant tous les incidents survenus dans des systèmes maritimes durant les 40 dernières années [14]. Il ressort que les codes malveillants et notamment les rançongiciels (ransomware) sont devenus les types d'attaques les plus courantes dans le monde maritime et portuaire au cours des trois dernières années (Fig. III.2).
Aussi dans un contexte où chaque action professionnelle quotidienne est rythmée par les restric-

12. https ://www.welivesecurity.com/wp-content/uploads/2017/06/Win32*Industroyer.pdf*
13. https ://cyware.com/news/remembering-operation-titan-rain-c54ad3e4
14. https ://gitlab.com/m-cert/admiral

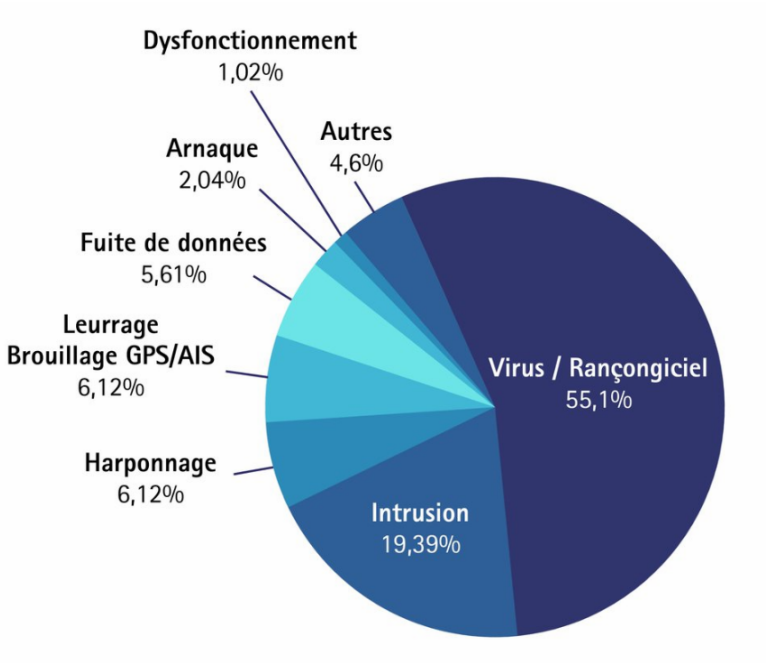


FIGURE III.2 – Typologie des évènements de cybersécurité maritime de 1980 – 2021 (Source M-CERT France Cyber Maritime).

tions de voyage à l'échelle mondiale, les mesures de distanciation sociale et la récession économique, la capacité d'autodéfense des entreprises s'amenuisent logiquement. Par exemple, les techniciens des OEM (*Original Equipment Manufacturer*) ayant plus de mal à se déplacer pour entretenir les systèmes à bord des navires, ils opèrent à distance ce qui oblige l'opérateur à contourner les protections de sécurité, ouvrant ainsi potentiellement une brèche. Alors que les budgets sont réduits et en l'absence d'ingénieurs de service à bord des navires, nous voyons le personnel des navires et des plateformes offshore connecter leurs systèmes à l'Internet des réseaux côtiers, à la demande des OEM, pendant de brèves périodes de temps afin d'effectuer des diagnostics et télécharger eux-mêmes les mises à jour et les correctifs logiciels. La cybersécurité sur un navire est mise à mal par le non-respect de ces procédures et surtout par la situation exceptionnelle qui rend impossibles celles en cours.

III.3.1 Études de pénétration cyber : challenge de NavalDome

La société de cybersécurité maritime NavalDome [15] a effectué des tests de pénétration sur le navire *Zim Genevoa* en 2017, en réussissant trois types de cyberattaques réalisées sans la coopération de l'équipage du navire.

✓ ECDIS : les attaquants ont envoyé un e-mail, via la liaison satellite du navire, avec une pièce

15. https ://navaldome.com/threat.html

jointe malveillante à l'ordinateur du capitaine, qui est régulièrement connecté à l'ECDIS pour les mises à jour des cartes de navigation. Ainsi, lors du cycle de mise à jour des cartes, le virus s'est naturellement retrouvé installé sur l'ordinateur ECDIS. Le virus a alors pu modifier la position du navire sans modifier l'affichage, de subtiles modifications ont été apportées aux informations relatives à la position, au cap, à la profondeur et à la vitesse sans que personne sur la passerelle ne s'en aperçoive. Il s'agit d'une exploitation très spécifique au système ciblé.

- ✓ Radar : Cette attaque a utilisé le commutateur du réseau Ethernet qui relie le Radar, l'ECDIS, le VDR et les réseaux du système d'alerte de la passerelle. Le logiciel malveillant a ainsi supprimé les cibles des systèmes Radars de la passerelle, rendant le navire aveugle aux navires proches. L'affichage du système montrait que le Radar était parfaitement opérationnel (seuils de détection correctement réglés). Les opérateurs de la passerelle n'avaient aucune raison de soupçonner une défaillance systémique.
- ✓ Système industriel : Un virus a été inséré dans un ICS par le biais d'une clé USB infectée trouvée par un membre du personnel, qui a inséré le dispositif directement dans un ordinateur en réseau. Le virus s'est exécuté automatiquement et a attaqué d'autres systèmes informatiques auxiliaires. La première cible a été le système de ballast ; les valves et les pompes ont été perturbées et ont cessé de fonctionner, mais l'écran affichait des opérations normales.

Les résultats des études [19, 96] montrent que le secteur maritime connaît généralement des incidents à faible fréquence, mais à fort impact et cela les rend particulièrement difficiles à prévoir. Ces résultats ont également permis de déduire que les attaquants utilisent une variété de points d'entrées et des techniques d'attaques différentes.

III.3.2 Cyberattaques sur le secteur portuaire

Nous faisons dans ce qui suit une synthèse de quelques attaques de grands ports maritimes, qui sont symptomatiques de la situation [16] :

- ✓ En 2013, un cartel de la drogue détourne le système d'aiguillage de conteneurs du port d'Anvers. Il s'avère que le réseau informatique est espionné depuis juin 2011, date à laquelle le réseau aurait été infiltré par des malwares et notamment un "*Keylogger*" (enregistrement des frappes clavier et capture de mots de passe des opérateurs) ;
- ✓ Le 30 juin 2017, le port de Rotterdam a été infecté par le ransomware Petwarp, qui a rendu inopérant les terminaux, paralysant ainsi les activités de la filiale APMT du groupe Møller-Maersk. Notons que le port de Rotterdam est l'un des ports qui investissent le plus dans l'automatisation de ses processus opérationnels (Smart Port intégrant l'IoT et l'IA pour accroître ses performances de production) [69] ;

16. https ://cybermaretique.fr/les-incidents-connus/ ou : https ://www.stormshield.com/fr/actus/cybermaretique-petite-histoire-des-cyberattaques-contre-le-secteur-portuaire/

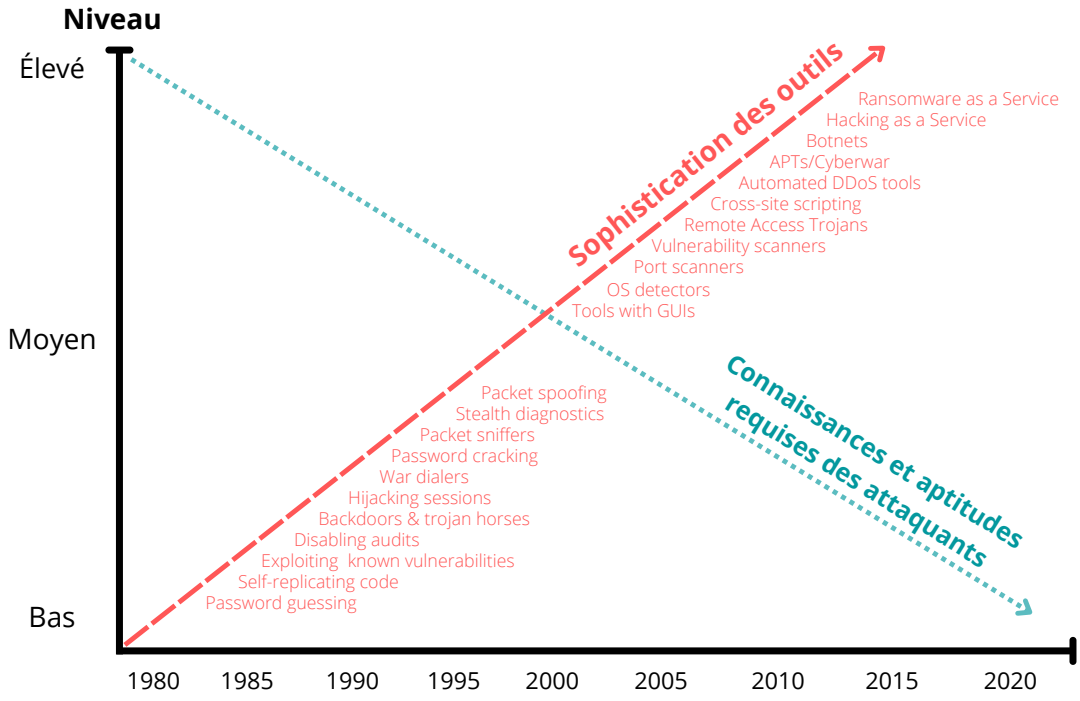


FIGURE III.3 – Évolution de la complexité des outils de hacking comparé aux connaissances des attaquants.

- ✓ Le 20 septembre 2018, le port de Barcelone a été visé par une attaque sur ses installations informatiques impactant fortement les processus de chargement/déchargement des marchandises. Quelques jours plus tard, c'est le port de San Diego qui subit le même type d'attaque. Les impacts vont réduire les capacités de gestion administratives du port ;
- ✓ En mars 2020, le port de Marseille a subi les effets du ransomware Mespinoza/Pysa. Dans ce cas, il s'avère que les infrastructures maritimes ne sont pas visées directement, mais font les frais de leur interconnexion avec les systèmes d'information de la métropole d'Aix-en-Provence, qui était la cible initiale et principale de cette attaque ;
- ✓ En mai 2020, c'est au tour du port iranien Shahid Rajaee de subir une cyberattaque occasionnant une interruption quasi complète de l'ensemble des systèmes informatiques permettant de réguler les flux des navires, des camions, etc. créant un véritable chaos sur les voies navigables et sur les routes ;
- ✓ En novembre 2020, le port de Kennewick est infecté par un ransomware verrouillant l'accès à ses serveurs. Les autorités portuaires mettront plus d'une semaine pour rendre l'ensemble du système opérationnel grâce à des sauvegardes ;
- ✓ En juillet 2021, le principal gestionnaire de fret d'Afrique du Sud a été massivement attaqué (de type ransomware), rendant inutilisable l'ensemble des systèmes informatiques des quatre

grands ports du pays (Cape Town, Ngqura, Port Elizabeth et Durban).

✓ En janvier 2022, les ports de Gand et Anvers ainsi que celui d'Hambourg ont signalé avoir été la cible de plusieurs cyberattaques, de type ransomware, provoquant des perturbations (arrêt des déchargements/chargements) importantes notamment sur les terminaux pétroliers des différents ports [17].

III.3.3 Cyberattaques des systèmes de positionnement par satellites

Comme présenté au Chapitre II, l'expérience d'usurpation d'identité réalisée par des chercheurs de l'Université du Texas à Austin a montré que la modification de la route et le cap d'un yacht à l'insu de l'équipage est possible, et ce en leurrant le GPS. Cette expérience, qui a été très médiatisée, a montré la vulnérabilité du GPS et s'est répétée malheureusement plusieurs fois. Si en 2017, seules cinq attaques ont été signalées, ce chiffre passe à 31 incidents en 2019. Selon des études réalisées par des associations à but non lucratif comme SkyTruth ou encore Global Fishing Watch, il apparaît clairement comme une forte augmentation des navires dit "fantômes" dans toutes les mers du monde, y compris des navires militaires [18]. Classiquement, un navire est qualifié de "fantôme" s'il est signalé à un endroit où il ne se trouve pas. Ces fausses positions peuvent résulter d'émetteurs (GPS/AIS) défectueux ou encore d'une mauvaise utilisation des systèmes. Les analyses fines des anomalies dans les positions GPS montrent qu'elles peuvent être fausses (il n'y a en réalité aucun navire à l'endroit donné par l'AIS et cela ne correspond à aucun navire existant), mais aussi détournées (dans ce cas, la vraie position GPS est falsifiée : un navire usurpe et utilise les informations d'un vrai navire pouvant se trouver à l'autre bout du monde). Enfin, il peut y avoir une attaque via le brouillage ou le leurrage des signaux GNSS et dans ce cas, l'attaquant envoie directement au navire de fausses positions [19].

✓ Le 24 juin 2017, le capitaine du pétrolier *Atria* au large de Novorosiysk indique, dans un premier temps, la perte du signal GPS puis, dans un deuxième temps, le GPS indique que le navire se situe près de l'aéroport de la ville Russe de Gelendzhik alors qu'il est en réalité à 25 milles de la ville. Cet incident va impliquer plus d'une vingtaine de navires ce même jour. Selon des experts, cette attaque de grande ampleur suppose de fortes capacités de guerre électronique. A ce jour, il s'avère que les interférences GNSS, les pertes de signal et la réduction de la précision de la position en mer Noire se poursuivent, plaçant couramment des navires sur les aéroports de Sochi, St-Petersbourg ou encore de Vladivostok.

17. https ://www.lemonde.fr/international/article/2022/02/03/cyberattaque-des-sites-portuaires-vises-en-allemagne-en-belgique-et-aux-pays-bas_6112185_3210.html

18. https ://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/ ou https ://www.businessam.fr/comment-des-navires-de-guerre-fantomes-apparaissent-sur-toutes-les-mers-du-globe

19. https ://cybermaretique.fr/les-incidents-connus/ou https ://www.revistaejercitos.com/fr/2020/02/27/suplantacion-de-gps/

- ✓ En juillet 2017, le pétrolier britannique *Stena Impero* est arraisonné par des garde-côtes dans le détroit d'Ormuz pour avoir pénétré illégalement dans les eaux territoriales après une modification inattendue de sa route. Une première analyse de la trajectoire du navire, à l'aide de satellites, montre en effet une modification soudaine de sa route. Le pétrolier a reçu des signaux AIS falsifiés le faisant alors dévier vers les eaux iraniennes alors qu'il naviguait dans le détroit.
- ✓ Depuis 2018, le port de Shanghai connaît des attaques GPS et AIS. D'après la police fluviale (*China Maritime Safety Administration* - CMSA), il semble que cela soit l'œuvre de contrebandiers locaux (transportant du sable interdit du fleuve Yangtze River) qui usurpent les signaux AIS d'autres navires légitimes afin d'échapper à la surveillance des autorités. Toujours dans la même région, en juin 2019, on peut citer la falsification d'un signal AIS par un pétrolier soupçonné de contrebande de pétrole ayant éperonné un patrouilleur de la CMSA afin d'échapper à son arraisonnement [20]. L'usurpation d'identité par GPS n'est alors plus l'affaire des États.
- ✓ En janvier, toujours à Shanghai, le capitaine du porte-conteneurs le *Manukai* naviguant à l'embouchure de la rivière Huangpu note soudain l'apparition et la disparition d'un autre navire navigant à 7 nœuds dans le même chenal alors même que celui-ci est resté à quai en réalité. Alors que le *Manukai* arrivait à son poste d'amarrage, ses systèmes GPS et AIS sont brusquement tombés en panne. Le navire n'était alors plus capable d'obtenir des coordonnées précises sur sa réelle position.
- ✓ En août 2020, au large des îles Galápagos, une importante flotte de pêche chinoise a été accusée de falsifier ses positions GPS dans le but de tromper les organismes de surveillance et de pêcher dans des zones interdites à la navigation. L'association Global Fishing Watch affirme que les navires de pêche transmettaient de faux signaux GPS les positionnant entre les îles Chatham et la Nouvelle-Zélande, à 10000 km des îles Galápagos. Il s'avère qu'en réalité il n'y avait aucun navire chinois proche de la Nouvelle-Zélande.
- ✓ En juillet 2021, lors d'exercices militaires de grandes ampleurs des forces de l'OTAN en mer Noire, plusieurs navires de guerre dont des Américains sont signalés au large de la Crimée alors qu'ils n'y participent pas. L'US Navy ira même jusqu'à publier des images d'un de ces navires amarrés dans le port d'Odessa (Ukraine) au moment des faits. La marine russe effectuait à la même époque des exercices aussi dans la mer Noire. Les mêmes mésaventures sont arrivées au destroyer britannique *HMS Defender* ou encore la frégate néerlandaise *HNLMS Evertsen* en juin 2021 toujours dans la mer Noire. Le 17 septembre 2021, le porte-aéronef *HMS Queen Elizabeth* de la Royal Navy est signalé en mer d'Irlande, accompagnée d'une armada de destroyers et escorteurs britanniques, belges et hollandais. En réalité, il n'y avait aucun navire navigant dans cette zone d'après des images satellites. Les systèmes de localisation maritime montrent régulièrement, et de plus en plus souvent, la présence de navires de guerre "fantômes"

20. https ://owdin.live/2019/11/26/des-vaisseaux-fantomes-des-agroglyphes-et-de-lor-doux-un-mystere-gps-a-shanghai/

à proximité d'endroits sensibles à fortes valeurs géopolitiques : les ports rivaux, détroits, zones contestées, etc.

III.4 Vers la cybersécurité du secteur maritime

III.4.1 Cybersécurité des systèmes navals

Bien qu'il n'existe pas de normes spécifiques aux ICS maritimes, les organismes du domaine maritime recommandent d'appliquer les normes qui existent déjà dans d'autres domaines industriels souvent sous la forme de guides de "bonnes pratiques". Par exemple, il existe plusieurs normes et guides rédigés par des agences gouvernementales, notamment IEEE 1613, International Society for Automation SP99, NIST SP8000, etc. Tous ces éléments tentent de bâtir une meilleure cybersécurité [88, 89]. Certaines approches s'appuient sur ces normes et tentent d'étudier les vulnérabilités des CPS. Ainsi, Shin *et al.* [119] ont développé un modèle d'analyse de la sécurité des ICS basée sur les automates. La première analyse porte sur la vérification du respect des guides réglementaires et les normes par les développeurs et les opérateurs du CPS. La seconde est une évaluation quantitative et qualitative des effets des vulnérabilités spécifiques aux systèmes et des mesures d'atténuation sur la cybersécurité. Chatterjee *et al.* [34] ont présenté une approche d'apprentissage itérative pour évaluer les propriétés dynamiques de vulnérabilité du système cyberphysique qui fait la distinction entre la vulnérabilité du sous-système et la sécurité globale du système. Les auteurs ont présenté quatre mesures de posture du système : stabilité, anti-fragilité, sécurité et dispersion qui fournissent collectivement une caractérisation holistique de la sécurité globale du système. Zang *et al.* [140] proposent de révéler les mécanismes de propagation des défauts en modélisant la défaillance en cascade du CPS électrique. Sur la base de ce modèle, deux graphiques sont construits pour analyser la vulnérabilité du CPS. Ces graphiques sont utilisés pour construire les indices de vulnérabilité du CPS électrique. De nombreuses approches sont créées et sont spécifiques aux logiciels, firmwares, et matériels utilisés par les composants ICS afin de protéger les ICS. Sur la couche matérielle, Ren *et al.* [112] ont proposé une approche pour sécuriser le port JTAG où l'exécution des instructions JTAG est surveillée par l'algorithme de Séparateur à Vaste Marge (SVM) pour identifier les séquences d'instructions anormales. Concernant la couche firmware, Basnight *et al.* [18] ont proposé une méthode d'analyse de firmware basée sur l'ingénierie inverse pour identifier la faiblesse du contrôleur et proposer des méthodes défensives contre les attaques de modification de firmware. De la même manière, Schuett *et al.* [117] ont utilisé une méthode d'ingénierie des recommandations de conception pour atténuer les potentielles vulnérabilités dans le développement futur des firmwares. La couche logicielle est également étudiée pour assurer la protection des ICS. Ainsi, McLaghlin *et al.*, [95] ont proposé une approche permettant de protéger la couche logicielle via le développement d'un vérificateur de sécurité pour l'analyse minutieuse du code de PLC considéré comme critique

pour la sécurité avant son exécution.

Comme nous l'avons suggéré ci-dessus, l'IoT peut être utilisé à de nombreux endroits sur le système de "Transport Maritime". Des termes tels que "Shipboard Internet of Thing" (SIoT) ou "Internet of Ships" (IoS) ont été introduits par la communauté du domaine [98]. Ces termes désignent les systèmes actuels et nouveaux combinés aux technologies IoT, aux nouveaux types de capteurs et aux CPS qui peuvent permettre aux concepteurs de systèmes de construire un nombre quelconque de systèmes de contrôle intégrés à bord des navires, de la passerelle à la salle des machines.

Bien que les stratégies de cyberdéfense se concentrent souvent sur les cyberattaques externes, d'autres facteurs peuvent entraîner la défaillance d'un dispositif et rendre les informations indisponibles. Nous pouvons citer comme facteurs de défaillance des dispositifs, la congestion du système et la charge de trafic, les interférences radio avec les dispositifs sans fil, les problèmes d'itinérance avec les dispositifs mobiles IoT. La sécurité de l'information ne se limite pas à la défense du périmètre, mais nécessite également une excellente conception du réseau et du système.

La question de savoir si les menaces peuvent être considérées comme des problèmes de Radio-Fréquence (RF) et non comme des problématiques cyber fait part d'un questionnement ouvert et donne lieu à de nombreuses discussions entre experts. Le simple fait que l'exploitation offensive de la RF puisse conduire à des données corrompues circulant dans les systèmes d'information est suffisant pour la considérer comme un risque cybernétique parmi d'autres. Des travaux récents ont également montré l'intérêt de l'analyse RF pour la détection de l'usurpation d'identité des AIS [111]. Des solutions pour la détection et la correction du brouillage et de l'usurpation du GPS ont été développées [24], mais elles restent coûteuses et leur intégration à bord des navires sera un long processus. La détection des intrusions commence également à gagner le monde maritime. Il existe des conceptions d'architecture et des flux de travail adaptés pour contribuer à l'élaboration de l'état des connaissances du MCSA. Cependant, la plupart des propositions s'appuient souvent sur les NIDS traditionnels, qui peuvent être des outils efficaces pour détecter les attaques courantes et acquérir des connaissances sur les réseaux surveillés, mais restent insuffisants. Deux limites de ces capteurs peuvent être mentionnées. Tout d'abord, la plupart des acteurs du marché des NIDS utilisent des technologies de détection d'abus telles que des signatures, provenant de flux de renseignements sur les cybermenaces publics ou commerciaux. Même si elles sont fréquemment mises à jour, ces signatures ne sont pas en mesure de détecter l'exploitation de vulnérabilités de type "zero-day". Pour être plus efficace, cette couche unique de signatures devrait être enrichie de signatures décrivant l'activité normale du réseau, qui doivent être développées pour chaque instance de détection sur un réseau spécifique, ce qui reste une tâche difficile pour la plupart des compagnies maritimes qui n'ont pas d'experts en cybersécurité ou un budget limité pour le cyber. Il est également essentiel de noter que la plupart des réseaux OT et industriels maritimes manquent de documentation précise, d'architecture, d'inventaire des actifs et de description des flux du réseau.

Dans certains cas, il est possible pour le récepteur GNSS de détecter les tentatives de brouillage du signal et plusieurs produits notamment GPS incluent cette capacité. Le meilleur moyen d'atténuer les effets du brouillage est probablement d'utiliser des récepteurs GNSS qui emploient plusieurs constellations.

Plusieurs mécanismes visant à renforcer la sécurité du réseau AIS ouvert et public ont été proposés, mais il est peu probable qu'ils soient mis en œuvre dans l'avenir. La première norme AIS intégrant la sécurité est la norme OneNet de la National Marine Electronic Association (NMEA) qui est apparue dans les produits à partir de 2021. Cette norme ajoute des champs supplémenbtaires dédiés à la cybersécurité dans les données AIS. Les normes OneNet et NMEA ne décrivent toutefois que la communication entre les appareils à bord d'un navire. Les messages diffusés par voie aérienne sont décrits dans les recommandations de l'Union internationale des télécommunications, secteur des radiocommunications (UIT-R). Ainsi, la sécurité interdispositifs à l'intérieur d'un navire n'élimine pas les vecteurs d'attaque par voie aérienne.

III.4.2 Les Systèmes de détection d'intrusion

L'intrusion peut être définie comme tout type d'activités non autorisées qui causent des dommages à un système d'information. Ainsi, toute attaque issue d'une intrusion peut constituer une menace pour la confidentialité, l'intégrité ou la disponibilité, qui sont trois concepts fondamentaux de l'information. La problématique d'intrusion est une thématique d'intérêt basée sur ces trois concepts. Il est admis qu'une cyberattaque peut se définir comme toute activité non autorisée qui compromettent une, deux ou ces trois concepts. Anderson [10, 11] détaille plusieurs méthodes pour améliorer le contrôle et la surveillance des menaces à la sécurité informatique. Il introduit alors l'idée d'automatiser la détection d'intrusion dans un réseau afin de détecter les utilisateurs « clandestins ». Le concept d'un système de détection d'intrusion (IDS) est né et va prendre son plein essor quelques années plus tard. L'objectif de cet IDS était d'aider les administrateurs à examiner les journaux d'événements système, les journaux d'accès aux fichiers et les journaux d'accès des utilisateurs. Denning [37] propose en 1986 l'un des premiers modèles de détection d'intrusion en temps réel. Développé entre 1984 et 1986, ce modèle est basé sur un prototype appelé Intrusion Detection Expert System (IDES) prémisse des approches IDS d'aujourd'hui. L'IDES utilise un système expert basé sur des règles pour détecter les attaques connues et une détection statistique des anomalies sur les données des utilisateurs et du réseau. Ce système produit plusieurs types d'alertes, en utilisant un format spécifique afin d'être indépendant du système. Dans ce qui suit, nous définissons les trois concepts fondamentaux des informations.

La confidentialité

La confidentialité est définie par la norme ISO 27000 comme la « propriété selon laquelle les informations ne sont pas rendues disponibles ou divulguées à des personnes, entités ou processus non

autorisés » [39]. Le défi de la confidentialité consiste à permettre aux utilisateurs légitimes d'accéder à ces informations tout en empêchant les autres de le faire. Ainsi, un défaut de confidentialité entraîne une violation et une exfiltration des données à laquelle il est impossible de remédier si ce n'est en coupant les liens de communications, mais qui peut être gérée de manière à minimiser son impact sur les utilisateurs. La confidentialité est mise en œuvre à l'aide de différents mécanismes de sécurité tels que le chiffrement ou l'authentification. Le niveau de confidentialité des informations est corrélé à la force des mesures de sécurité associées. Une même information peut ainsi être protégée par plusieurs couches de protection, combinant des mécanismes d'authentification et de sécurité, de protection, combinant mécanismes d'authentification et cryptographie. Par exemple, pour les protocoles utilisés dans les systèmes de navigation, les fabricants doivent s'assurer que seules les parties autorisées sont les seules à pouvoir modifier les données fournies. Des mécanismes de contrôles d'accès et des procédures de chiffrement peuvent être appliqués pour améliorer la protection des données. En raison de la limitation de la bande passante dans de nombreux protocoles de réseaux maritimes, les mécanismes de chiffrement ne sont pas toujours, voire rarement, mise en œuvre. En tant que telle, la principale approche pour assurer la confidentialité de ces systèmes passe principalement par le contrôle d'accès.

L'intégrité

L'intégrité est définie par la norme ISO 27000 comme la « propriété d'exactitude et exhaustivité » [39]. L'intégrité garantit que les informations sont protégées contre les modifications par des parties non autorisées ou accidentellement par des parties autorisées. L'intégrité est généralement mise en œuvre à l'aide de mécanismes de chiffrement, de sommes de contrôle ou bien de mécanismes de hachage. Les données reçues sont hachées et comparées au hachage des données d'origine. Les informations peuvent être modifiées par des événements tels qu'une panne de serveur ou une impulsion électromagnétique. En somme, garantir l'intégrité implique de protéger les informations contre toute modification par des parties non autorisées. Semblables à la confidentialité, le contrôle d'accès et la validation sont des méthodes courantes que les fabricants utilisent pour garantir l'intégrité des données de communications. En outre, de nombreux navires contiennent plusieurs appareils qui génèrent un trafic de communication, comme mentionné dans le Chapitre II. Certains d'entre eux génèrent une grande quantité de trafic réseau qui dépasse la bande passante qu'un navire peut raisonnablement gérer. Cela peut entraîner des perturbations et des latences lorsque les services tentent de se disputer cette bande passante limitée.

La disponibilité

La disponibilité est définie par la norme ISO 27000 comme la « propriété d'être accessible et utilisable à la demande par une entité autorisée » [39]. L'indisponibilité des informations peut avoir de graves conséquences. Les attaques par déni de service (DoS attack) sont des attaques courantes contre la disponibilité. Par exemple, les attaquants peuvent faire tomber des serveurs et rendre les services indisponibles aux utilisateurs légitimes en inondant les machines ciblées avec des demandes

superflues. Un plan de reprise est alors nécessaire pour minimiser l'impact de ces catastrophes. Les réseaux maritimes doivent garantir l'accès aux données et aux services qui, sous certaines conditions, peuvent devenir critiques pour les opérations et la mission du navire. La majorité des protocoles de communication maritime prennent en charge des vitesses de transfert lentes. En tant que telle, la protection de la disponibilité dépend des spécifications et de la configuration du matériel pour permettre le transfert des données en respectant le débit maximal imposé par le protocole.

L'authenticité

L'authenticité est une exigence complémentaire (définie par la norme ISO 27001) à respecter afin de mettre en place la vérification d'identité. À cela on peut ajouter l'autorisation puisque de nombreux protocoles intègrent un mécanisme pour identifier les nœuds de communication, ainsi que leurs privilèges et droits d'accès, à l'intérieur du réseau. Il est primordial de vérifier que le récepteur qui a reçu un message soit sûr de l'identité de l'expéditeur. Cette nouvelle exigence devient de plus en plus importante dans de nombreux domaines comme dans le domaine médical ou judiciaire. Certains protocoles utilisés par les navires prennent en charge des mécanismes d'authentification facultatifs qui sont rarement mis en œuvres comme pour le GNSS. Il est quasiment acquis que ces protocoles seront exploités dans un proche avenir afin d'assurer la sécurité de positionnement du navire. La non-répudiation est vouée à devenir aussi plus pertinente pour les entreprises maritimes. La question "comment un port peut-il vérifier qu'un exploitant de navire a bien reçu les bonnes instructions alors que l'armateur prétend le contraire ?" en est une très bonne illustration.

De manière générale le processus de détection d'intrusion fait référence aussi bien à la surveillance du trafic que la détection par des outils informatiques des activités malveillantes ou non autorisées. Cette détection d'intrusion est essentielle pour obtenir davantage de protection contre les actions qui compromettent la disponibilité, l'intégrité ou la confidentialité des systèmes informatiques. Afin de maintenir la sécurité du système, chaque appareil (matériel) ou application logicielle permettant de réaliser une détection d'intrusion est alors considéré comme un IDS. Plus précisément, l'objectif d'un IDS est d'analyser différents types de trafic (signal, réseau informatique, trame NMEA, etc.) et d'identifier les utilisations malveillantes qui ne peuvent pas être détectées par des outils traditionnels comme un pare-feu ou un antivirus. La figure (III.4) illustre comment un IDS transforme les activités surveillées en alertes en utilisant ses connaissances (base de données, statistiques, intelligence artificielle, etc.). Ces alarmes sont alors signalées soit à un administrateur, soit collectées de manière centralisée à l'aide d'un système de gestion d'événements et des informations de sécurité (SIEM). Grâce aux informations remontées par l'IDS, un SIEM est capable d'analyser en temps réel des sorties de plusieurs sources pour corréler les différentes alertes et donner une supervision centralisée de la sécurité informatique de l'ensemble du système. Les IDS sont parfois confondues avec des outils de sécurité informatique comme le pare-feu ou encore le système de prévention d'intrusion (IPS) même si leurs fonctions sont en grande partie différentes. Si on considère le caractère opérationnel de certains processus navals, il n'est pas viable de penser qu'un IPS puisse

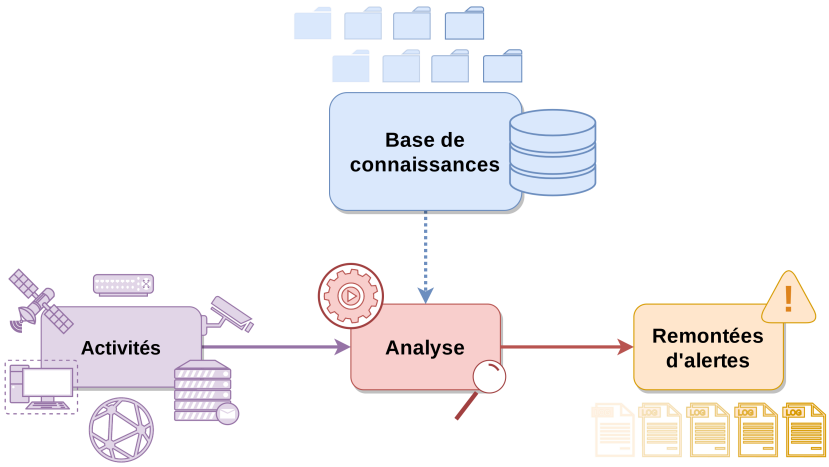


FIGURE III.4 – Illustration du fonctionnement d'un Système de Détection d'Intrusion (IDS).

venir arrêter le processus impacté par une attaque lorsqu'il s'agit par exemple de système de navigation ou de processus industriel critique pour le bon fonctionnement du navire. Ces systèmes ne sont donc que rarement utilisés dans ce cas de figure. Classiquement, il existe plusieurs types d'IDS que l'on peut catégoriser en trois grandes catégories (Fig. III.5) selon le type d'activité qu'ils sont voués à analyser : les IDS analysant le comportement utilisateur (*Host-based IDS* - HIDS), les IDS analysant le réseau (NIDS), et les IDS analysant les applications (*Application-based IDS*) [82, 65].

Un IDS basé sur l'hôte (HIDS) est un agent installé sur des hôtes individuels qui analyse leur activité : fichiers, processus, journaux système, etc. Les HIDS ont plusieurs ressources à leur disposition. Les instances du système peuvent être comparées pour vérifier l'absence d'activités non autorisées ou suspectes. Plusieurs tentatives de connexion échouées, une utilisation inhabituellement élevée du CPU, de mémoire vive, d'espace disque ou encore une longue période d'activité non autorisée sont autant d'indications d'une potentielle attaque. Certains HIDS peuvent également effectuer une détection basée sur le noyau en analysant les appels système et les modifications apportées aux binaires du système.

Un IDS basé sur le réseau (NIDS) utilise généralement des capteurs en divers points du réseau. L'analyse du trafic est effectuée soit par le capteur lui-même, soit à distance par un contrôleur central. Les solutions (HIDS et NIDS) peuvent être utilisées simultanément pour assurer un niveau de sécurité plus élevé. De façon générale, les IDS peuvent aussi être identifiées en fonction de leur méthode de détection respective pouvant être répartie en 3 grandes catégories : les détections basées sur les signatures, les détections basées sur les anomalies que l'on peut considérer comme basés sur le comportement et les détections hybrides, c'est-à-dire qui réalisent les deux en même temps. La détection basée sur les signatures s'accompagne d'une base de données de signatures d'attaques connues. Elle compare les données surveillées avec la base de données de signatures. Un IDS de

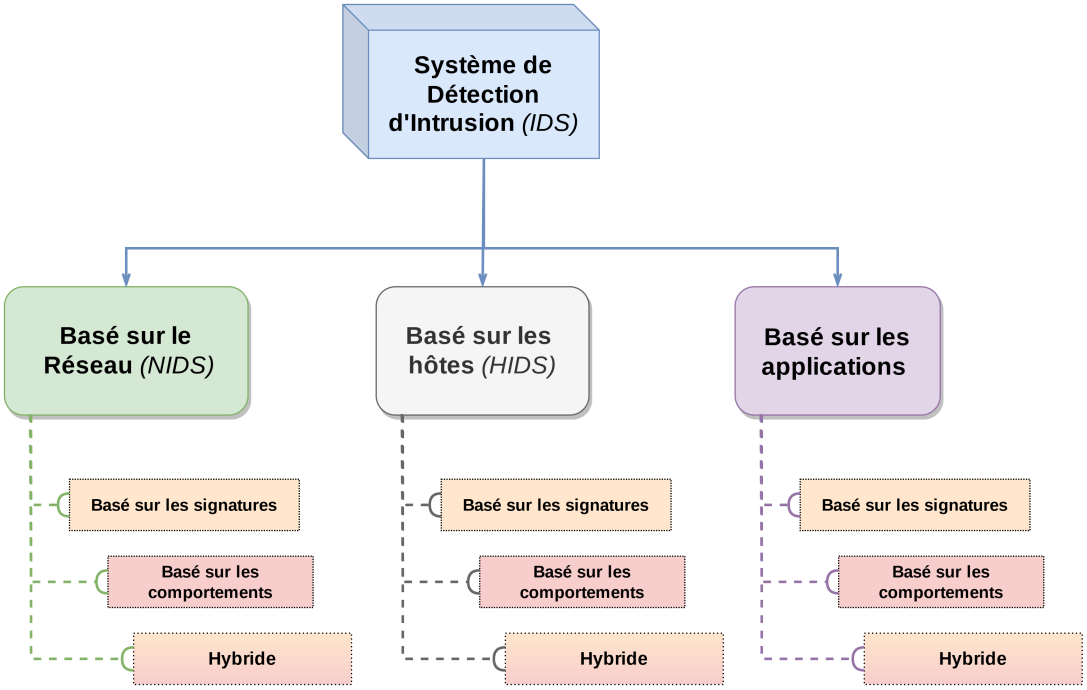


FIGURE III.5 – Classification des IDS en fonction de l'activité analysée et de la méthode de détection.

ce type vérifie le flux d'entrée pour détecter la présence d'un modèle d'attaque présent dans sa base. Pour être efficace, la base de données de ce type d'IDS doit être mise à jour régulièrement. Cependant, même avec les dernières mises à jour, seules les attaques connues peuvent être détectées par cette méthode [82].

La détection des anomalies de son côté tente d'apprendre un comportement "normal" ou "attendu" du système. Toute déviation de ce comportement est considérée comme une attaque potentielle et génère une alarme. Cette méthode ne nécessite pas de mises à jour ni même la présence d'une base de données. Il est également plus difficile de collecter des informations sur l'attaque puisqu'elle n'est pas clairement identifiée par une signature. Actuellement, la plupart des IDS basés sur les anomalies et l'étude du comportement du système reposent sur des algorithmes d'apprentissage automatique dont certains seront détaillés à la fin de ce Chapitre.

La détection hybride, quant à elle, combine les deux solutions pour atténuer les faiblesses de chaque catégorie : détection des anomalies puis détection des abus, détection des abus puis détection des anomalies, ou les deux à la fois. L'objectif est de détecter les attaques connues grâce à leurs signatures et d'utiliser la détection d'anomalies pour identifier les intrusions inconnues.

III.4.3 Méthodes de détection d'anomalie

III.4.3.1 La détection d'anomalie

Dans un état de l'art sur la détection d'anomalies, Chandola *et al.* [33] montrent que cette étape consiste à trouver des modèles dans les observations qui ne sont pas conformes au comportement attendu, qui ne suivent pas le même schéma ou qui sont atypiques lorsqu'on observe l'ensemble des données. Ces modèles caractérisés comme non conformes au regard du comportement attendu sont souvent appelés des anomalies, mais peuvent être définis comme des observations discordantes, des exceptions, des aberrations, du bruit, des nouveautés, des écarts ou encore des particularités ou bien des valeurs aberrantes. Une anomalie peut, par exemple, être d'abord anodine, mais dans un second temps devenir un incident lorsque l'analyse a déterminé qu'il ne s'agit pas d'un faux positif. Il existe ainsi de nombreux termes pour appréhender la détection d'anomalie dans des domaines d'applications tous aussi différents les uns que les autres (médecine, télédétection, acoustique sous-marine, bancaire, etc.) Reste que la difficulté du problème reste souvent la même et provient du fait qu'on ne connaît pas au préalable la loi de distribution derrière l'ensemble des données observées. Parmi tous ces termes, ceux d'anomalies ou de valeurs aberrantes (*Outliers*) sont les deux les plus couramment employés dans le contexte de la détection d'anomalies. Dans le cadre de nos travaux, il est important de préciser que les anomalies dans les données se traduisent par des informations exploitables et significatives et souvent déterminantes quant au bon fonctionnement des systèmes présents sur un navire.

Historiquement, la détection des valeurs aberrantes ou des anomalies dans les données est issue d'études en statistiques [42]. Au fil du temps, diverses techniques de détection des anomalies ont été développées. Ce concept est largement utilisé dans une grande variété d'applications telles que la détection de fraude dans le domaine bancaire, des assurances [57], la détection de pathologie ou la surveillance des données physiologiques d'un malade dans le domaine de la santé [40], la détection de défaut dans un capteur dans le domaine spatial [47], la détection de défauts dans les systèmes de sécurité critiques ou encore la détection d'intrusion en ce qui concerne la cybersécurité [49, 78]. Plus précisément, un modèle de trafic anormal dans un réseau informatique peut être symptomatique qu'un système piraté envoie des données à un autre système via un canal ou une destination non autorisé (le principe de la porte dérobée). Des anomalies dans le contexte de transactions bancaires peuvent, par exemple, indiquer un vol d'identité ou de carte de crédit [7]. Dans notre cas, la détection d'anomalies est associée à l'étude des données pouvant circuler sur un réseau (informatiques, industriels, communications). Plus précisément, dans le cadre de détection d'intrusion réseau, les "observations" intéressantes sont rarement des "observations rares", mais sont associées à des sursauts d'activités inattendues synonymes, très souvent, d'attaque. [1]

Il existe deux grandes catégories de techniques de détection d'anomalies (non supervisée,

supervisée, semi-supervisée) faisant partie du domaine de l'apprentissage automatique (Machine Learning). Cet apprentissage, appelé également apprentissage statistique, fait partie du domaine de l'IA dont l'objectif est d'extraire et d'exploiter automatiquement l'information présente dans le jeu de données. Cette technique peut être appliquée à différents types d'observations à savoir les images, les signaux, les graphes, les courbes ou plus simplement les vecteurs de caractéristiques, qui peuvent représenter des variables qualitatives, quantitatives, continues ou discrètes. Cette méthode utilise principalement des algorithmes qui permettent à un système informatique d'apprendre de manière itérative à partir de données d'observations. Par ailleurs, ce système informatique est capable d'améliorer ses performances au cours du temps, en s'enrichissant de nouvelles observations. L'apprentissage automatique comporte deux étapes. La première étape consiste à estimer le modèle du système à partir des données d'entrée. Plus précisément, l'estimation du modèle consiste à résoudre une tâche d'intérêt et est particulièrement utilisée en ce qui concerne la reconnaissance d'objets. Cette étape est dite d'apprentissage ou d'entraînement. La deuxième étape consiste à tester le modèle estimé sur un nouveau jeu de données. L'apprentissage peut être supervisé ou non supervisé [87]. Dans le cas supervisé, les données sont étiquetées (la réponse à la tâche est connue) et les algorithmes apprennent à prédire le résultat des données d'entrée. Si les étiquettes (ou labels) sont discrets, on parle de classification sinon on parle de régression [74]. Pour l'apprentissage non supervisé, les données ne sont pas étiquetées et les algorithmes apprennent par eux-mêmes la structure inhérente à partir des données en entrée [20]. Une autre classe d'apprentissage automatique est l'apprentissage par renforcement (Reinforcement Learning) dont le but est de diriger l'apprentissage non supervisé à l'aide de récompenses ou de pénalités. Plus exactement, cette méthode apprend à partir d'expériences successives de façon à trouver la meilleure solution. Elle consiste à récompenser les comportements souhaités et/ou à sanctionner les comportements non désirés. L'algorithme interagit avec son environnement d'analyse pour trouver la solution optimale [67].

En général, pour chaque apprentissage, il existe des algorithmes spécifiques qui dépendent du type de problème à résoudre ainsi que du type de données en entrée et en sortie. Pour le problème de détection d'intrusion en cyber, une taxinomie acceptée dans ce domaine est donnée par la figure (III.6). À cette liste d'algorithmes, on peut ajouter aussi les approches relevant de l'apprentissage profond (Deep Learning).

Les techniques supervisées

Les techniques de détection d'anomalies supervisées [20] nécessitent un jeu de données étiquetées comme "normal" ou "anormale" et la construction d'un classifieur. En apprentissage supervisé le but est de trouver une fonction ou un modèle qui, à partir d'échantillons en entrée, permet de prédire le plus précisément possible le label, la nature, la classe de cet échantillon. La phase d'apprentissage est cruciale, car les données doivent être suffisamment nombreuses et représentatives pour que le modèle soit le plus exhaustif et précis possible, et l'apprentissage lui-même doit être suffisamment régulier pour prendre en compte les éventuelles fluctuations du trafic dans le temps.

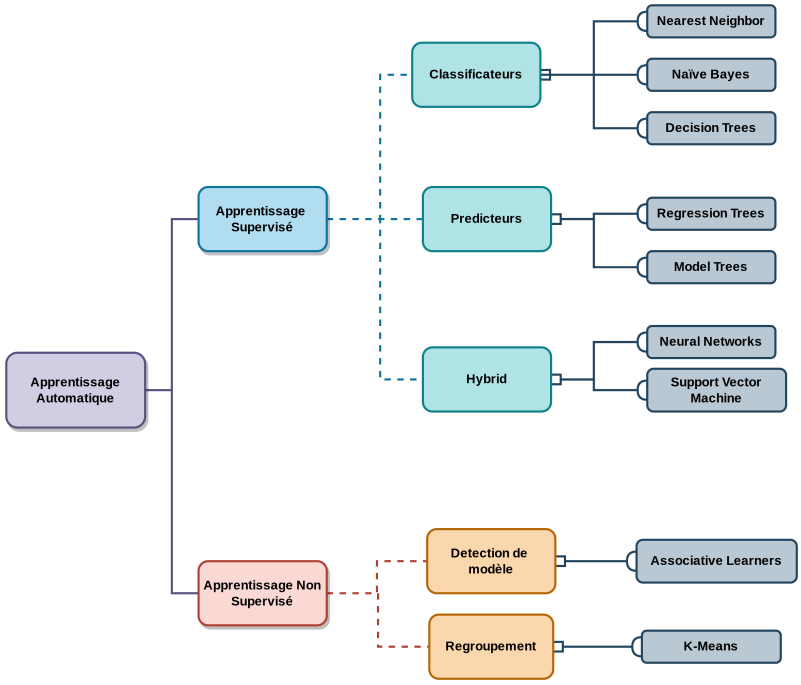


FIGURE III.6 – Taxonomie des algorithmes d'apprentissage pour la détection d'intrusion [15] - *"Handbook of Big Data Privacy"*

Les algorithmes supervisés tels que les arbres de décision, les k-plus proches voisins, SVM [108], les perceptrons ou la "classification naïve Bayesienne" sont rarement utilisés pour la détection d'intrusion, car, en pratique, il est compliqué et coûteux de produire des labels sur un jeu de données. Comme nous n'avons aucune connaissance en théorie sur les types d'attaques, il est difficile de faire un apprentissage exhaustif. Cependant, ces algorithmes ont inspiré un certain nombre d'algorithmes semi-supervisés (utilisant un ensemble à la fois de données étiquetées et non-étiquetées) qui sont maintenant mieux adaptés à la détection de valeurs aberrantes.

L'algorithme SVM est l'une des techniques d'apprentissage automatique les plus efficaces, utilisées dans de nombreux problèmes tels que la classification d'images, la classification par sac de mots ou la détection de valeurs aberrantes. Contrairement à la régression logistique et à d'autres modèles de réseaux neuronaux, les SVM tentent de maximiser la séparation entre deux classes de points. En particulier, cette méthode est largement utilisée dans la détection des anomalies [32] et plusieurs études ont été menées sur le trafic réseau [77, 132] pour détecter des cyberattaques.

Les techniques non supervisées

Les techniques non supervisées [20] visent à détecter les anomalies dans un jeu de données test non étiquetées en supposant que la majorité des instances de l'ensemble de données sont normales. Le principe est de rechercher les instances qui semblent correspondre le moins au reste de l'ensemble de données. D'ailleurs, le modèle de la détection d'intrusion réseau ne respecte pas la définition

statistique commune d'une valeur aberrante en tant qu'observations rares. Ainsi, de nombreuses méthodes de détection non supervisées ne seront pas efficaces sur de telles données, à moins qu'elles n'aient été regroupées de manière appropriée. Au lieu de cela, un algorithme d'analyse de « cluster » ou de clustering peut être capable de détecter ceux formés par ces modèles d'observations.

Le but de l'apprentissage non supervisé est d'extraire des classes au sein des échantillons en les regroupant par une mesure de similarité la plupart du temps sans aucune connaissance préalable, mais en supposant le nombre de classes connu. L'idée est de trouver des modèles cachés à partir de données non étiquetées.

Cette méthode est très souvent utilisée pour la classification du trafic de masse d'Internet et la détection d'anomalies, car il est souvent compliqué d'assurer que le jeu de données d'apprentissage pour un algorithme supervisé est garanti "100% sans anomalie". Le trafic Internet varie beaucoup en volume, avec des fluctuations selon le jour/l'heure. L'évolution des topologies réseaux, l'apparition de nouveaux protocoles, la mutation des anomalies, etc. font qu'un apprentissage sans aucun *a priori* est plus adapté. Alors que de son côté le non supervisé est souvent associé aux techniques de regroupement dit de "clustering" qui sont très fréquemment utilisées.

Les techniques de détection d'anomalies semi-supervisées construisent un modèle représentant le comportement normal d'un ensemble de données d'entraînement, puis détermine la probabilité qu'une instance de test soit générée par le modèle utilisé.

À noter que dans un problème de classification relativement classique, afin que l'apprentissage puisse se dérouler correctement, un prétraitement est appliqué sur les données afin de supprimer les données aberrantes au regard de l'ensemble des données. Il s'agit de nettoyer l'ensemble des données en supprimant celles qui sont incomplètes et inintelligibles pour faciliter au maximum l'apprentissage. Ainsi dans le cadre de l'apprentissage supervisé, la suppression des données anormales de l'ensemble de données entraîne souvent une augmentation statistiquement significative de la précision. Ici, il ne s'agit pas de mettre en place de telles pratiques, car il s'agit justement de détecter des données anormales.

Dans le cas particulier où nous réussissons à n'utiliser que des échantillons d'une seule classe, dans notre cas de label "normal", on peut parler de classification de classe unique (ou one-class). Il y a beaucoup de méthodes statistiques pour la détection de valeurs aberrantes en délimitant l'unique classe par des seuils en considérant tout ce qui y est extérieur comme des outliers. Dans ce qui suit, nous présentons les méthodes de détection à une classe les plus utilisées dans la littérature. Nous testerons ces méthodes et analysons leurs performances au Chapitre 6, sur le jeu de données que nous avons nous-mêmes généré (Chapitre 5).

III.4.3.2 Descriptions de méthodes de type "One class"

De nombreuses applications nécessitent de pouvoir décider si une nouvelle observation appartient à la même distribution que les observations existantes, ou doit être considérée comme différente (ou aberrante). Souvent, cette capacité est utilisée pour nettoyer des ensembles de données réels. Deux distinctions importantes doivent être faites : dans le cas de la détection de valeurs aberrantes, les données d'apprentissage contiennent des valeurs aberrantes qui sont définies comme des observations éloignées les unes des autres. Les algorithmes de détection de valeurs aberrantes tentent donc d'ajuster les régions où les données d'apprentissage sont les plus concentrées, en ignorant les observations déviantes. Concernant la détection de nouveauté, les données d'apprentissage ne sont pas polluées par des valeurs aberrantes et les algorithmes s'intéressent à détecter si une nouvelle observation est une valeur aberrante. Dans ce contexte, une valeur aberrante peut être également appelée une nouveauté.

La détection de valeurs aberrantes et la détection de nouveauté sont toutes deux utilisées pour la détection d'anomalies, où l'on s'intéresse à la détection d'observations anormales ou inhabituelles. La détection des valeurs aberrantes est alors également connue sous le nom de détection d'anomalies non supervisée et la détection de nouveauté sous le nom de détection d'anomalies semi-supervisée. On peut aussi appeler l'apprentissage ou la classification à classe unique ou encore classification à une classe. Il s'agit d'algorithmes d'apprentissage non supervisés qui tentent de modéliser des exemples jugés comme "normaux" afin de classer les nouveaux exemples normaux ou anormaux que l'on peut qualifier de valeurs aberrantes ou non suivant les données que l'on connaît déjà jugée comme étant normales. [21]

Les techniques de classification à une classe peuvent être dédiées pour les tâches de classification binaire avec une distribution de classe fortement asymétrique. Ces techniques peuvent être adaptées aux exemples d'entrée de la classe majoritaire dans l'ensemble de données de formation, puis évaluées sur un ensemble de données de test d'exclusion. Ces méthodes de classification à une classe peuvent être utilisées dans les données déséquilibrées avec très peu d'exemples de la classe minoritaire. On peut citer comme méthodes de classification à classe unique : le SVM, "Local Outlier Factor", "Isolation Forest" ou la méthode de "Covariance robuste".

One-Class Support Vector Machine

L'algorithme One-Class Support Vector Machine (OC-SVM), est une extension naturelle du SVM [118]. C'est un algorithme qui vise à déterminer le contour d'une classe et qui permet de détecter les points qui ne sont pas de la classe concernée. Afin d'identifier les observations suspectes, l'algorithme estime une distribution qui englobe la plupart des observations, puis étiquette comme suspectes celles qui s'en éloignent, et ce en utilisant une métrique appropriée. Une solution OC-SVM est construite en estimant une fonction de distribution de probabilité qui rend la plupart des données observées

21. https ://scikit-learn.org/stable/modules/outlier$_d$*etection.html*

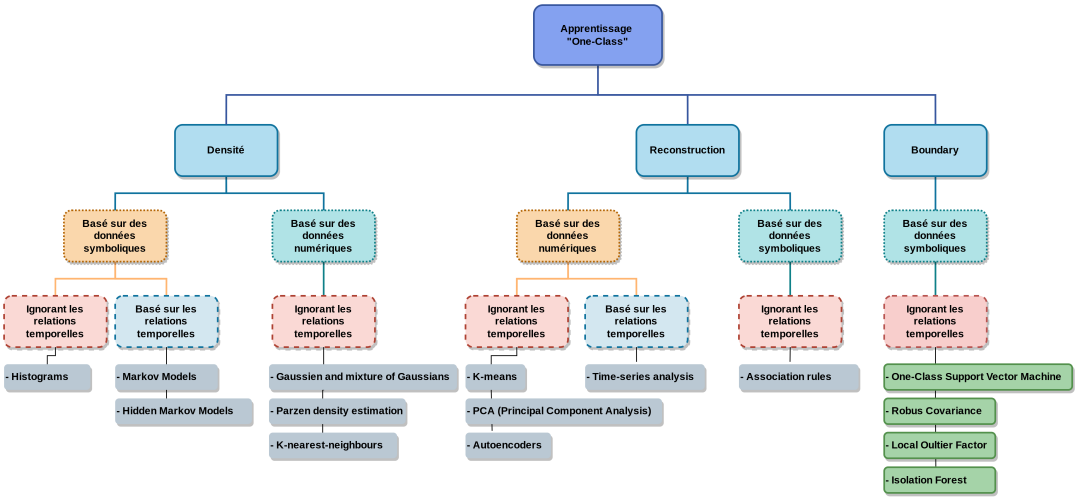


FIGURE III.7 – Taxonomie des algorithmes d'apprentissage dits "One Class" - [15] - *"Handbook of Big Data Privacy"*

plus probables que le reste et une règle de décision (qui peut être appelée limite de décision) qui sépare ces observations par la plus grande marge possible. Une transformation non linéaire utilisant un noyau permet même de considérer les SVM comme une technique de réduction de la dimension de l'espace des données. Les SVM à une classe supposent qu'une seule classe est connue et l'objectif est de détecter ce qui en dehors de cette classe. Contrairement aux SVM classiques, les OC-SVM apprennent une frontière de décision qui réalise une séparation maximale entre les échantillons de la classe connue et l'origine. Cet algorithme est très souvent utilisé aujourd'hui et à fait ses preuves dans de nombreux domaines et notamment pour améliorer les systèmes de détections d'intrusions réseau [5, 6].

Local Outlier Factor

L'algorithme Local Outlier Factor (LOF) est une méthode non supervisée de détection des anomalies basée sur le calcul de l'écart de densité locale d'un point observé par rapport à ses voisins [25]. Plus précisément, s'il existe une divergence entre le point observé et ses voisins, le point est considéré comme une anomalie. La densité locale d'une observation est évaluée en considérant les k plus proches observations ou voisins du point observé. En comparant la densité locale d'un point aux densités locales de ses voisins, il est possible d'identifier des régions de densité similaire et des points dont la densité est nettement inférieure à celle de leurs voisins. L'algorithme LOF génère une fonction "score" qui permet de quantifier le degré d'anomalie supposé des observations et via un seuil choisi permettant de qualifier les résultats de "normaux" et/ou "d'anormaux". Cette méthode est également employée pour améliorer les performances des NIDS [8].

Isolation Forest

L'algorithme Isolation Forest (IF) est une technique utilisée pour la classification binaire non supervisée et la détection des anomalies [84]. L'isolation se fait sans faire appel à une mesure de similarité entre les données et signifie séparer un point du reste des points. Formellement, la méthode IF est construite autour de la théorie des arbres de décision et des forêts aléatoires. Cette méthode calcule un score d'anomalie pour chaque observation du jeu de données. Le principe est de calculer un score qui donne une mesure de la normalité de chaque observation en fonction de l'ensemble des données puis de comparer ce score dans un second temps pour isoler les anomalies. On part de l'idée qu'une donnée anormale ou atypique sera plus facile à isoler qu'une donnée standard ou normale due à son écart, par exemple en distance, à ces dernières. Ainsi, les branches des arbres d'isolement contenant les points atypiques sont sensiblement moins profondes, par conséquent la distance de la feuille à la racine est utilisée comme l'inverse du score d'anomalie. On peut également retrouver cette méthode dans le cadre d'analyses de trafic réseau [130].

Robust Covariance

L'algorithme Robust Covariance (RC) peut être utilisé si les variables d'entrée ont une distribution gaussienne, car des outils statistiques simples peuvent être utilisés pour détecter les valeurs aberrantes [28]. Par exemple, si l'ensemble de données comporte deux variables d'entrée suivant une loi de Gauss, alors l'espace des caractéristiques forme une gaussienne multidimensionnelle et la connaissance d'une telle distribution peut faciliter l'identification des valeurs éloignées de la distribution. Cette méthode peut être généralisée en définissant une hypersphère (ellipsoïde) qui couvre les données normales et les données qui sortent de cette forme sont considérées comme des valeurs aberrantes. Une mise en œuvre efficace de cette technique pour les données multivariées est connue sous le nom de covariance robuste. Comme pour les autres algorithmes de détection de nouveauté, nous avons testé celui-ci sur des données de navigation comportant des falsifications dues à l'usurpation de leurre.

III.4.3.3 Métriques d'évaluation

Pour évaluer les algorithmes de détection, des métriques sont utilisées pour déterminer leurs performances en termes de résultat de détection ou de classification. On peut également utiliser la matrice de confusion pour avoir une image ou une carte plus complète lors de l'évaluation des performances du modèle (Fig. III.8).

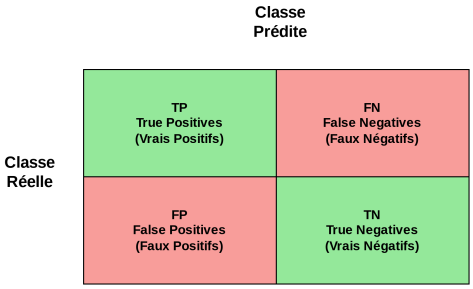


FIGURE III.8 – Principe théorique de la matrice de confusion pour les métriques d'évaluation.

Des éléments de la matrice de confusion (Fig. III.8) comme les taux de faux négatifs ou de vrais positifs sont exploités pour calculer par exemple les métriques d'évaluation comme "Recall" ou "F1 Score". Les métriques utilisées en pratique sont reportées dans la table (III.1).

TABLE III.1 – Tableau des différentes métriques d'évaluation

Métrique	**Formule**	**Signification**
Accuracy	$\frac{TP+FP}{TP+FP+TN+FN}$	Performance globale du modèle
Precision	$\frac{TP}{TP+FP}$	Précision des prédictions positives
Recall	$\frac{TP}{TP+FN}$	Couverture de l'échantillon positif réel
Specifity	$\frac{TN}{TN+FP}$	Couverture de l'échantillon négatif réel
F1 Score	$\frac{2TP}{2TP+FP+FN}$	Métrique hybride utile lorsque les classes sont déséquilibrées

III.5 Conclusion

Dans ce chapitre nous avons détaillé quelques exemples d'incidents de cybersécurité dans différents secteurs comparables au secteur monde maritime, notamment par ses composantes industrielles touchées, car très vulnérables. Après avoir présenté des exemples de cyberattaques spécifiques au monde maritime dû à des vulnérabilités, nous avons évoqué en quoi la prise de conscience de ces vulnérabilités permet d'instaurer progressivement des politiques de cybersécurité dans le domaine maritime. Quelques solutions bien connues et issues de récents travaux de recherche, comme les méthodes de détection d'anomalies, sont largement exploitées au service de la cybersécurité, tous secteurs confondus. Il est d'ailleurs présenté que ces méthodes ont diverses origines et notamment des méthodes d'apprentissage automatique, très utilisées pour améliorer les performances des systèmes de détection d'intrusion dans les systèmes critiques actuels. C'est d'ailleurs le cas de certains entreprises comme la société Darktrace [22]. Quelques-unes de ces méthodes seront exploitées et évaluées dans la suite de ce manuscrit. Ce chapitre permet de répondre à une deuxième partie de la question de recherche **QR1** et répondre à la **QR3**.

Le chapitre IV suivant abordera dans un premier temps une description de la plate-forme de simulation permettant l'exploitation d'une méthodologie de génération de données issues du monde maritime.

22. darktrace.com - arktrace est une société de technologie de l'information anglo-américaine spécialisée dans la cyberdéfense. La société a été créée en 2013 et est basée à Cambridge, en Angleterre, et à San Francisco, en Californie, aux États-Unis.

Chapitre IV

Description d'une Plate-forme Simulant l'Environnement Numérique d'un Navire

Sommaire

IV.1 Introduction

Ce chapitre décrit l'ensemble des méthodologies mises en place pour mener à bien les différentes expérimentations permettant la génération de données homogènes (issues de réseaux informatiques, ICS, systèmes de navigations, etc.). Pour ce faire, nous avons activement participé à la conception

d'une plate-forme de simulation pour reproduire les caractéristiques fonctionnelles et opérationnelles d'un navire. Cette plate-forme a vocation à générer et à collecter des jeux de données assez réalistes et maîtrisées, pour le traitement, l'analyse ou l'identification à des fins d'analyse de risque, de prévention, de résilience, de détection d'anomalies ou de maintien en condition opérationnelle (MCO). Rappelons que les données d'un navire en fonctionnement ne sont pas accessibles et ce essentiellement à cause des processus de protection et de propriétés industrielles. De plus, très peu de laboratoires académiques s'orientent vers la génération de jeux de données navire. À notre connaissance, une plate-forme orientée navire intégralement dédiée à la recherche académique n'existe pas en pratique (même si des plates-formes dédiées aux problématiques industrielles ont vu le jour [121]). Indéniablement, le développement de cette plate-forme rentre totalement dans cette dynamique de visualisation des systèmes physiques [1] dont l'objectif est de combler un manque de données dans le domaine.

Ici il est question de finir de répondre à la **QR1** et à la **QR2** comme indiqué dans le Tableau (IV.1).

Correspondance : Question de Recherche / Chapitre					
	Chap. II	Chap. III	**Chap. IV**	Chap. V	Chap. VI
QR I					
QR II					
QD I					
QR III					

FIGURE IV.1 – Tableau de correspondances entre les Questions de Recherche et les Chapitres.

Pour comprendre les imbrications entre les différents systèmes de cette plate-forme, la maîtrise des différents protocoles de communications pouvant coexister au sein d'un navire est nécessaire afin d'identifier les attributs potentiellement pertinents pour mener à bien les analyses cyber. Dans le cadre de cette thèse, différents attributs discriminants sont proposés, dont l'analyse des variations permet la détection d'anomalies ou les cyberattaques. Nous pouvons citer à titre d'exemple les variations des données du protocole S7COMM pour les ICS ou les trames NMEA pour le système de navigation. Des scénarios mettant en évidence l'exploitation de vulnérabilités par plusieurs types de cyberattaques (couvertes par le framework MITE ATT&CK [2] sont décrits. La véracité des scénarios est inspirée d'événements et de cyberattaques déjà survenus dans le contexte maritime.

1. Le déploiement de plates-formes de simulation se développe énormément, parfois sous des formes totalement numériques et simulées, ou encore sous des formes hybrides à l'image de valises transportables proposées par des industriels. Voir par exemple le lien https ://www.diateam.net/what-is-a-cyber-range/.

2. https ://attack.mitre.org/ - The Adversarial Tactics, Techniques, and Common Knowledge ou "MITRE ATTCK" est un guide de classification et de description des cyberattaques et des intrusions.

Dans ce chapitre, l'ensemble de la plate-forme de simulation est décrit afin de conserver une cohérence tout au long du manuscrit. L'architecture de la plate-forme sera présentée dans un premier lieu par une description générale suivie par une description des différents systèmes informatiques, des ICS et des systèmes de navigation employés. Les spécificités et les vulnérabilités des protocoles utilisés seront également détaillées.

IV.2 Plate-forme de simulation navale : Naval Cyber-Range

Cette section décrit la plate-forme installée à l'École Navale dans les locaux de la Chaire de Cyberdéfense des systèmes navals, qui reproduit le fonctionnement cybernétique d'un navire. Les caractéristiques et fonctionnalités de la plate-forme sont présentées. L'objectif de cette plate-forme est la génération des jeux de données réalistes afin de concevoir des scénarios plausibles et représentatifs, et illustrer les performances des algorithmes de détection d'anomalies.

IV.2.1 Description générale de la plate-forme

La plate-forme a été déployée dans des locaux sécurisés spécialement aménagés au sein de l'École Navale à partir de 2018. Elle est également exploitée dans le cadre du projet européen H2020 *Foresight*[3] (2019-2023), dont l'École Navale est un des partenaires, qui vise à rassembler des plates-formes d'expérimentation dédiées à la formation du personnel confronté à des problématiques de cybersécurité industrielle. Ces plates-formes d'expérimentation apportent des solutions de simulation et de reproduction en environnements maîtrisés, pour couvrir des besoins d'analyse et d'étude en matière de cybersécurité de domaines à enjeux critiques. Dans notre cas, il s'agit de présenter l'architecture du Naval Cyber-Range destiné au contexte maritime.

Cette plate-forme est développée avec la coopération de professionnels provenant du monde industriel (Thales, Naval Group), opérationnel (Marine Nationale) et de la recherche académique (École Navale, IMT-Atlantique, ENSTA-Bretagne). Il faut préciser que cet outil est destiné aussi bien à la formation qu'à la recherche scientifique en cybersécurité maritime. Cette plate-forme de simulation est bien une représentation numérique et fictive d'un vrai navire. Cela étant, elle n'est pas une représentation fidèle à 100% d'un vrai navire. D'une part parce que le budget alloué au projet est loin d'être équivalent à celui nécessaire pour construire un navire ; et d'autre part, par le fait qu'elle occupe une surface relativement petite d'environ $20m^2$, bien loin des dimensions classiques d'un navire transporteur de fret ou militaire.

N'étant qu'une représentation numérique d'un navire, cette plate-forme génère des biais qui peuvent impacter la pertinence des données générées, la véracité des scénarios imaginés et donc la

3. https ://cordis.europa.eu/project/id/833673/fr

crédibilité des analyses proposées. Le premier biais est lié à la manière dont les données sont générées. Celles-ci proviennent de plusieurs logiciels de simulation et de divers sous-systèmes (simulés ou non) interconnectés les uns aux autres afin de reproduire le comportement (simulation) d'un navire. Cette forte interconnexion peut naturellement produire des biais méthodologiques (notamment des effets de bord et souvent involontaires) pouvant être difficiles à identifier (que ce soit dans le trafic réseau des systèmes informatiques, des automates industriels ou des systèmes de navigation).

Le deuxième biais provient du fait que les différents systèmes (simulés ou réels) sont des versions souvent simplifiées de ce que l'on peut trouver sur un véritable navire. Mais le principe reste cependant que le fonctionnement de ces systèmes soit le plus représentatif et le plus réaliste possible. Par souci de simplification, les automates industriels sont programmés de la même façon que s'ils étaient en condition réelle, sans prendre en compte néanmoins des contraintes opérationnelles (comme par exemple les états d'alerte particuliers dans lesquels peut se retrouver le navire comparé à une situation plus "normale"). Il en est de même pour les IHM en passerelle et celles présentes dans les armoires industrielles des ICS. Cela signifie que le fonctionnement des systèmes installés dans la plate-forme ne correspond pas exactement au fonctionnement des vrais systèmes dans des conditions réelles et opérationnelles. Cependant, cela reste vrai pour tout type de simulation [4].

Enfin, toujours dans un souci de simplification, le parc informatique (réel ou simulé) de l'architecture a été configuré de la même manière que celui d'un réseau informatique normal en mettant en œuvre des règles de filtrage et de routage relativement classiques. Cette simplification des systèmes est nécessaire d'une part par l'objectif initial du Naval Cyber-Range et d'autre part par le coût.

Cependant, il réside également des biais qu'il n'a pas été possible de réduire car ils sont produits par l'utilisation de matériels différents de ceux d'un vrai navire. Par exemple, les capteurs de pression ou de température ne sont pas identiques à ceux utilisés dans un navire où les valeurs de sortie peuvent ne pas avoir les mêmes plages de fonctionnement et leurs précisions sont moindres. Le principe est de limiter au maximum ces biais pour contenir leurs impacts sur les différentes conclusions proposées. Pour cela, les sections suivantes permettent de dresser l'étendue de l'architecture et les limites des systèmes constituant cette plate-forme. Il s'agit de montrer en quoi cette plate-forme de simulation peut être véritablement pertinente dans des problématiques cybernétiques navales.

Tout au long de cette partie, la description de la plate-forme tournera autour de la modélisation et la simulation de fonctionnement d'un navire générique civil. Le Naval Cyber-Range est constitué de sous-systèmes réels ou simulés qui assurent différentes fonctionnalités d'un navire civil classique afin de mettre à disposition un outil d'expérimentation le plus réaliste possible. Dans les travaux de thèse d'Olivier Jacq [61], une première modélisation de l'architecture technique de ce prototype de navire générique a été proposée. Tout comme un navire réel, l'architecture du Naval Cyber-Range

4. "La simulation est la représentation du comportement d'un processus physique, industriel, biologique, économique ou militaire au moyen d'un modèle matériel dont les paramètres et les variables sont les images de ceux du processus étudié." - Dictionnaire Larousse

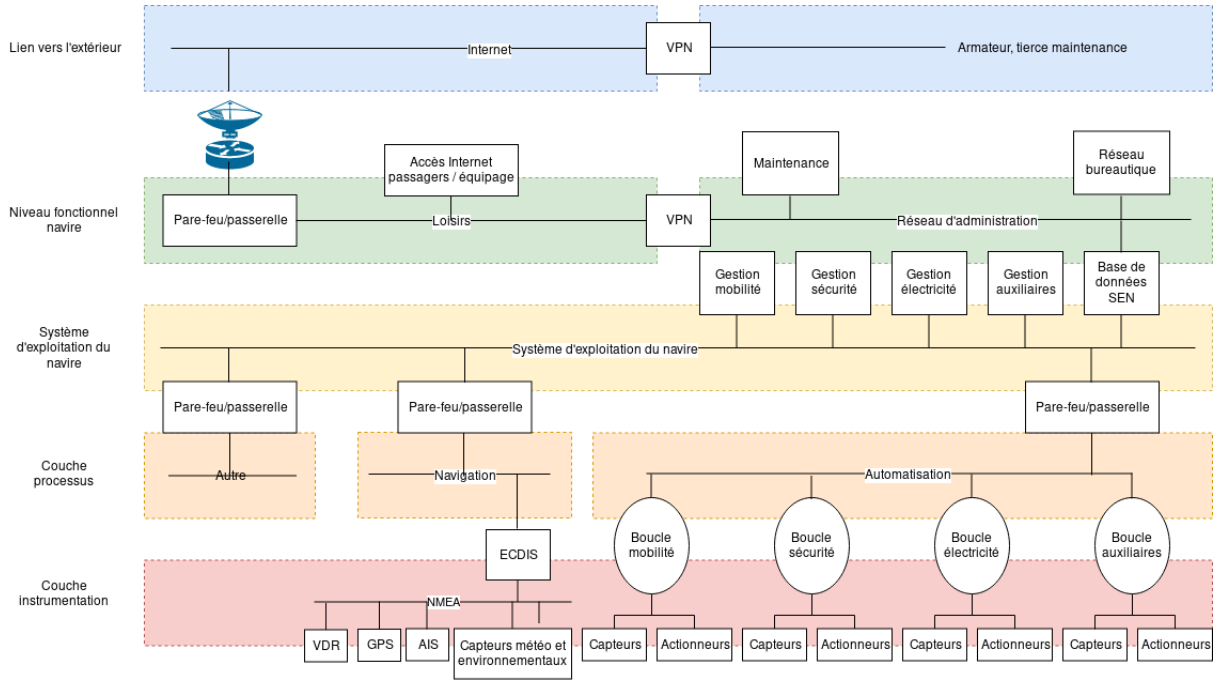


FIGURE IV.2 – Modélisation technique d'un navire générique civil. Architecture apparue dans [62]

est composée de différents systèmes IT et OT nécessaires à son bon fonctionnement (Fig. IV.2). Dans le cadre de cette thèse, l'ensemble de l'architecture repose sur ce même modèle, mais seuls les systèmes OT seront étudiés par la suite et catégorisés en trois grands blocs considérés : la couche fonctionnelle, une couche de processus, et enfin la couche d'instrumentation. Les différents blocs représentent les parties importantes du navire et permettent d'assurer le bon fonctionnement des systèmes à bord de celui-ci. Même si tous les systèmes ne sont pas représentés, cette architecture est amplement suffisante pour décrire la plupart des couches classiques à bord d'un navire (Fig. IV.2). Chacune des couches de la plate-forme a une fonction bien précise :

1. **La couche hors du navire :** elle représente les systèmes qui ne font pas partie du navire (liens vers l'extérieur). Dans notre cas, il s'agit, par exemple, du réseau des systèmes de maintenance à distance de l'armateur ou encore du fournisseur Internet ;
2. **La couche fonctionnelle du navire :** elle représente la partie la plus conséquente en termes d'architecture réseau. Elle comprend, par exemple, les différents systèmes de gestion (maintenance interne au navire, mobilité, sécurité, bureautique, etc.), les accès Internet, etc. ;
3. **La couche système d'exploitation du navire :** elle permet de faire le lien entre la partie réseau (couche fonctionnelle) et la partie plus matérielle (couche des processus) des automates notamment avec la présence des IHM permettant de gérer à distance les différents ICS (SCADA, PLC) voire même des cartes électroniques (Arduino, Raspberry Pi) ;
4. **La couche processus du navire :** cette couche est divisée en plusieurs parties avec d'un côté la gestion de la navigation au niveau de la passerelle (via l'ECDIS) et de l'autre la partie

automatisation représentée par quatre boucles : Mobilité, Sécurité, Énergie et l'Auxiliaire ;

5. **La couche instrumentation du navire :** cette couche basse est associée à l'ensemble des capteurs ou actionneurs comme le système GNSS, le transpondeur AIS, le VDR, les capteurs météorologiques, les vannes, les sondes de température, etc. Dans le Naval Cyber-Range, ces éléments peuvent être à la fois simulés ou alors mis en œuvre à partir de véritables capteurs.

IV.2.2 Les systèmes informatiques

En plus des systèmes OT permettant de représenter de véritables boucles industrielles et les systèmes de navigation, la plate-forme est constituée d'un certain nombre de composants informatiques traditionnels (ordinateurs, équipements réseaux, etc.) fortement interconnectés. Pour cela, un serveur de virtualisation des flux réseaux est mis en œuvre afin de simuler les différents postes informatiques qu'il peut y avoir à bord d'un véritable navire comme les réseaux dédiés aux passagers ou les réseaux utilisés en passerelle ou encore les réseaux des ICS. Par souci de réalisme, aucune protection supplémentaire autre que celle proposée nativement n'est appliquée sur ces systèmes. Les réseaux informatiques ne sont pas isolés et il est facile de passer d'un réseau à l'autre par une simple « attaque par rebond » (*Smurf Attack*) [5]. Pour chaque ordinateur virtualisé, un comportement utilisateur est simulé reproduisant une activité humaine en fonction du contexte, du rôle et du réseau dans lequel il se trouve. Concernant les biais, il est important de préciser que les systèmes virtualisés sont générés à l'identique avec une configuration similaire à ceux d'un navire. Les comportements normaux des utilisateurs sont simulés via des trafics Internet basiques ou par l'utilisation d'outils bureautiques classiques afin de pouvoir reproduire les mêmes actions. Dans ce qui suit, à défaut d'une description complète de l'architecture, nous nous limitons à quelques profils spécifiques d'utilisateurs autour et à bord du navire :

1. **Profil de l'armateur et de la maintenance à distance :** ces profils ne font pas partie directement du navire, mais assurent la maintenance à distance depuis un centre de contrôle en cas de panne complexe ou ceux permettant d'établir le lien direct entre le navire et l'armateur ;
2. **Profil générateur de trafic Internet :** il permet de simuler le fait que les passagers ont un accès à Internet. Si des requêtes sur un site Internet sont faites depuis n'importe quel ordinateur de la plate-forme, le simulateur de trafic va lui répondre. Cela permet de simuler entièrement le comportement normal du trafic Internet à bord ;
3. **Profil des passagers :** ce sont les PC classiques de l'équipage et des passagers à bord qui sont souvent utilisés pour accéder à Internet, pour réaliser des tâches simples (bureautique),

5. Une attaque par rebond (Smurf Attack) consiste à envoyer de nombreuses requêtes à un réseau, comme dans le cas des attaques "ping flood" afin de submerger un système. Toutefois, l'attaque est amplifiée, car les requêtes sont envoyées simultanément à de très nombreux ordinateurs pour noyer le réseau et le rendre inutilisable. Classiquement, le Smurf Attack est une forme d'attaque par DDoS. Ce type de programme exploite les vulnérabilités du protocole IP et du protocole de messages de contrôle sur Internet, utilisé par les administrateurs pour connaître l'état d'un réseau.

ou pour gérer des médias personnels (photos, vidéos, etc.). Un point d'attaque *Hacking Point* a été placé ici pour « permettre » à un attaquant de pénétrer le réseau interne au bateau ;

4. **Profil de bureautique et de maintenance :** Ces profils représentent les PC classiques (sous Win7 ou WinXP) utilisés par l'équipage pour rédiger des rapports de mission, lire des documents techniques et réaliser des tâches simples assurant le bon fonctionnement du navire. Le PC de maintenance joue un rôle plus important, car il est directement relié à la gestion des automates. Ce PC est souvent plus protégé que les autres, mais dispose tout de même de vulnérabilités exploitables pouvant avoir un impact important sur le fonctionnement du navire. Un point d'attaque *Hacking Point* a également été placé ici ;
5. **Profil d'automaticien :** il permet de configurer les automates principaux du bateau via le réseau. L'automaticien utilise cette voie pour accéder à distance aux PLC ;
6. **Profil de navigation :** il représente les yeux et les oreilles du navire. En effet, le multiplexeur NMEA ainsi que l'ECDIS permettent de gérer les informations cybernétiques de navigation à bord (VDR, GPS, AIS, etc.). Un *Hacking Point* a également été placé ici ;
7. **Profil d'automatique :** cette partie représente physiquement les armoires au sein du navire. Chaque boucle a une fonction cruciale dont la moindre compromission peut mettre à mal l'intégrité fonctionnelle et les biens supports du navire. Chaque armoire est reliée à différents capteurs et actionneurs qui sont directement gérés par les automaticiens et les techniciens. Il peut être tentant pour un attaquant de venir corrompre ce système afin de nuire à l'intégrité et à la disponibilité des systèmes du navire. Un *Hacking Point* peut également être placé ici.

IV.2.3 Les Systèmes de Contrôle Industriels

IV.2.3.1 Les différentes boucles

À bord du navire, différents systèmes de la plate-forme assurent des tâches de productions industrielles essentielles à son bon fonctionnement et à la garantie de conditions de vie optimales pour l'équipage et les passagers. Ces productions sont caractérisées par des processus industriels dont la stabilité est primordiale. Pour cela, des ICS assurent leur contrôle et leur automatisation à partir d'une grande variété de sous-systèmes. Les sous-systèmes industriels du Naval Cyber-Range sont organisés en quatre boucles réseau à savoir mobilité, sécurité, électricité et auxiliaire (Fig. IV.3) :

1. **la boucle mobilité** : ce système gère les modes de propulsion principale et des auxiliaires ainsi que les aides à la navigation (gouvernail, barre, hélice et ligne d'arbre, etc.) ;
2. **la boucle sécurité** : ce système gère la détection et la lutte contre le feu et les inondations, l'ouverture et la fermeture des vannes, des portes et des portes étanches et la ventilation ;

3. **la boucle électricité** : ce système assure la production d'énergie haute tension à bord indépendamment des sources (turbine, batteries, etc.). Le système transforme également la haute tension en basse tension et fournit l'alimentation des équipements nécessaires à bord ;
4. **la boucle auxiliaire** : ce système gère la consommation de carburant et d'huile, la distribution pneumatique et hydraulique à bord.

Pour assurer les fonctions qui leur sont attribuées, chacune de ces boucles est composée de divers capteurs et actionneurs réels ou simulés (Fig. IV.3), qui sont reliés à un ou plusieurs PLC(s). Ils sont chargés de fournir des ordres de commandes aux actionneurs à partir des différents programmes embarqués. La simulation de ces sous-systèmes présente de nombreux avantages dans le cadre des expérimentations réalisées au sein du Naval Cyber-Range. Premièrement, cela permet de faciliter la préparation des expérimentations par rapport au processus classique d'installation et de mise en service d'un sous-système réel. Un sous-système réel simulé est moins complexe tant au niveau du câblage que de son utilisation. Deuxièmement, l'utilisation des sous-systèmes simulés permet de générer très facilement et rapidement de nombreux changements d'état au regard de la complexité de la plate-forme. Ainsi, si l'on altère le fonctionnement des systèmes pendant une expérimentation, la plate-forme est faite pour revenir facilement à son état initial et cela permet de fournir des capacités de rejouabilité accrues au niveau de cette plate-forme d'expérimentation. Des sauvegardes sont faites de façon très fréquente, de sorte à pouvoir reconstruire très facilement l'entièreté de l'architecture après chaque expérimentation mettant à mal les systèmes qui la compose. Ainsi, la génération d'attaques n'a aucune incidence sur le Naval Cyber-Range, car ce dernier a justement été imaginé dans cette optique. Pour finir, le découpage en plusieurs sous-systèmes simulés permet de réduire les coûts d'acquisition là où certains sous-systèmes sont très onéreux. De la même manière, le fait que de nombreux systèmes soient simulés permet une meilleure adaptabilité et une évolution de la plate-forme. Le troisième type de sous-systèmes OT employé au sein de la plate-forme regroupe les sous-systèmes de communication qui sont associés à la réception et à l'envoi d'information depuis un lien par satellite vers l'extérieur du navire. Cette liaison est définie par de fortes contraintes liées à ses caractéristiques et à son utilisation. Parmi ces contraintes, on peut citer une bande passante limitée, de la latence, des délais de connexion importants et des pertes temporaires de liaison de sorte à modifier artificiellement la fiabilité et la disponibilité de certains systèmes.

L'ensemble de ces systèmes et sous-systèmes interconnectés a fait émerger une stratégie généralisée de collection de données. Cette stratégie permet de collecter et de rassembler tous les types de données issues de part et d'autre de la plate-forme, le tout horodaté par des serveurs de temps NTP - Network Time Protocol respectant les contraintes de temps spécifiques aux différents systèmes présents pour favoriser les expérimentations et les futures analyses présentées dans les chapitres suivants. Cette architecture a d'ailleurs permis de coordonner nos outils et logiciels de simulations utilisées (BridgeCommand et OpenCPN) avec des éléments physiques (les récepteurs / émetteurs GNSS et les boucles industrielles). De la même façon, il était nécessaire de placer aux

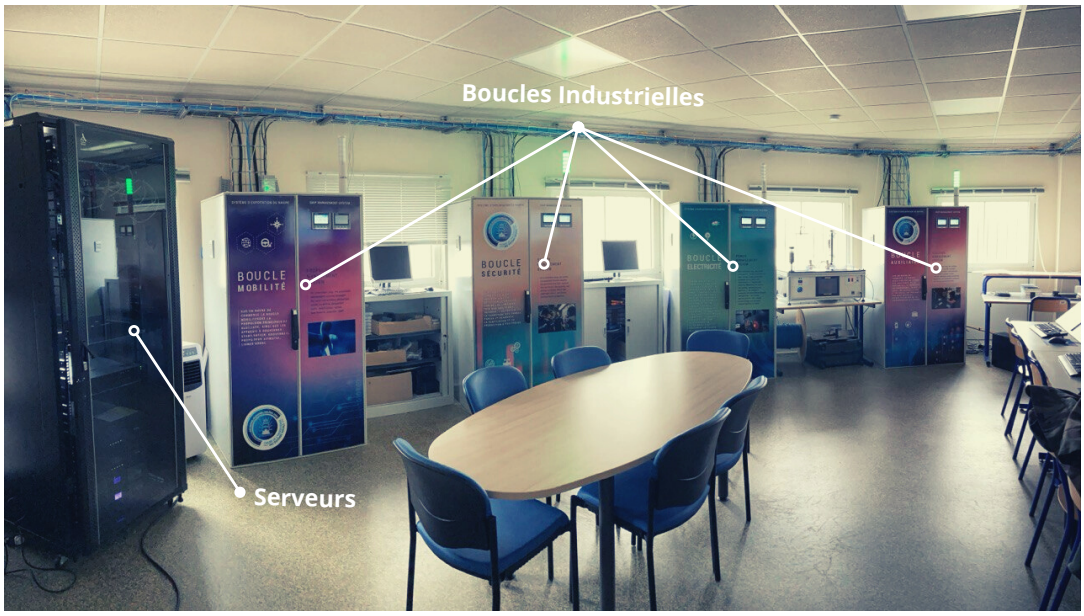


FIGURE IV.3 – Aperçu des quatre boucles de la plate-forme Naval Cyber-Range.

bons endroits un certain nombre d'éléments pour favoriser la détection comme l'ajout de sondes réseau NIDS propres aux protocoles spécifiques, que ce soit pour les données de navigation ou les données industrielles d'ailleurs. Enfin, différents capteurs, contrôleurs et actionneurs ont été installés par souci de réalisme. L'ensemble de ces outils et systèmes sont présentés dans la figure IV.4.

IV.2.3.2 Les capteurs et actionneurs

Pour la maniabilité du navire, des capteurs et des actionneurs ont été installés et configurés pour reproduire (de façon simplifiée) la passerelle de navigation du navire et effectuer les manœuvres classiques d'un navire. Ces systèmes sont reliés à un logiciel de simulation de navigation proposant un environnement virtuel de navigation qui a été modifié pour qu'il puisse interagir dans un environnement réaliste (la rade de Brest) et prendre en compte les autres éléments de la plate-forme. Pour cela, des « ponts de liaisons » ont été développés avec les autres équipements afin de permettre les échanges d'informations. Par exemple, si on diminue la vitesse via la manette (soit virtuellement ou soit via un joystick (*Ship Console* voir Fig. IV.8(b)) des gaz, alors cela est pris en compte dans les ICS par une action de décélération. Concrètement, cette action engendre la diminution de la vitesse de rotation de l'hélice et par une baisse de la consommation de carburant.

Pour rendre le Naval Cyber-Range plus réaliste, la plate-forme expose sur des choix technologiques spécifiques (Fig. IV.5). Ainsi, le choix s'est porté sur un système de propulsion hybride (diesel et électrique) appelé CODLAG (COmbined Diesel eLectric And Gas) [6]. L'intérêt d'une telle

6. On peut citer comme techniques de propulsion pour les navires civiles, le CODOG (COmbined Diesel Or

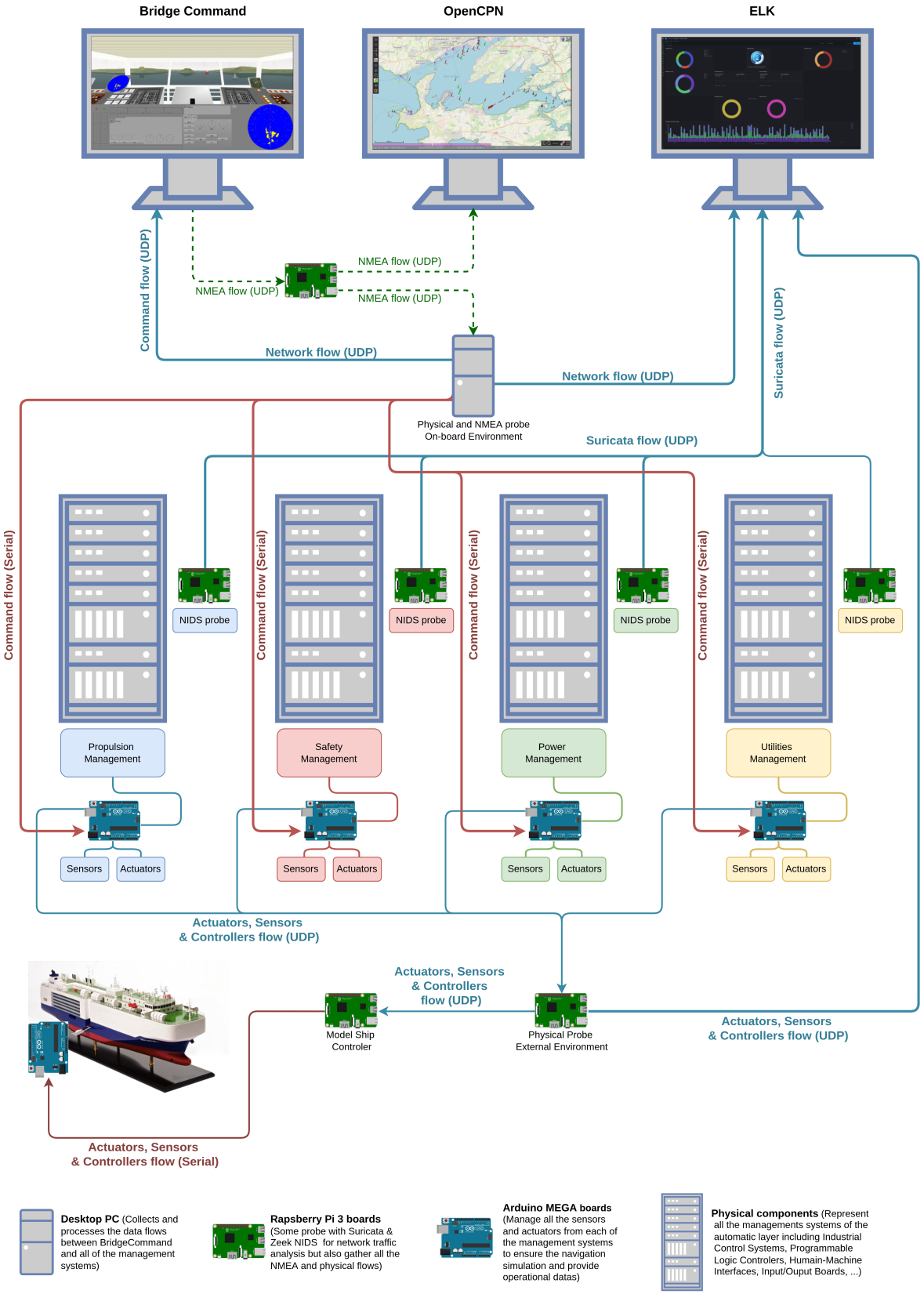


FIGURE IV.4 – Aperçu de la stratégie de collection de données de la plate-forme Naval Cyber-Range.

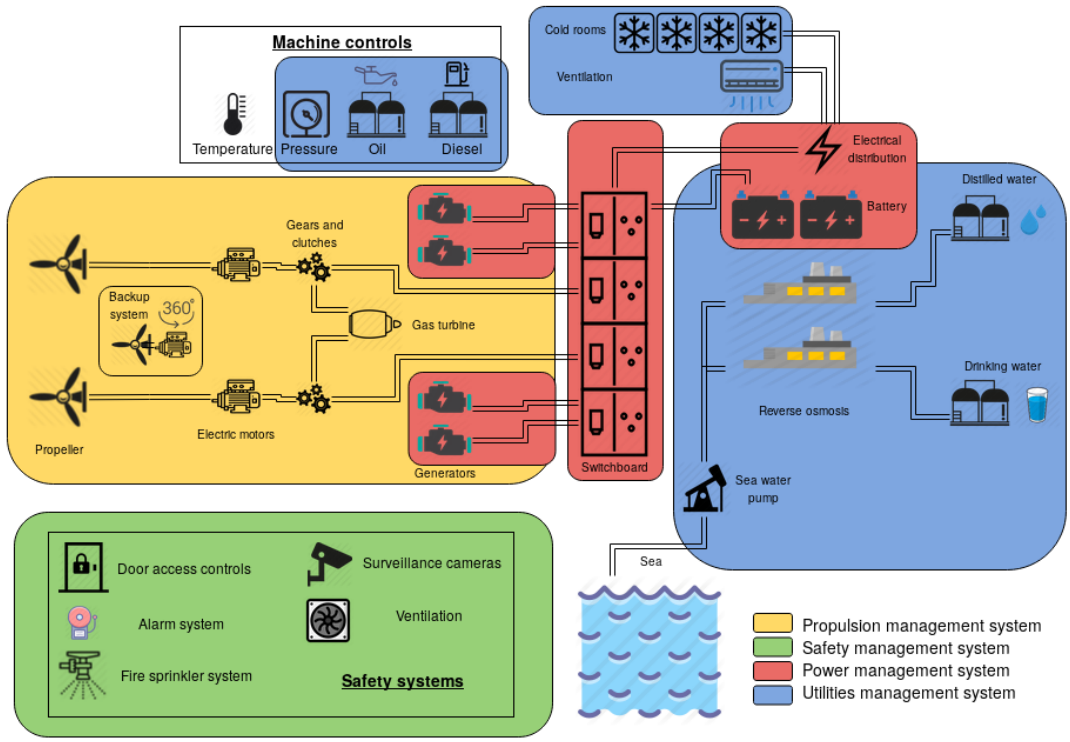


FIGURE IV.5 – Architecture de la partie capteurs et actionneurs de la plate-forme Naval Cyber-Range.

propulsion est de pouvoir faire appel à de nombreuses technologies différentes permettant de couvrir un plus large spectre de navires civils, mais aussi militaires.

Pour la gouverne, la technologie des safrans a été retenue, car c'est la plus commune. Ce choix permet ainsi de séparer naturellement la partie propulseur de la partie gouverne permettant ainsi, dans un cadre cyber, de proposer plus facilement une plus grande variété de scénarios d'attaques. Un système de propulsion auxiliaire a été ajouté, pour simuler certains manœuvres (pannes de propulsion, pertes de gouverne, etc.). Le choix s'est porté sur un propulseur azimutal à bascule (*Z-drive*) que l'on retrouve typiquement sur des embarcations nécessitant une grande flexibilité (remorqueurs, dragueurs, etc.), qui permet à lui seul de simuler le couple propulseur-gouvernail d'un navire. Nous listons ci-dessous, les spécifications de chaque automate (PLC) ainsi que les informations capteurs/actionneurs susceptibles d'être exploitées :

Propulsion management system (plus de détails dans le Tab. IV.1.)

— "PLC01 BCL1" : Propulsion modes *(with or without GT, backup system, etc.)*.

— "PLC02 BCL1" : Gas turbines *(sensors, power, etc.)*.

— "PLC03 BCL1" : Rudder & propeller shaft *(angle, speed, etc.)*.

Gas), le CODAG (COmbined Diesel And Gas), le CODLOG (COmbined Diesel eLectric Or Gas), le CODLAG ou le CODAD (COmbined Diesel And Diesel).

— "PLC04 BCL1" : Backup system.

Safety management system (plus de détails dans le Tab. IV.2.)

— "PLC01 BCL2" : Fire safety *(detectors, alarms, etc.)*.

— "PLC02 BCL2" : Ballast *(pump control, level or each compartment, etc.)*.

— "PLC03 BCL2" : Access controls *(doors, cameras, etc.)*.

— "PLC04 BCL2" : Ventilation systems.

Power management system (plus de détails dans le Tab. IV.3)

— "PLC01 BCL3" : Power distribution *(electrical distribution, battery, etc.)*.

— "PLC02 BCL3" : Power distribution.

— "PLC03 BCL3" : Alternator power *(generator controls, frequency, etc.)*.

— "PLC04 BCL3" : Alternator power.

Utilities management system (plus de détails dans le Tab. IV.4)

— "PLC01 BCL4" : Gasoil distribution *(pump, level, etc.)*.

— "PLC02 BCL4" : Fresh/Distilled water production and oil distribution.

— "PLC03 BCL4" : Air distribution *(pressure, repartition, etc.)*.

— "PLC04 BCL4" : Food/Cooling distribution.

Plusieurs capteurs et actionneurs utilisés au niveau de la plate-forme sont simulés (température, consommation, etc.) permettant ainsi, des alternatives réalistes comme le système de cuves simulant la consommation de carburant (Fig. IV.6) ou encore la console de commande (Fig. IV.8(b)). Pour plus de réalisme, la boucle système de propulsion et gouverne est modélisée à l'aide de petits moteurs à courant continu et de servomoteurs avec des LED traduisant leurs états *(marche, arrêt, anomalies, etc.)*. La boucle de sécurité utilise ce même système pour les alarmes, les détecteurs et les accès. Des interrupteurs de fin de course ou à contact magnétique sont utilisés pour détecter l'ouverture ou la fermeture des portes de chaque automate permettant de simuler des alertes d'intrusions sur les systèmes. Pour la boucle d'électricité, les générateurs sont des petits moteurs et le réseau électrique est reproduit à l'aide de LED adressables, de tubes lumineux ou de la fibre optique diffusante. De petits écrans OLED (*Organic LED*) ont été ajoutés afin de remonter certaines données comme la production électrique. Un système de petites pompes et de cuves est utilisé pour reproduire les systèmes de distributions d'eau, de fuel et d'huile sans oublier la simulation des ballasts (Fig. IV.6). Certaines pièces ont été réalisées à l'impression 3D pour compléter la plate-forme *(hélices, engrenages, etc.)*.

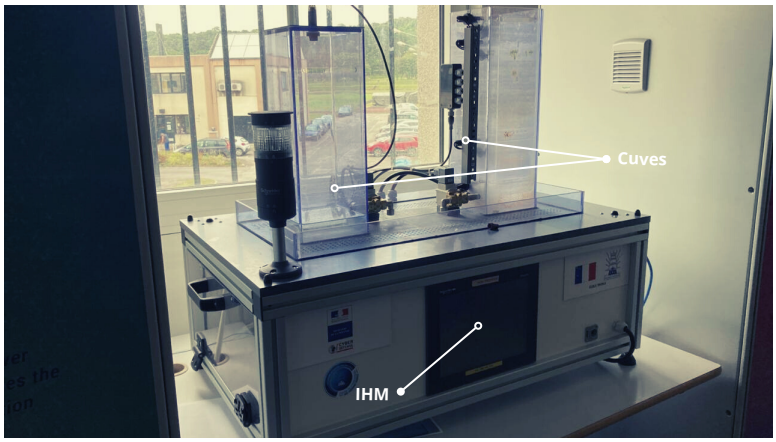


FIGURE IV.6 – Aperçu d'un système de cuves fonctionnelles au sein du Naval Cyber-Range permettant de reproduire le fonctionnement de la consommation de carburant.

TABLE IV.1 – Liste des données PLC de la boucle propulsion.

Propulsion management system				
Liste des données de la Boucle 1 (BLC1)				
PLC	Nom	Type	Unité	Notes
PLC 01	propulsion_modes	integer	...	0 : Arrêt, 1 : Croisière (uniquement D-E), 2 : Turbine à gaz + D-E, 3 : Manoeuvre (Utilisation du Backup), 4 : Backup only
PLC 02	gt_temperature	float	°C	Virtual
	gt_consumption	integer	g/kWh	Virtual
	gt_rpm	integer	tr/min	Virtual
	gt_load_rate	integer	%	DC Motor
	gt_power	float	MW	Virtual
	gt_nox_emissions	float	g/kWh	Virtual
PLC 03	rudder_angle	integer	°	Servomoteur
	ps_temperature	float	°C	Virtual
	ps_consumption	integer	g/kWh	Virtual
	ps_rpm	integer	tr/min	Virtual
	ps_load_rate	integer	%	DC Motor
	ps_power	float	MW	Virtual
PLC 04	backup_system_angle	integer	°	Servomoteur
	backup_system_temperature	float	°C	Virtual
	backup_system_consumption	integer	g/kWh	Virtual
	backup_system_rpm	integer	tr/min	Virtual
	ps_load_rate	integer	%	DC Motor
	backup_system_power	float	MW	Virtual

TABLE IV.2 – Liste des données PLC de la boucle sécurité.

Safety management system				
Liste des données de la Boucle 2 (BLC2)				
PLC	Nom	Type	Unité	Notes
PLC 01	fire_safety_alarms	boolean	...	Haut-parleurs
	fire_safety_lights	boolean	...	NeoPixel LEDs
PLC 02	ballast_level	integer	%	Capteur de niveau d'eau
	ballast_quantity	integer	L	Virtual
	ballast_pump_control	integer	L/min	Pompe
	ballast_valve_control	integer	L/min	Pompe
PLC 03	access_controls	boolean	...	NeoPixel LEDs
	camera_control	boolean	...	NeoPixel LEDs & camera
PLC 04	system_ventilation	integer	...	Fibre optique lumineuse

TABLE IV.3 – Liste des données PLC de la boucle électricité.

Power management system				
Liste des données de la Boucle 3 (BLC3)				
PLC	Nom	Type	Unité	Notes
PLC 01 & 02	power_distribution_state	integer	...	NeoPixel LEDs
	battery_level	integer	%	Virtual
	battery_capacity	integer	MW	Virtual
	battery_time	integer	h	Virtual
PLC 03 & 04	alternator_temperature	integer	°C	Virtual
	alternator_state	boolean	...	NeoPixel LEDs
	alternator_consommation	integer	g/kWh	Virtual
	alternator_rpm	integer	tr/min	Virtual
	alternator_taux_de_charge	integer	%	Virtual
	alternator_puissance	integer	MW	Virtual
	alternator_nox_emissions	integer	g/kWh	Virtual

IV.2.4 Les systèmes de navigation

Les sous-systèmes dits de "passerelle" sont similaires à ceux d'un navire civil de taille moyenne. On y distingue des récepteurs GNSS, AIS, ainsi que les différentes antennes associées. Ces éléments sont reliés à des connexions aux standards NMEA 0183 et 2000. Divers écrans sont utilisés pour l'affichage du système de cartes électroniques et la visualisation du simulateur de navigation 3D.

IV.2.4.1 Les systèmes de navigation intégrés

Cette plate-forme bien que disposant d'une partie entièrement physique (console de navire avec le joystick ou VDR (Fig. IV.8)), de nombreux éléments sont simulés. Pour représenter virtuellement

TABLE IV.4 – Liste des données PLC de la boucle auxiliaire.

Utilities management system				
Liste des données de la Boucle 4 (BLC4)				
PLC	Nom	Type	Unité	Notes
PLC 01	gasoil_level	integer	%	Capteur de niveau d'eau
	gasoil_quantity	integer	L	Virtual
	gasoil_time	integer	h	Virtual
	gasoil_pump	integer	L/min	Pompe
	gasoil_valve	integer	L/min	Pompe
PLC 02	oil_level	integer	%	Capteur de niveau d'eau
	oil_quantity	integer	L	Virtual
	oil_time	integer	h	Virtual
	oil_pump	integer	L/min	Pompe
	oil_valve	integer	L/min	Pompe
	fresh_water_quantity	integer	m^3	Virtual
	fresh_water_time	integer	jour	Virtual
	fresh_water_level	integer	%	Capteur de niveau d'eau
	fresh_water_pump	integer	L/min	Pompe
	fresh_water_valve	integer	L/min	Pompe
	distilled_water_quantity	integer	m^3	Virtual
	distilled_water_time	integer	jour	Virtual
	distilled_water_level	integer	%	Capteur de niveau d'eau
	distilled_water_pump	integer	L/min	Pompe
	distilled_water_valve	integer	L/min	Pompe
PLC 03	compressor_state	boolean	...	NeoPixel LEDs
	compressor_capacity	integer	L	Virtual
	compressor_debit	integer	L/min	Virtual
	compressor_pressure	integer	bar	Virtual
PLC 04	cooling_distribution_temperature	integer	C	Virtual
	cooling_distribution_humidity	integer	%	Virtual

l'environnement du bateau et les diverses informations liées à celui-ci, des logiciels sont installés à des endroits bien spécifiques de l'architecture. Comme la plate-forme est aussi exploitée pour le projet européen *Foresight*, l'idée a été de se tourner vers des solutions open source (Fig. IV.7) :

— **Logiciel Bridge-Command** [7] : ce simulateur de passerelle de bateau interactif en 3D, permet de se mettre aux commandes du bateau pour réaliser des entraînements aux manœuvres de navigation. Il comprend plusieurs systèmes, un Radar ainsi que la possibilité d'exécuter des contrôles directement depuis le PC. Pour notre plate-forme, ce logiciel permet la modélisation 3D du navire dans son environnement ;

— **Logiciel OpenCPN** [8] : ce logiciel de navigation maritime est basé sur une cartographie aussi

7. https ://www.bridgecommand.co.uk/
8. https ://opencpn.org/OpenCPN/info/downloads.html

en "open-source" OpenSeaMap [9] et permet de visualiser la position en temps réel du navire virtuel sur une carte prédéfinie. Combiné à Bridge-Command, il permet de générer des trafics NMEA, GPS et AIS et de simuler une boite noire (VDR) via l'ajout de "plugins" ;

— **Tableau de bord simplifié** : basé sur Grafana [10], ce tableau est relié à Bridge-Command et permet d'avoir un tableau beaucoup plus explicite avec plusieurs vues et de choisir ce que l'on veut afficher via l'ajout ou la suppression de différents modules.

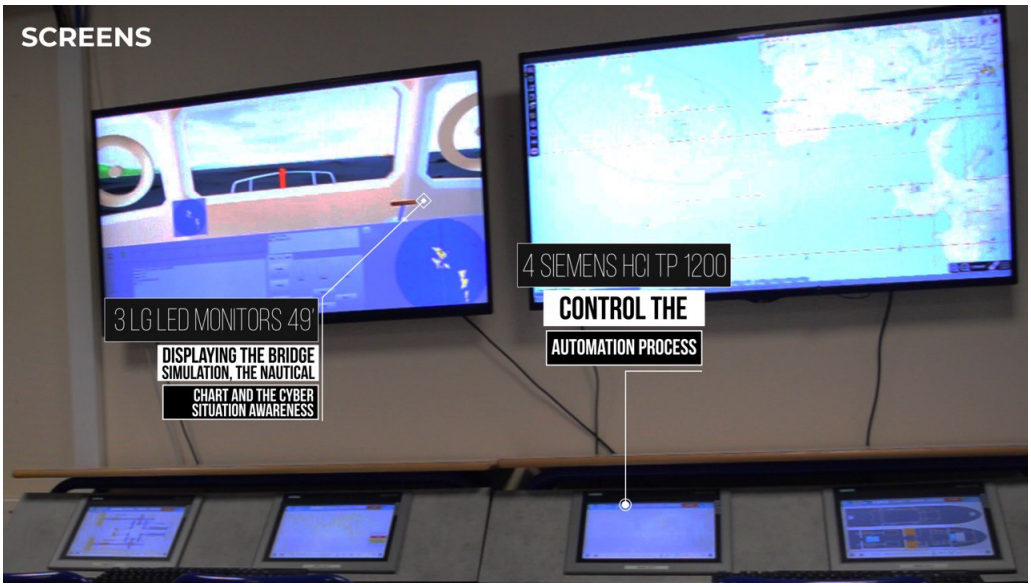


FIGURE IV.7 – Passerelle du navire simulé à l'aide des logiciels Bridge-Command (simulateur de navigation) à gauche et d'OpenCPN (cartographie maritime) à droite.

(a) (b)

FIGURE IV.8 – Prototype de VDR développé au sein du Naval Cyber-Range (à gauche). Console de commande utilisée pour la partie passerelle du navire au sein du Naval Cyber-Range (à droite).

9. http ://openseamap.org/index.php
10. https ://grafana.com/

IV.2.4.2 Les systèmes de positionnement

À l'image de l'installation des ICS réalistes intégrés dans la plate-forme, des systèmes de navigation ont été installés pour bénéficier de données de navigation réalistes (Fig. IV.9). Ainsi, un GPS Furuno $GP-33$ [11] et un récepteur Furuno AIS $FA70$ [12], dont les données transitent via un Bus NMEA sont utilisés. Ces derniers sont munis d'antennes réceptrices installées à l'extérieur du bâtiment dans lequel se situe la plate-forme. Pour des raisons évidentes, les données reçues par le récepteur GPS sont souvent toujours les mêmes puisque la plate-forme ne bouge pas. L'intérêt est d'obtenir des données réalistes et suffisamment riches (en volume) pour comprendre le fonctionnement spécifique des protocoles. L'ensemble des données sont envoyées sur l'ECDIS. La figure IV.10 illustre les systèmes de navigation installés dans la plate-forme. À noter que nous reviendrons sur cette limite de réalisme à la fin du chapitre en proposant une solution originale (section V.4).

FIGURE IV.9 – Aperçu des systèmes de navigation intégrés à la plate-forme.

IV.3 Descriptions et vulnérabilités des protocoles industriels

Dans cette section, il s'agit de présenter et d'analyser les différents protocoles utilisés dans les ICS. Dans un second temps, les vulnérabilités de ces protocoles sont détaillées. Pour finir, un démonstrateur permettant des attaques sur les PLC de la plate-forme est décrit.

11. https ://www.furuno.fr/v18a/lang–fr–art–GP-33–GP33.html
12. https ://www.furuno.fr/lang–fr–art–FA-70–FA70.html

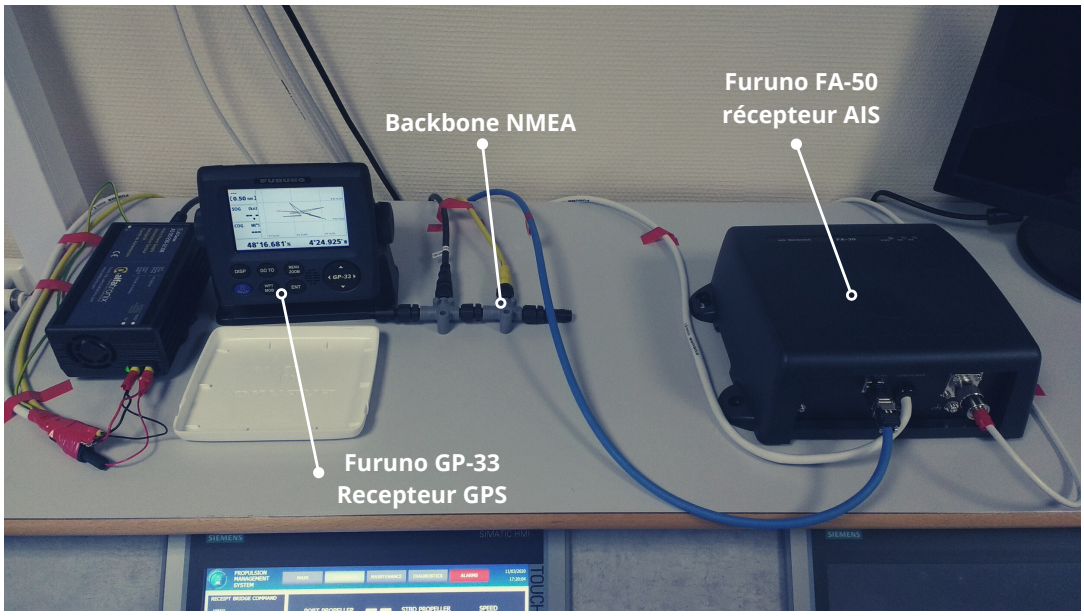


FIGURE IV.10 – De gauche à droite : récepteur GPS, connecteur NMEA 0183 et BUS NMEA 2000 avec récepteurs AIS intégrés à la plate-forme.

IV.3.1 Spécificités des protocoles industriels

Pour le Naval Cyber-Range, les ICS utilisés sont des PLC qui utilisent un protocole propriétaire pour leurs interconnexions appelé "S7comm" (pour S7 COMMunication). Le protocole "S7comm" est utilisé pour les PLC : S7-300/400 et le protocole "S7comm Plus" pour les séries : S7-1200/1500. Ce protocole permet la communication entre automates et systèmes de gestion, l'échange de données entre eux, l'accès aux données des automates à partir de systèmes SCADA à des fins de contrôles, de supervision ou de diagnostics. Le protocole a largement été "rétro-ingénieuré" pour en comprendre son fonctionnement et ses vulnérabilités. Les données "S7comm" sont fournies sous forme de paquets de données COTP (Connection Oriented Transport Protocol).

La principale fonction de ce protocole est de faire communiquer un PLC avec la station d'ingénierie. En fonctionnement nominal, la plupart des fonctions implémentées dans le protocole S7comm ne sont pas exploitées et donc peuvent être détournées dans un cadre malveillant afin de modifier arbitrairement le comportement du processus industriel. De par sa conception, le protocole S7 est orienté sous forme de blocs et repose sur l'ISO TCP/IP (ou RFC 1006). Chaque bloc appelé PDU (Protocol Data Unit [13]) suit les principes d'encapsulation TCP/IP et possède une taille maximale dépendant du type d'automate et il est prédéfini lors de l'initialisation de la connexion S7comm. Ainsi si la taille de la commande dépasse celle de la PDU, alors celle-ci sera automatiquement répartie en plusieurs PDU. Chaque bloc PDU est ainsi composé :

13. https ://www.techtarget.com/searchnetworking/ definition/protocol-data-unit-PDU

- ✓ d'une en-tête (obligatoire) ;
- ✓ d'un ensemble de paramètres (obligatoire) ;
- ✓ de données de paramètres (optionnel) ;
- ✓ d'un bloc de données (optionnel).

La figure (IV.11) illustre le principe d'encapsulation historique du protocole S7comm dans le protocole TCP/IP. Ce protocole est en charge des sessions COTP ainsi que de la taille des données à transporter (*Transport PacKeT* - TPKT). Afin de mieux comprendre le fonctionnement du proto-

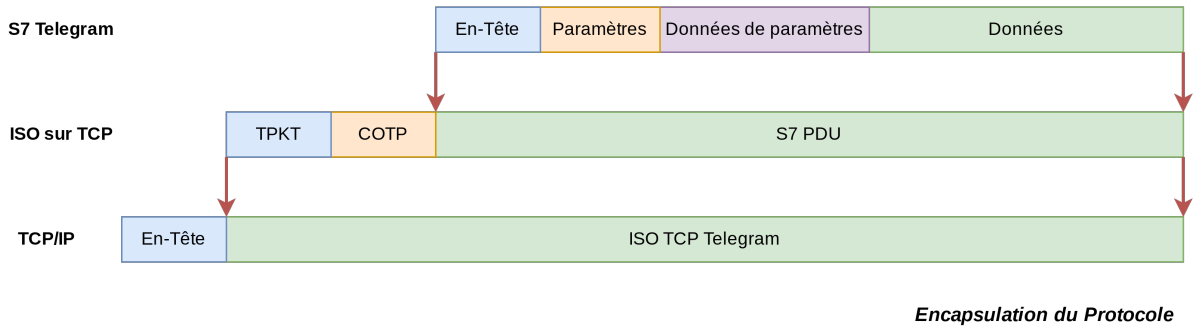


FIGURE IV.11 – Principe d'encapsulation du protocole *S7* dans le protocole TCP/IP.

cole S7comm et potentiellement identifier les sources de vulnérabilités, il est intéressant de décrire les différents blocs constituant le programme d'un automate. Classiquement, celui-ci est constitué de différentes zones : organisation, fonctionnelle, préprogrammée, donnée, etc. (Table IV.5).

IV.3.2 Vulnérabilités des protocoles industriels

Les protocoles de communications industriels ont été conçus en tenant compte de la performance des systèmes sans prise en considération de la sécurité des échanges. La sûreté est assurée par l'isolation des systèmes entre eux. Cependant, avec l'évolution des ICS, ils sont de plus en plus exposés à des risques de sécurité causés par les vulnérabilités des protocoles utilisés. Les communications utilisant le protocole Modbus ou S7comm ne présentent aucun mécanisme de chiffrement ou d'authentification [14]. Certes, l'absence de mécanisme de chiffrement et d'authentification permet de rendre la communication efficace en termes de temps de réponse, mais représente la principale porte d'entrée pour de graves problèmes de sécurité. Le détail des différents protocoles industriels utilisés sur la plate-forme montre clairement un manque de considération au niveau de la sécurité lors de la conception des protocoles industriels et est donc la porte ouverte à un grand nombre de failles de sécurité [15]. Cependant, les outils utilisés pour programmer les automates proposent des

14. https ://www.datasecuritybreach.fr/la-securite-informatique-au-sein-des-environnements-industriels-4-0-le-savoir-est-la-meilleure-protection/
15. https ://conference.hitb.org/hitbsecconf2021ams/materials/D2%20COMMSEC%20-%20Breaking%20Siemens%20SIMATIC%20S7%20PLC%20Protection%20Mechanism%20-%20Gao%20Jian.pdf

TABLE IV.5 – Différents types de bloc d'un programme d'automate.

Types de blocs	**Description des fonctions associées**
Blocs d'organisation (OB)	Les OB déterminent la structure du programme. Par exemple, l'OB 100 définit la séquence d'initialisation du programme lors d'un démarrage.
Blocs fonctionnels système (SFB)	Les SFB sont préprogrammés et faisant partie du système d'exploitation intégré à la CPU S7. Ils sont utilisés par la communication par liaisons configurées. Ces blocs permettent, par exemple, de gérer les fonctions de copie de blocs, le contrôle du programme, la gestion de l'horloge et du compteur d'heure de fonctionnement ou la gestion des événements d'erreurs et des alarmes.
Blocs d'état du système (SZL)	Les blocs de zone mémoire des données fournissent la liste d'états du système. C'est dans cette zone que l'on trouve le niveau de protection de la CPU.
Blocs fonctionnels (FB)	Les FB permettent d'écrire une zone de code implémentant une fonction comparable au C. Ces blocs doivent être appelés avec un bloc DB en paramètre.
Blocs fonctionnels (FC)	Les FC permettent de décrire une fonction (comme en C). Contrairement aux blocs FB, ces blocs n'ont pas de paramètres et sont utilisés pour programmer des routines.
Blocs de données (DB ou DataBlocks)	Les blocs sont des zones mémoires dans lesquelles sont enregistrées les données utilisateurs. Ces données globales sont utilisables par tous les blocs. es DB sont affectés aux blocs fonctionnels FB et SFB appelés. Ils sont générés automatiquement lors de la compilation du programme.

fonctions de protection en lecture/écriture des programmes. Cette fonction permet ainsi de limiter l'accès des zones mémoires SFB, SFC, OBB, FB, FC via le protocole "S7comm". Un mécanisme d'authentification par mot de passe est alors mis en place lorsque ce paramètre est activé. Il permet soit de protéger ces zones en lecture seulement, soit en lecture et en écriture. Cependant, il est important de noter que les zones mémoires de type DB restent toujours accessibles en lecture et en écriture offrant des portes dérobées à toutes intrusions malveillantes.

De nombreuses fonctions ont été développées pour assurer la communication entre un automate et sa station de maintenance. Cependant, à cause des faiblesses de sécurité non prises en compte, ces fonctions peuvent être détournées et exploitées dans un but malveillant par un attaquant. Ci-dessous, une liste de certaines des faiblesses est décrite.

Protocole en texte brut (absence de chiffrement)

Le protocole S7 est transmis en brut sur le canal de communication sans aucune politique de chiffrement. Cela peut permettre à un attaquant (via une écoute du réseau par un Man-In-The-Middle (MITM)) d'analyser totalement le contenu des communications et donc des informations contenues dans les trames. Un autre type d'attaque avec le protocole S7 est l'attaque par "rejeu". Un attaquant peut enregistrer les trames sur le réseau, forger de nouvelles trames à sa guise avec, par exemple, des informations fausses ou partiellement vraies et les rejouer pour leurrer l'opérateur ou perpétrer des opérations de sabotage.

Saturation des connexions à un PLC S7-300

La connexion à un PLC via le protocole S7 est toujours possible si le nombre de connexions simultanées (au maximum 16) n'est pas atteint. Cette information est relativement aisée à trouver via des logiciels permettant la programmation et la gestion à distance des automates. En ayant cette connaissance, il est aisé de provoquer un DoS en saturant les connexions. Ainsi, aucune opération de maintenance ne devient possible.

Utilisation de la commande "stop"

Une autre attaque via le protocole S7 est l'envoi de la commande "stop". Elle permet de stopper le programme utilisateur et, habituellement, cette commande est accessible via la station de développement. Il est à noter que cette fonction est classiquement implémentée par le constructeur pour faciliter le développement du système, mais il est indéniable que cette dernière peut avoir de lourdes conséquences si elle est détournée de son but initial.

Modification du comportement d'un programme Siemens

Un attaquant souhaitant saboter un navire cherchera à modifier au moins un des processus industriels vitaux afin d'en modifier son comportement. Pour cela, il est nécessaire de modifier le comportement du logiciel utilisateur implémenté dans le PLC. La difficulté majeure pour un attaquant, cherchant à mettre en place une Advanced Persistent Threat, est alors de se procurer les mêmes versions de logiciels. Cela lui permet, par la suite, d'altérer des zones mémoires OB, FB et FC contenant le programme.

Modification (en écriture) directement sur les DB (DataBlocks)

Ce type de zone mémoire contient toutes les variables internes du programme. Or, les zones mémoires DB n'étant pas protégées, un attaquant peut facilement y récupérer le contenu en téléchargeant le bloc voulu et en y injectant de fausses valeurs. Par exemple, dans un programme permettant de contrôler un moteur, il existe une variable mémorisant la vitesse de rotation (ou du moins un équivalent). Cette dernière est stockée dans une zone DB. Pour modifier la valeur de la vitesse du moteur, l'attaquant peut ainsi écraser la valeur de la variable dans la zone DB par celle de son choix. On comprend aisément la criticité d'un tel accès.

Modification "fine" du programme
Il est possible de télécharger le programme contenu dans un automate. La fonction "download" du protocole S7 permet de modifier les zones OB, FB et FC sans modifier en profondeur l'ensemble du programme. Cette fonction permet aussi de changer les paramètres système SFB et SFC. C'est de cette façon que le PC de maintenance met à jour le programme de l'automate et sa configuration.

Niveau de sécurité de la protection de la CPU toute relative
Les zones mémoires OB, SFB, SFC, FB et FC peuvent être parfois protégés par un mot de passe, mais ce dernier peut facilement être contourné puisqu'il est souvent en visible en clair ou renseigné la plupart du temps par défaut.

Rappelons que tous ces systèmes n'ont pas été développés avec un esprit de sécurité informatique, mais plutôt en termes de résilience et de performance. D'où cette facilité à pouvoir contourner ou à exploiter aussi facilement les failles de sécurité. Cela sera abordé au chapitre suivant (section V.2) portant sur un outil que nous avons développé qui permet d'injecter des attaques sur le logiciel de PLC.

IV.4 Descriptions et spécificités des protocoles NMEA

Avant qu'une normalisation de la circulation de l'information à bord des bateaux ne s'impose, chaque fabricant de matériel développait ses propres protocoles et ses Bus de communication. La norme NMEA (National Marine Electronic Association) a permis tout cela et grandement facilité l'intégration des sous-systèmes. Nous donnons dans ce qui suit une description détaillée de l'enveloppe du standard NMEA 0183, permettant de proposer, par la suite, des méthodes de détection d'anomalies adaptées à notre problématique.

IV.4.1 Descriptions des protocoles de navigation NMEA

La NMEA est une organisation américaine [16] fondée en 1957 fédérant les fabricants d'électronique marine pour standardiser la communication entre les différents composants électroniques présents au sein d'un navire. Le principe de fonctionnement est de connecter sur un unique réseau l'ensemble des capteurs/actionneurs allant des capteurs/actionneurs moteur(s) (températures, pressions, etc.), mais aussi le Radar, le sondeur, l'AIS, le GPS, le loch, le compas, l'anémomètre, ou tous autres capteurs disponibles sur un bateau. Il ne reste plus qu'à brancher un ou plusieurs afficheurs (PC ou afficheur NMEA spécifique du commerce) pour lire les données envoyées sur le réseau. Il existe principalement trois standards : les normes 0183, 2000 et OneNet.

16. https ://www.nmea.org/

La norme NMEA 0183

Après quelques versions (NMEA 0400, NMEA 0180 et NMEA 0182), ce standard a été publié et progressivement utilisé dans le monde entier dans de nombreux segments de l'industrie nautique. La norme définit les exigences en matière de signaux électriques, le protocole et l'heure de transmission des données, ainsi que les formats de "phrases" spécifiques pour un bus de données série en 4800 bauds voire même 38400 bauds (pour les données AIS typiquement). Cette norme est destinée à prendre en charge la transmission de données en série unidirectionnelle d'un locuteur unique à un ou plusieurs auditeurs. Ces données sont sous forme ASCII relativement simple et peuvent inclure des informations telles que l'heure, la position, la vitesse, la profondeur de l'eau, etc. Depuis novembre 2018, NMEA a publié une nouvelle version de NMEA 0183. Cette version inclut des mises à jour importantes sur la "phrase GNSS" ou "trame GNSS" (détaillée dans la suite du chapitre). Cela inclut la clarification de l'interface pour l'interopérabilité avec les différents systèmes GNSS comme le GPS, GALILEO ou QZSS (Japon). Si le déploiement de ces nouveaux systèmes a accru le besoin des mises à jour, rien n'a vraiment été réalisé d'un point de vue sécurité des informations.

La norme NMEA 2000

Cette norme plus récente (année 2000), basée sur un bus CAN, permet une évolution et une installation plus efficace comparées à la version précédente. La communication est multidirectionnelle. Ainsi, un appareil électronique comme un échosondeur peut à la fois émettre des informations et recevoir les données des autres appareils du réseau NMEA 2000. Sa mise en œuvre est relativement plus coûteuse que la norme historique 0183 puisqu'elle nécessite des équipements plus récents.

La norme NMEA OneNet

Cette nouvelle norme est encore peu utilisée, car peu de matériel existe actuellement avec cette norme. Elle ne remplace pas la norme 2000, mais redéfinit la couche physique du réseau en se basant sur un réseau Ethernet à haut débit et IPV6 offrant ainsi des débits plus importants (partage de données volumineuses). Les trames logicielles sont identiques à la norme NMEA 2000. L'intérêt est qu'il est possible d'utiliser un câble RJ45 ou le Wi-Fi et de connecter jusqu'à 65000 appareils (contre 50 avec la norme NMEA 2000). Cette norme ne nécessite pas d'alimentation électrique, et permet une communication standardisée avec les objets du quotidien (PC, téléphone, etc.). Comme pour la norme NMEA 2000, l'ajout d'appareils est dit « Plug & Play » permettant ainsi des installations plus simples. L'inconvénient est que cette norme utilise le protocole UDP qui permet la diffusion de messages sans demander un acquittement de bonne réception. De plus, le fait d'utiliser Ethernet le rend plus vulnérable à des attaques de type réseau.

IV.4.2 Quelques spécificités du standard NMEA 0183

La NMEA a conçu différentes normes largement utilisées dans le secteur maritime pour atteindre l'interopérabilité entre chaque système. Cela permet l'échange d'informations entre les ins-

truments fabriqués par différents fabricants. Le principe étant de normaliser une interface commune aux niveaux physique, électrique et logique entre les capteurs, les actionneurs et les moyens de navigation utilisés à bord des navires. Tous les appareils compatibles NMEA peuvent envoyer, recevoir et interpréter les données envoyées à l'aide de cette norme (Fig. IV.13).

Les sources embarquées qui échangent des données NMEA via le bus/réseau peuvent être par exemple des capteurs de profondeur, de cap, de mouvement (vitesse, tangage, roulis, gouvernail) ou encore l'ECDIS. Les sources produisant des données NMEA peuvent également provenir de données externes (météo, etc.). Elles utilisent généralement des récepteurs radio et des antennes permettant de capter les signaux RF, de les démoduler et de les transmettre au format NMEA (VHF). Ces sources sont principalement les récepteurs GNSS (signaux GPS) et les systèmes AIS (Fig. IV.12).

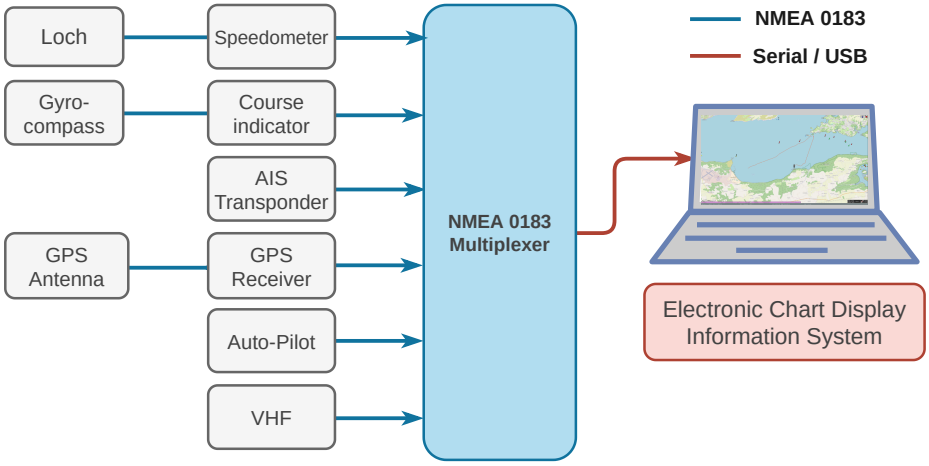


FIGURE IV.12 – Exemple de réseau au sein d'un "backbone" NMEA-0183.

La norme NMEA 0183 permet une communication unidirectionnelle avec un faible débit est contraignante puisqu'un seul émetteur est autorisé par nœud. Afin de permettre une communication complète entre plusieurs émetteurs NMEA 0183, un multiplexeur est nécessaire pour agréger toutes ces sources et les transmettre à un ou plusieurs récepteurs, comme illustrés sur la figure IV.13.

Pour la plate-forme, un réseau NMEA (versions 0183 et 2000) utilisant un récepteur GPS Furuno GP-33 et un récepteur AIS Furuno FA-30, ainsi que les antennes associées a été déployé. Le bus NMEA connecte chaque équipement pour permettre l'alimentation et les échanges de données (émission et/ou réception) (Fig. IV.12). Dans notre cas, le récepteur GPS émet ses données sur sa sortie NMEA 0183 et celles-ci passent par un multiplexeur à moindre coût composé d'un Raspberry Pi équipé d'un module (*Hat*) RS-422 (permettant de décoder/analyser les communications NMEA circulant sur le port série du GPS). Les données issues du Raspberry Pi peuvent ensuite être émises avec le protocole UDP sur un réseau Ethernet classique pour être utilisées par l'ECS, éléments permettant l'affichage des données de navigation, mais via un système non homologué par l'OMI [17].

17. https ://www.imo.org/ - Organisation Maritime Internationnale

En pratique, de nombreux équipements peuvent être connectés ensemble, soit directement sur le bus NMEA soit via un multiplexeur. Sur un navire de fort tonnage, ce réseau est appelé *Integrated Navigation System* (INS) et il est parfois directement intégré dans un réseau industriel comprenant les systèmes de contrôle-commande des ICS, appelé *INtegrated DBridge System* (IBS).

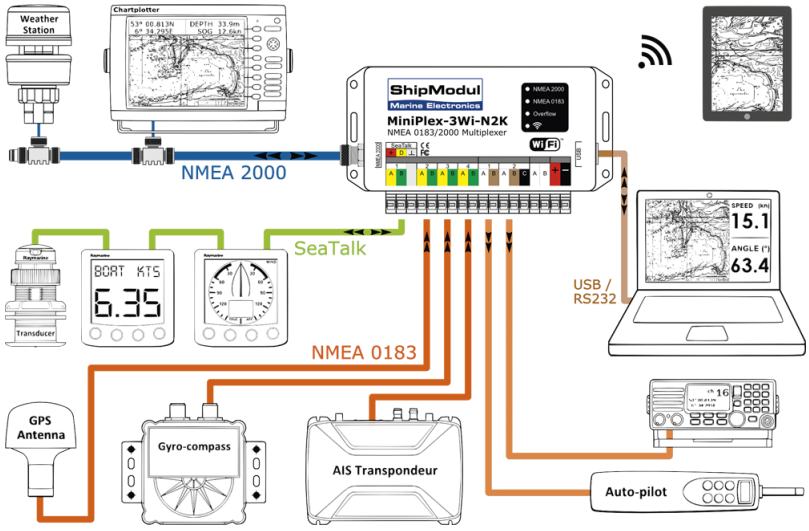


FIGURE IV.13 – Image d'un réseau multiplexeur NMEA 0183 et 2000 (Source Uship : https ://www.uship.fr/default/multiplexeurs-nmea-41223.html.

Si l'intrusion physique sur le bus NMEA (ajout d'équipement pour l'injection de données) est parfaitement envisageable, il a été décidé de se focaliser sur la connexion Ethernet et les données NMEA qui y circulent, car ce point d'accès est plus vulnérable et plus pertinent dans le cadre d'un accès (attaque) à distance. La détection d'anomalies sur un réseau NMEA peut s'effectuer à trois niveaux. Le premier concerne les données brutes transmises par le standard NMEA, c'est-à-dire les données contenues dans les différents champs des différentes trames (positions, géographiques, piste, AIS, données environnementales, etc.). Le second consiste à analyser l'enveloppe de la trame NMEA et ses caractéristiques via une connexion directe sur le Raspberry Pi et le module RS-422. Enfin, le troisième niveau se situe essentiellement une fois que le trafic est multiplexé et encapsulé dans le protocole UDP. Il s'agit de détecter des anomalies dans le trafic circulant sur le réseau INS. Cela est réalisé par une sonde réseau (NIDS).

À l'instar des enregistreurs de données de vol embarqués à bord des avions, l'OMI exige pour certaines catégories de navires l'embarquement d'un VDR qui permet aux enquêteurs d'examiner les procédures et les instructions dans les moments précédant un incident et aide à identifier les causes d'un accident. Les VDR recueillent des informations sur les communications radio VHF, les alarmes principales, les ouvertures des portes étanches de la coque, les contraintes exercées sur la coque, les valeurs du gouvernail, du moteur, de l'hélice, des propulseurs et de l'anémomètre, etc. En tant qu'outil de centralisation de la plupart des données relatives à la passerelle, aux moteurs,

à la sécurité et à la sûreté, les VDR sont exposés aux cyberattaques qui peuvent les compromettre. Dans cette thèse, l'exploitation des vulnérabilités de ce système n'a pas été prise en compte bien qu'un prototype développé en interne soit déployé sur la plate-forme (Fig. IV.8(a)).

IV.4.3 Quelques types de phrases NMEA 0183

Les dispositifs d'envoi de données sont appelés "Talkers". L'équipement qui reçoit les informations, tel qu'un Radar, ou un écran NMEA, est appelé un "Auditeur". Le protocole NMEA peut être envoyé par différents équipements, identifiés par leur identifiant "Talkers" et il est composé d'une variété de phrases (trames ou "sentences") qui suit un format prédéfini et propriétaire (voir Tableaux IV.6 [18] et IV.7 [19]). Une phrase NMEA 0183 est un message composé de 82 caractères au plus chacun étant codé sur 8 bits. Tous les caractères imprimables sont utilisables. La trame a une encapsulation relativement simple :

- ✓ un caractère de début spécifique généralement "$" (" !" pour les données AIS) ;
- ✓ un caractère de fin, classiquement, une étoile " * " ;
- ✓ deux caractères hexadécimaux autour de l'étoile correspondant à un checksum (somme de contrôle) permettant de confirmer la validité de la phrase (qui est en fait le résultat d'une opération "XOR" sur le contenu de la trame tout entière) ;
- ✓ et pour finir, deux caractères "invisibles" : le retour chariot [CR] et le passage à la ligne [LF].

Le message de la phrase NMEA 0183 se trouve ainsi entre le délimiteur de début "$" et l'étoile " * " et se décompose en différents champs séparés par des virgules. Le premier champ se compose normalement d'un code d'identification du locuteur (*Talker id* - Talker service) à deux lettres (Tableau IV.6), suivi d'un code de trois lettres pour la description du message (Table IV.7). On peut recenser plus d'une centaine de références de *Talker id* et 210 références de "sentences". L'ensemble de ces informations ont permis la création d'un dissecteur NMEA.

Trois trames NMEA en lien avec la localisation d'un système de positionnement (Table IV.9) sont reportées dans la Table IV.8. La phrase GPRMC correspond aux informations de navigation recommandées. La phrase GPGGA représente les données de localisation GPS et contient des informations sur la liaison satellite. La phrase GPVTG représente la vitesse vraie et celle au sol.

18. https ://www.nmea.org/Assets/NMEA 0183 Talker Identifier Mnemonics.pdf
19. https ://www.nmea.org/Assets/NMEA 0183 V4.11 Sentence Talker Identifiers.pdf

TABLE IV.6 – Exemples d'acronymes classiques (normes) d'identificateur de services.

Identificateur	Systèmes (Talker service)
AI	Mobile AIS station
CD	Digital Selective Calling (DSC)
EC	Electronic Chart Display & Information System (ECDIS)
GA	Galileo
GP	GPS (Global Positioning System) receiver
GL	GLONASS
GN	Mixed GPS and GLONASS data
II	Integrated Instrumentation
IN	Integrated Navigation
SD	Sounder Depth

TABLE IV.7 – Exemples d'acronymes classiques (normes) des messages NMEA (liste non exhaustive).

Code	Description du message
AAM	Waypoint Arrival Alarm (GPS)
APB	Phrase "B" pilote automatique
BOD	Relèvement de la destination d'origine
BWC	Relèvement et distance au point de route
GGA	Global Positioning fix data (GPS)
GLL	Latitude / Longitude data (GPS)
GSV	Satellites informations
GSA	Satellites IDs (GPS)
HDM	Cap magnétique
HDT	Cap vrai
RMA	Données LORAN spécifiques minimales
RMC	Recommended Minimum Navigation information (GPS)
RMB	Recommended Minimum data for Waypoints (GPS)
RPM	Revolutions (GPS)
RSA	Rudder Sensor Angle (GPS)
VTG	Track Made Good and Ground Speed (GPS)
VDR	Voyage Data Recorder
VDM	Information from other ships (AIS)
VDO	Information from your own ship (AIS)
XTE	Ecart de route traversier, mesuré
ZDA	Time and Date (GPS)

TABLE IV.8 – Exemples de trames (différentes) GPRMC, GPGGA, GPVTG, IIRPM, IIRSA, AIVDM issues de la plate-forme.

Trames GPRMC (GP RMC)
$ $GPRMC,215835.000,A,4817.1982,N,00424.8201,W,9.50,79.65,161220,,,A*54$
$ $GPRMC,130008,A,4817.053,N,00424.905,W,0.07,359.967133,301119,,A*60$
Trames GPGGA (GP GGA)
$ $GPGGA,125244,4816.8792,N,00424.4526,W,1,10,1.5,0.8,M,,M,,*4F$
$ $GPGGA,130026,4817.056,N,00424.905,W,8,8,0.9,0.0,M,0.0,M,,M,,*59$
Trames GPVTG (GP VTG)
$ $GPVTG,,T,143.4,M,11.5,N,21.4,K,A*0$
$ $GPVTG,,T,134.6,M,0.7,N,1.2,K,A*09$
Trames IIRPM (II RPM)
$ $IIRPM,S,1,70,100,A*76$
$ $IIRPM,S,2,100,100,A*40$
Trames IIRSA (II RSA)
$ $IIRSA,10,A,,*00$
$ $IIRSA-10,A,,*2D$
Trames AIVDM (AI VDM)
$ $AIVDM,1,1,,B,13I3:M?P1SOcKfHKc‘8<cgvt0D0R,0*32$
$ $AIVDM,1,1,,B,13P;K8@P00Oc“JKck=Rcwwp0D0I,0*7B$

Le tableau IV.9 détaille trois trames de position (distinctes) transmises par un récepteur GPS sur un réseau utilisant le standard NMEA 0183. Par exemple pour la trame GPGGA, les deux premiers caractères "GP" indiquent qu'il s'agit d'un équipement GPS ; les trois lettres "GGA" indiquent le type de trame et donc sa syntaxe, en l'occurrence, l'heure d'envoi de la trame (UTC), la position (latitude et longitude), la qualité de réception, le nombre de satellites utilisés pour calculer les coordonnées, la précision horizontale, l'altitude en mètres, ainsi que plusieurs autres champs additionnels. La trame GPRMC fournit les informations suivantes : la latitude, la longitude, la date ainsi que la vitesse et la route sur le fond, mais aucune information sur l'altitude.

TABLE IV.9 – Description de trames (différentes) GPRMC, GPGGA et GPVTG.

Field	Comments
$GPRMC	Sentence ID
215835	Time of the fix, here 21 :58 :35 UTC
A	Status (A is active, V is void)
4817.1982,N	Latitude 48° 53.363' N
00424.8201,W	Longitude 8° 31.0608' W
9.50	Speed over the ground in knots is 0 kts
79.65	Track angle in degrees is 18,233°
161220	Date is 16th of December 2020
*54	Checksum of the data
$GPGGA	Sentence ID
125244	Time of the fix, here 12 :52 :44 UTC
4816.8792,N	Latitude 48° 53.363' N
00424.4526,W	Longitude 8° 31.0608' W
1	Quality of GPS (GPS fix)
10	Number of satellites in view (00 - 12)
1.5	Horizontal dilution of precision
0.8	Antenna altitude
	Above/below mean-sea-level, Orthometric Height
M	Units of Orthometric Height
*4F	Checksum of the data
$GPVTG	Sentence ID
T	True
143.4	Track Degrees
M	Magnetic
11.5	Speed
N	Knots
21.4	Speed kilometers per hour
K	Kilometers per hour
A*0D	Checksum of the data

IV.5 Conclusion

Dans ce chapitre, l'environnement dans lequel se situe l'ensemble des travaux de thèse a été présenté : la plate-forme de reproduction numérique d'un navire situé à l'École Navale : Naval Cyber-Range. Cette nouvelle plate-forme numérique de simulation, correspondant au volet expérimental de la thèse a pour objectif, en partie, de générer, de collecter, de simuler et de synthétiser des données réalistes en vue d'études cybernétiques (attaque, défense, sécurité, résilience, modélisation,...) sur une plate-forme navale. Elle propose un environnement permettant d'élaborer des scénarios pertinents d'attaques réalistes par rapport aux incidents déjà produits dans ce genre d'infrastructure.

Les différentes systèmes employés dans cette plate-forme ont été présentés et des spécificités de fonctionnement et de vulnérabilité propres aux systèmes de Contrôles Industriels et aux systèmes de navigation ont été détaillées. Ici, il était question de finir de répondre à la **QR1** et d'apporter des éléments de réponse pour la **QR2**. Dans le chapitre suivant (Chap. V), il est question de présenter et de décrire les outils associés à la génération de données et à l'élaboration de scénarios.

Chapitre V

Expérimentation pour la Collecte et la Génération de Données Navales

Sommaire

V.1 Introduction

Ce chapitre présente notre contribution concernant l'enrichissement des bases de données industrielles et des données de navigation générées par la plate-forme précédemment présentée. Pour cela, un outil de génération d'attaques facilitant la conception de scénarios réalistes sera présenté. Ensuite, nous aborderons les différentes expérimentations menées pour comprendre comment se déroulent réellement des attaques issues de vraies données de navigation. Les résultats de ces ex-

périmentations ont motivé la conception d'un système embarqué. Ce système, nommé balise HAPPINESS, permet de collecter en temps réel et sur le plus long terme des données de navigation réelles provenant de bateaux et d'alimenter la plate-forme. Il a d'ailleurs été conçu en plusieurs prototypes. Enfin, le développement d'un deuxième outil de génération d'attaques associées aux données de navigation sera décrit, facilitant une nouvelle fois la génération de scénarios d'attaques sur la plate-forme.

Ce chapitre répond à la question de Recherche **QR2** mais aussi à la question de développement **QD1** comme l'indique la Fig.V.1.

Correspondance : Question de Recherche / Chapitre					
	Chap. II	Chap. III	Chap. IV	**Chap. V**	Chap. VI
QR I					
QR II					
QD I					
QR III					

FIGURE V.1 – Tableau de correspondances entre les Questions de Recherche et les Chapitres.

V.2 Développement de l'outil AEGIS

Pour faciliter la génération de scénarios d'attaques concernant les ICS, en se basant sur ceux présents dans la plate-forme, un outil capable d'injecter des anomalies dans le trafic réseau entre les automates et les ordinateurs de maintenance a été développé. Le principe de cet outil est d'exploiter le manque de mécanismes de cybersécurité sur les protocoles de communication entre les automates (section IV.3.2).

Pour répondre à cette préoccupation, l'outil développé AEGIS pour "**A**ttack and **E**xploit **G**enerator on **I**ndustrial control **S**ystems" permet de positionner l'attaquant entre le PC de maintenance et la cible, en l'occurrence un automate industriel dans notre cas. Du point de vue attaquant, l'outil permet de réaliser plusieurs types d'attaques sur la plate-forme Naval Cyber-Range :

— saturer le nombre de connexions afin de bloquer de nouvelles connexions légitimes (Fig. V.2). Il devient impossible, pour l'automaticien, de se connecter sur l'automate victime de l'attaque à moins de l'être déjà, car certaines connexions lui sont réservées initialement ;

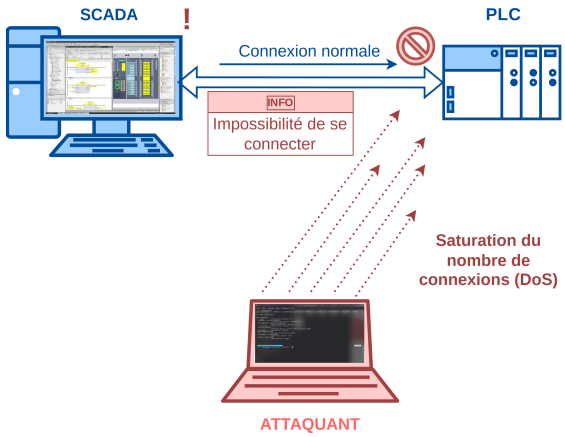


FIGURE V.2 – Schéma d'une attaque de saturation de connexions sur PLC.

— forcer le technicien à se déconnecter suite à un arrêt soudain et ensuite saturer les connexions ;

— supprimer à distance le bloc OB1 de l'automate (l'équivalent du « main » en C/C^{++}) (Fig. V.3). Cette attaque est subtile, car il n'y a pas, en général, de voyant visuel indiquant que l'automate rentre en « défaut ». Pour retrouver son fonctionnement nominal, il est nécessaire de réaliser une réinstallation complète du programme ;

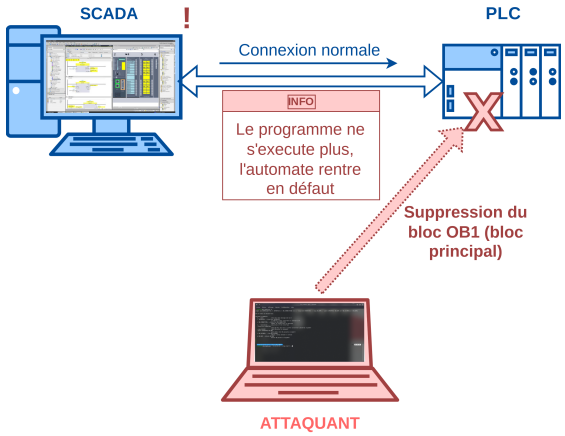


FIGURE V.3 – Schéma d'une attaque de suppression du bloc OB1 sur PLC.

— supprimer le bloc OB1 et saturation des connexions : cette attaque permet clairement de réaliser du DoS (Fig. V.4). L'automaticien n'a plus aucun moyen pour se connecter directement sur le système et de remettre en route l'automate en rechargeant le bloc du programme principal (plus aucune connexion n'est disponible) ;

— télécharger le bloc DB et OB1 d'un automate pour le charger dans un autre automate. En d'autres termes, un automate dédié à une tâche spécifique n'exécute plus les processus initiaux, mais ceux provenant d'un autre affecté à une autre tâche ;

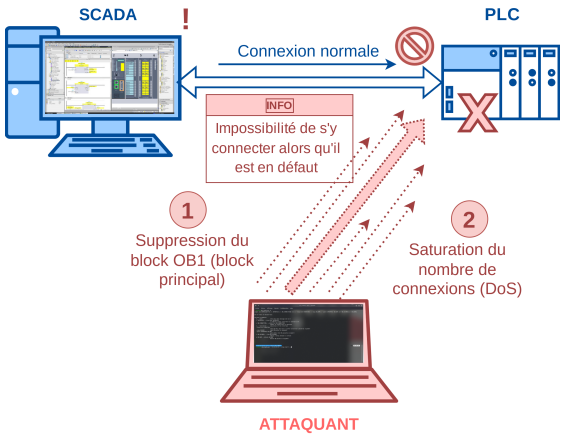


FIGURE V.4 – Schéma d'une attaque de suppression du bloc OB1 + Saturation de connexion sur PLC.

— téléchargement du bloc DB et OB1, mais cette fois-ci pour le charger en continu sur un automate (Fig. V.5). En plus d'exécuter des processus qui ne correspondent pas à la tâche initiale, l'automate ne pourra plus être reprogrammé pendant toute la durée de l'attaque. Cette attaque peut très bien se réaliser avec un programme vide ;

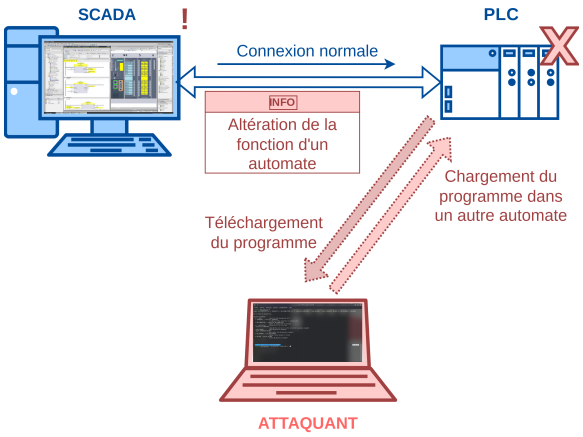


FIGURE V.5 – Schéma d'une attaque de "download and upload" illégitime d'un programme sur PLC.

— écrire dans les blocs mémoire des automates pour changer les valeurs initiales (falsification des informations) provenant des commandes de barres, les températures affichées sur les IHM, les consommations de carburant (Fig. V.6). Il s'agit ici de saboter le système ou du moins leurrer les opérateurs de bord ;

— envoyer une commande "stop" à l'automate en question (Fig. V.7). Le programme de ce dernier sera conservé, mais il ne répondra plus et n'effectuera plus la fonction qui lui est attribuée. C'est l'une des attaques les plus efficaces en termes de sabotage surtout dans le cas d'un système

critique comme une ligne d'arbre ou un gouvernail sur un navire.

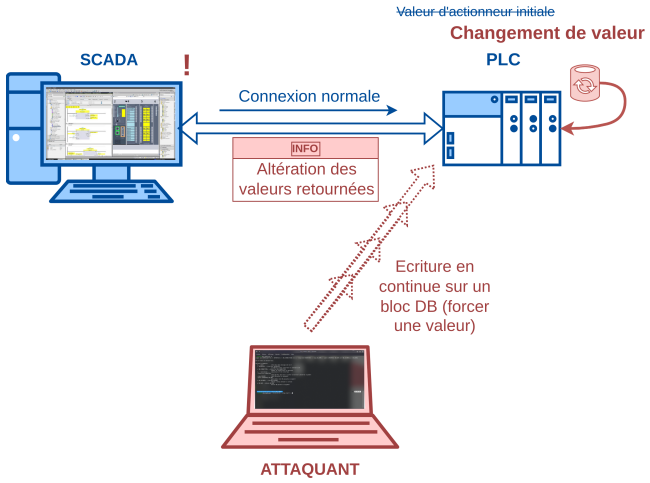


FIGURE V.6 – Schéma d'une attaque d'écriture en continu dans une variable de bloc mémoire sur PLC.

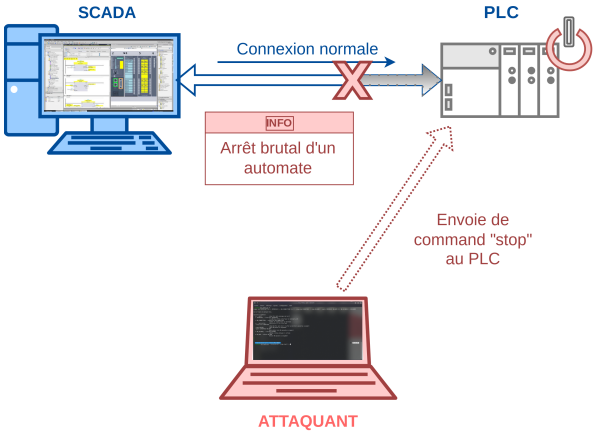


FIGURE V.7 – Schéma d'une attaque "stop" sur PLC.

Concrètement, chacune de ces actions peut être réalisée séquentiellement. Néanmoins, le réel intérêt est la possibilité de mener de bout en bout une véritable attaque généralisée sur un ou plusieurs automates (Fig. V.8) via une séquence qui pourrait être (approche classique dans une volonté de sabotage d'un automate) : la prise de renseignement sur l'automate cible, pour ensuite saturer le nombre de connexions et empêcher toutes actions légitimes, puis forcer le changement de la valeur, voire charger un programme malveillant ou supprimer le bloc principal. S'il s'agit par exemple d'une fonction assurant la navigation comme la vitesse des moteurs ou l'angle de barre, ce genre de situation peut vite devenir critique surtout si le bateau se trouve en mer.

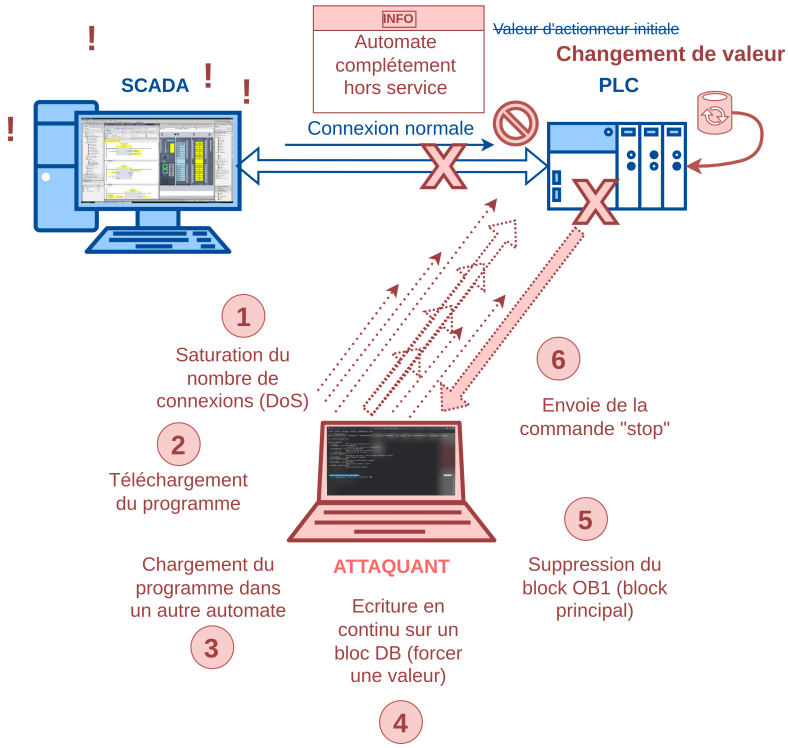


FIGURE V.8 – Schéma d'une attaque généralisée reprenant l'ensemble des attaques réalisables sur PLC en vue d'une opération de sabotage.

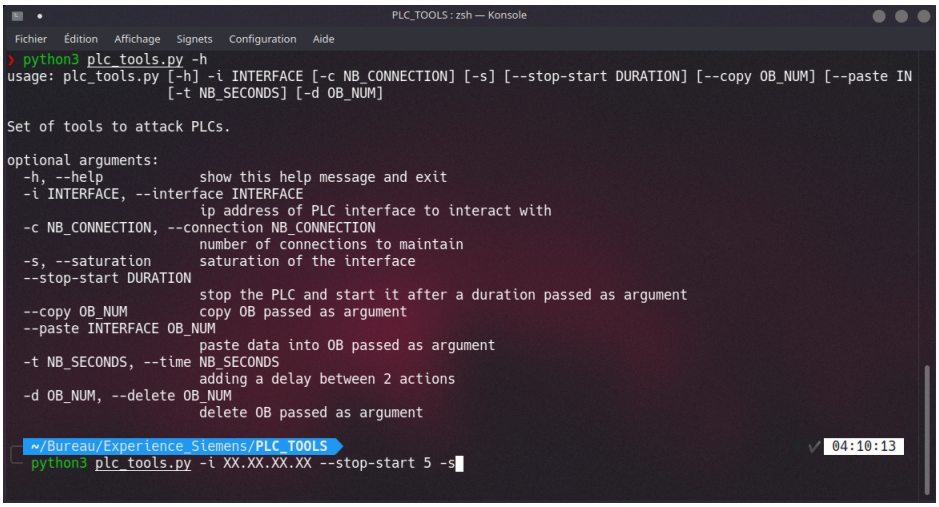


FIGURE V.9 – Exemple d'usage de l'outil AEGIS via le terminal attaquant.

La figure V.9 illustre la fenêtre de terminal utilisé pour injecter des anomalies dans les communications réseau entre SCADA et automates. Cet outil de démonstration permet d'automatiser et de regrouper l'ensemble des attaques que l'on souhaite effectuer sur l'ensemble des automates de la plate-forme. Il est important de remarquer que les automates exploités font partie des équipements physiques présents dans la plate-forme. L'idée n'est donc pas de venir réellement saboter ces équi-

pements au risque de compromettre le principe même de la plate-forme de simulation, mais bien de mettre en évidence les attaques possibles sur ce type d'équipements sans les rendre totalement hors service. Cet outil sera utilisé dans le chapitre VI pour les différents scénarios exploités dans les cas d'études sur les ICS (section VI.2).

Cet outil met en évidence la facilité d'accès et d'exécution de diverses commandes afin de mettre à mal toute une boucle de systèmes industriels critiques nécessaire au bon fonctionnement du navire.

V.3 Réalisation d'une Expérimentation : BELAMY

V.3.1 Motivation de l'expérimentation : les failles du NMEA

La norme NMEA 0183 comporte de nombreuses failles de sécurité, qui ne lui sont pas forcément directement imputables, et peuvent être classées en deux catégories. La première est associée aux capteurs eux-mêmes : ils peuvent être défaillants, de mauvaise qualité, ou encore soumis à des interférences extérieures (leurrage, brouillage dans le cas du GNSS). La deuxième est plus liée à des vulnérabilités sur le réseau NMEA lui-même et à sa conception : absence de dispositif garantissant l'authenticité, l'intégrité, la confidentialité, la disponibilité, la non-répudiation, la traçabilité des données.

Par la suite, ce travail propose d'explorer une autre voie en analysant et en traitant directement les trames NMEA de type GPRMC, GPGGA et GPVTG (chapitre VI - section VI.3). Aussi pour pouvoir concevoir des méthodes appropriées de détection d'anomalies en lien avec la norme NMEA, il est utile de bien identifier les vulnérabilités du GNSS (le "Jamming" et le "Spoofing" déjà abordés dans le chapitre II, section II.4.2.2). Rappelons que pour la constellation GPS, les signaux sont envoyés par les satellites avec une puissance allant de 25 à 50W et lorsqu'ils sont reçus par un récepteur GNSS (terrestre ou maritime), le signal est relativement faible, de l'ordre de 10^{-18}W dans la plupart des cas. Cela explique pourquoi il est facile de brouiller le GPS en produisant un signal RF suffisamment fort pour dépasser (aveugler) les signaux provenant des satellites, de sorte que les signaux légitimes ne puissent pas être récupérés et exploités [141]. La cible d'une attaque par brouillage GPS (Jamming) est la plupart du temps immédiatement consciente que quelque chose ne va pas, car le système GPS est rapidement incapable de produire un résultat de géolocalisation. Le brouillage du GPS peut être effectué de manière involontaire ou délibérée [52] (voir quelques exemples dans le chapitre III - section III.3.3). De son $c^o t, l'usurpation d'identit GPS (Spoofing) est une d'attaque plus labore qui consiste gnrer dlibrment de fausses in$

V.3.2 Expérimentation de cyberattaque en condition réelle

Afin de bien comprendre les conséquences de cette usurpation (leurrage) sur la trame NMEA, il est intéressant de pouvoir analyser et traiter de véritables trames NMEA obtenues dans le cadre de scénarios d'attaques réellement réalistes (Fig. V.10). Pour cela, nous avons mis au point BELAMY (en référence à Samuel Bellamy, dénommé "le Prince des pirates" célèbre pour ses actions comme pour pour sa fin tragique) l'acronyme de **B**asic **E**xperimentation of **L**ight spoofing **A**ttack on **M**aritime S**Y**stems). Cette campagne de tests reflète différentes expériences des conditions réelles à bord d'un bateau pneumatique à moteur de l'École Navale. Pendant plusieurs heures sur deux jours, dans la rade de Brest (face à l'École Navale) des tests et mesures ont été réalisés avec un niveau élevé de mesures de sécurité afin d'éviter les conséquences réelles avec d'autres utilisateurs GNSS (aériens, terrestres et maritimes) se trouvant à proximité. De telles expériences, bien que faciles à réaliser une fois que le matériel utilisé est maîtrisé, sont totalement interdites en France selon la législation en vigueur depuis 2012. La détention et l'utilisation de brouilleurs et autres systèmes radio permettant de rendre inopérants (ou de détourner) des systèmes de télécommunication est totalement proscrite par l'ARCEP (Autorité de Régulation des Communications Électroniques, des Postes et de la distribution de la presse). Des autorisations pour réaliser de telles expériences dans un environnement totalement sécurisé, sans gêner les bateaux se trouvant aux alentours et sous couvert d'autorisations officielles ont été demandées. De plus, pour le bon déroulement des expériences, la puissance d'émission du dispositif a été considérablement réduite pour limiter au maximum les impacts sur les actions opérationnelles environnantes en mesurant et en limitant la sphère d'impact du leurrage et du brouillage GNSS à 80m.

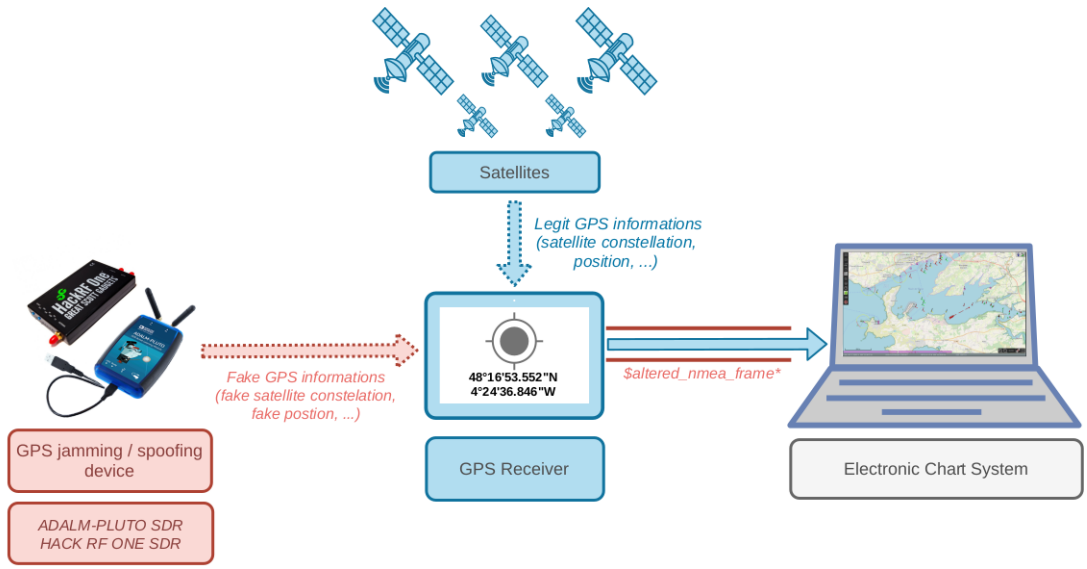


FIGURE V.10 – Modélisation d'une attaque de leurrage sur systèmes GPS par un attaquant externe.

Pour réaliser le leurrage et le brouillage GPS en conditions réelles, nous avons utilisé diffé-

rents outils de radio logicielle (*Software Defined Radio* - SDR). Le premier, un Adalm-Pluto SDR d'Analog Devices [1], normalement dédié à une fonction plus pédagogique, permet de réaliser ce type de manipulation lorsqu'on le détourne de sa fonction initiale. Le second, un HackRF-One SDR de Great Scott Gadgets [2], est un système dédié à ce type de pratiques. Dans les deux cas, la méthode reste globalement similaire. Le principe théorique du Spoofing GPS consiste à émettre une fausse constellation de satellites avec une puissance supérieure à celle émise par les vrais satellites de manière à modifier ou à faire dériver progressivement la position du récepteur GPS. Dans notre cas, il est important de récupérer les éphémérides (les informations contenant les paramètres orbitaux détaillés de chaque satellite). Ces données changent d'heure en heure et sont disponibles gratuitement sur l'un des sites dédiés de la NASA [3]. Ensuite, il est possible de générer une nouvelle constellation de satellites qui sera différente de la constellation réelle à un moment donné. Enfin, en définissant correctement au préalable les paramètres de latitude, longitude, altitude et l'intensité du signal, un signal faisant croire au récepteur qu'il se trouve à une autre position est généré puis émis à l'aide d'un module SDR. La figure (V.11) illustre le matériel utilisé ainsi qu'un acte de Spoofing "volontaire et maitrisé" sur de véritables systèmes d'acquisitions GNSS.

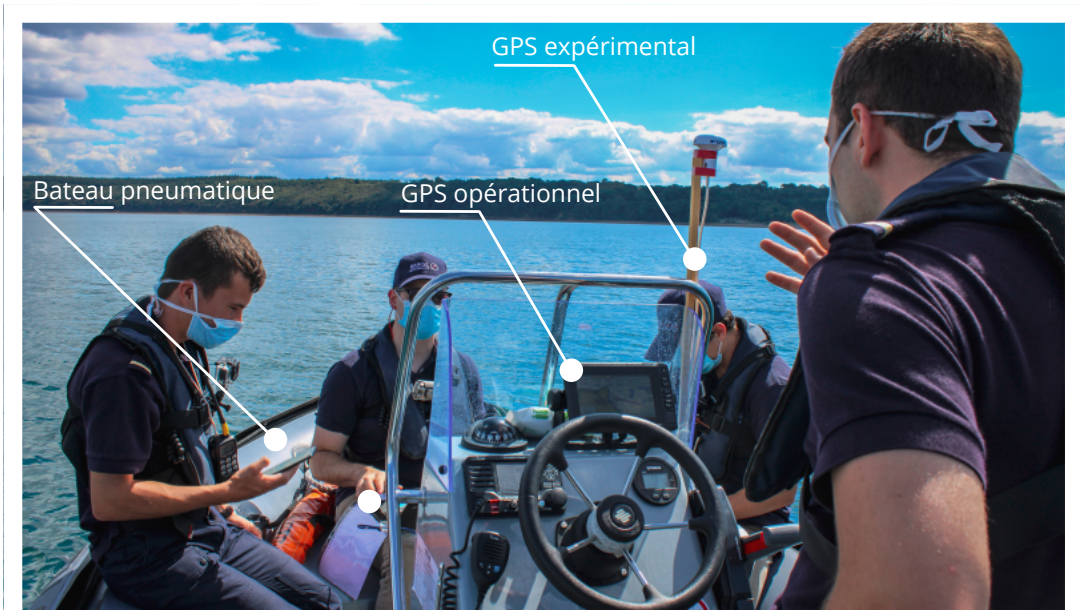
L'intérêt de telles expérimentations est en réalité double. La première est de comprendre et d'analyser l'impact d'une attaque (Jamming ou Spoofing) sur les données NMEA (plus spécifiquement les phrases de type GPRMC, GPGGA et GPVTG) (Tab. V.1, Tab. V.2 et Tab. V.3).

TABLE V.1 – Exemples de trames NMEA normales et anormales de type "GPRMC".

Trames GPRMC (comportement normal)
$\$\ GPRMC, 125630, A, 4817.0063, N, 00423.8260, W, 22.9, 105.8, 010920, 1.3, W, A*23$
$\$\ GPRMC, 125631, A, 4817.0062, N, 00423.8250, W, 22.9, 105.8, 010920, 1.3, W, A*20$
$\$\ GPRMC, 125632, A, 4817.0062, N, 00423.8243, W, 22.9, 105.8, 010920, 1.3, W, A*21$
Trames GPRMC (comportement anormal)
$\$\ GPRMC, 125633, V, 4817.0061, N, 00423.8238, W, 0, 0, 010920, 1.3, W, N*02$
$\$\ GPRMC, 125634, V, 4817.0061, N, 00423.8234, W, 0, 0, 010920, 1.3, W, N*09$
$\$\ GPRMC, 125635, V, 4817.0061, N, 00423.8231, W, 0, 0, 010920, 1.3, W, N*0D$

Ainsi, lors de l'analyse fine des trames NMEA, avant et après un réel Spoofing, il s'avère que le récepteur GPS perd soudainement la réception avec les satellites réels juste avant de recevoir la fausse position. Cela est dû au fait que le signal émis via le module SDR est plus puissant, ce qui peut être comparé à un brouillage court. Cette remarque va s'avérer importante lors de la mise en place d'un outil de simulation permettant de simuler de très nombreuses attaques de positionnement sur la norme NMEA (l'outil est décrit dans la section V.5 de ce chapitre). Le deuxième intérêt repose sur le fait qu'il est apparu que la plate-forme Naval Cyber-Range doit se doter d'un système

1. https ://wiki.analog.com/university/tools/pluto
2. https ://greatscottgadgets.com/hackrf/one/
3. https ://cddis.nasa.gov/Data_and_Derived_Products /GNSS/broadcast_ephemeris_data.html



(a)

(b)

FIGURE V.11 – Descriptions du matériel lors du leurrage/brouillage GPS (en haut). Résultat d'une expérience de leurrage GPS en conditions réelles (en bas).

TABLE V.2 – Exemples de trames NMEA normales et anormales de type "GPGGA".

Trames GPGGA (comportement normal)
$ $GPGGA, 125630, 4817.0063, N, 00423.8260, W, 1, 00, 2.8, 3.5, M, , M, , *47$
$ $GPGGA, 125631, 4817.0062, N, 00423.8250, W, 1, 00, 2.8, 3.5, M, , M, , *44$
$ $GPGGA, 125632, 4817.0062, N, 00423.8243, W, 1, 00, 2.8, 3.5, M, , M, , *45$
Trames GPGGA (comportement anormal)
$ $GPGGA, 125633, 4817.0061, N, 00423.8238, W, 0, 00, 0, 0, M, , M, , *46$
$ $GPGGA, 125634, 4817.0061, N, 00423.8234, W, 0, 00, 0, 0, M, , M, , *4D$
$ $GPGGA, 125635, 4817.0061, N, 00423.8231, W, 0, 00, 0, 0, M, , M, , *49$

TABLE V.3 – Exemples de trames NMEA normales et anormales de type "GPVTG".

Trames GPVTG (comportement normal)
$ $GPVTG, , T, 109.0, M, 22.9, N, 42.5, K, A * 0F$
$ $GPVTG, , T, 107.4, M, 22.9, N, 42.4, K, A * 04$
$ $GPVTG, , T, 105.8, M, 22.9, N, 42.3, K, A * 0D$
Trames GPVTG (comportement anormal)
$ $GPVTG, , T, 0, M, 0, N, 0, K, N * 2C$
$ $GPVTG, , T, 0, M, 0, N, 0, K, N * 2C$
$ $GPVTG, , T, 0, M, 0, N, 0, K, N * 2C$

d'acquisition des positions GPS et AIS suffisamment réaliste pour s'approcher au plus près des conditions de navigation d'un navire en intégrant un peu plus son environnement. Pour cela, un système d'acquisition autonome de signaux GNSS et AIS est développé dans la section suivante V.4.

Remarquons qu'il n'existe actuellement aucun dissecteur NIDS (open source) pour le protocole NMEA, ce qui complique l'écriture de règles de détection appropriées afin d'identifier des attaques sur la trame NMEA. Le fait d'avoir ce type d'expérimentation en conditions réelles permet de mieux identifier les caractéristiques (attributs) discriminantes pour la détection d'anomalies dans des trames NMEA en lien avec le positionnement du navire.

V.4 Conception d'une balise embarquée : HAPPINESS

L'une des préoccupations majeures de la plate-forme est la génération massive de données réalistes, exploitables, et en quantité suffisante. À long terme, l'ambition est d'offrir un environnement pertinent permettant de se concentrer sur des travaux et des études connexes pouvant exploiter sans ambiguïté les données provenant d'une telle plate-forme.

Le Naval Cyber-Range, de par sa conception initiale dédiée à la recherche et à la formation ainsi que pour des raisons évidentes de place, présente un nombre de limitations et de biais (voir section IV.2.1). Ainsi, des capteurs, des actionneurs et des contrôleurs sont simulés et permettent de reproduire dans la mesure du possible (plus ou moins fidèlement) un comportement réaliste des matériels susceptibles d'être présents dans un navire. Cependant, l'un des problèmes est la prise en compte de l'impact des données issues des systèmes de navigation et particulièrement GNSS et AIS. Pour rappel, la plate-forme est équipée d'un récepteur GPS Furuno GP-33 avec son antenne, d'un transpondeur AIS Furuno avec son antenne et d'un "Backbone" NMEA (BUS NMEA permettant de regrouper et multiplexer toutes les données NMEA en provenance des différents systèmes de navigation). Les données sont ensuite émises sur des systèmes de cartographie maritime (voir section IV.2.4.2). Lors de l'utilisation du simulateur de navigation, les données NMEA générées sont très génériques et trop pauvres en termes de détails (manque de pertinence). Même si elles sont cohérentes par rapport à la situation, elles restent néanmoins peu représentatives de ce qu'il en est vraiment dans des conditions réelles. Cet aspect représente l'une des principales limitations quant à l'utilisation du logiciel de navigation avec le reste des équipements de navigation présents dans la plate-forme. De façon plus explicite, les antennes de réception satellites des équipements de navigation ne sont que peu exploitées dans la mesure où le bateau, placé virtuellement au beau milieu d'un terrain de sport de l'École Navale dans un lieu fixe, ne bouge pas. Ce qui veut dire que si l'on se fie aux mesures reçues par ces systèmes, le bateau que l'on manœuvre est immobile, ce qui est évidement problématique pour la pertinence des scénarios mettant en œuvre ses instruments. Si l'on souhaite étudier l'impact d'une cyberattaque sur les systèmes de navigation via l'action d'un brouillage ou d'un leurrage GPS, l'évolution des données ne serait pas représentative. Alors que des conditions réelles avec un bateau ayant une situation et une cinématique particulières seraient plus pertinentes.

L'une des interrogations que peut susciter le développement d'un tel outil concerne l'intérêt de collecter ce genre de données alors que des données AIS sont aisément accessibles et existent déjà sur des sites spécialisés tels que Vesselfinder.com [4], marinetraffic.com [5] ou encore eurocontrol.int [6]. Il est vrai que les données contenues dans les trames AIS permettent déjà des informations comme la position (latitude, longitude), la vitesse, le cap ou encore le service d'identité mobile du navire. Le problème reste que ces données sont moins riches que celles présentes dans les données des trames GPS. Les trames GPS utilisées dans le standard NMEA 0183 sont plus complètes et donc plus pertinentes pour des analyses fines d'anomalies concernant les systèmes de navigation. Aussi pour répondre à cette problématique, nous proposons un système d'acquisition bas coût, non-intrusif et facile à déployer au sein d'un navire afin de fournir de véritables données GNSS et AIS : la balise embarquée HAPPINESS pour "**H**ollistic **APP**roach of **IN**tegrated **E**quipment for cyber**S**ecurity at

4. https ://www.vesselfinder.com/
5. https ://www.marinetraffic.com/
6. https ://www.eurocontrol.int/

Sea".

Le système doit être capable de collecter de vraies données depuis un navire en mouvement puis de les envoyer (en temps réel) sur le Naval Cyber-Range. Il s'agit de pouvoir rejouer la véritable cinématique du navire en injectant dans la plate-forme les données GNSS et AIS acquises et sauvegardées durant les campagnes de mesures. De par la présence de données réelles issues directement du terrain, les scénarios générés par cette plate-forme peuvent être considérés comme réalistes, permettant ainsi de réduire certains biais. Pour cela, le système embarqué d'acquisition de données doit respecter des règles et des contraintes :

1. **Système non-intrusif** : le système doit être totalement indépendant du navire et en aucun cas connecté aux systèmes cybernétiques internes du navire pour des raisons évidentes de sécurité afin de ne pas interagir ou même compromettre les systèmes à bord. Il ne doit pas impacter de quelque façon que ce soit l'intégrité des composantes fonctionnelles et opérationnelles du navire sur lequel est placé le système d'acquisition ;
2. **Acquisition automatique** : le système doit être totalement autonome avec la mise en place d'un système d'acquisition automatique limitant au maximum les interactions à partir du moment où il est alimenté. De plus ce système doit pouvoir envoyer des données GNSS et AIS en continu à la plate-forme ;
3. **Système autonome énergétiquement** : pour limiter l'impact de coupure de courant dans le cas, par exemple, de la mise à quai et l'arrêt des opérations du navire, le système doit être équipé d'une batterie avec une autonomie d'au moins une journée. Afin de limiter la consommation électrique (normalement, le système peut se brancher sur une prise de courant à bord du navire) et aussi pour des questions de sécurité, il doit être capable de démarrer ou de s'arrêter à des heures précises. Pour cela, une routine d'amorçage (*Bootloader*) doit être envisagée. De cette façon, si la coupure ne dure que la nuit ou encore que le bateau ne fonctionne que durant des périodes précises pour effectuer des trajets quotidiens (cas du « Transrade » à Brest), le système doit pouvoir redémarrer et envoyer les données en continu et cela sur plusieurs jours ou plusieurs semaines.
4. **Système interactif** : il est souhaitable d'interagir directement et facilement sur l'ensemble du système afin de pouvoir réaliser une maintenance rapide (mise à jour du programme, récupération des logs, etc.). Il est aussi souhaitable d'obtenir des remontées de métriques et de statistiques permettant d'analyser et de comprendre rapidement l'état du système ;
5. **Système télépilotable** : le système doit être conçu de manière à être pilotable à distance par ces propres canaux de communications sécurisés afin de réaliser des actions de maintenance (mise à jour de programme, récupération de logs, etc.) ;
6. **Système « ouvert » :** le système doit permettre de rajouter facilement d'autres systèmes de mesures (température, humidité, pression, gyroscope, etc.). L'ensemble de ces capteurs supplé-

mentaires permettent d'alimenter en continu la plate-forme du Naval Cyber-Range pour rejouer au plus près le comportement d'un véritable navire.

V.4.1 Description fonctionnelle

Une fois les différents besoins établis (section V.4), il ne reste plus qu'à élaborer l'architecture (hardware et software) capable de répondre aux caractéristiques souhaitées tout en prenant en compte les dimensions, les coûts, etc. des différents sous-systèmes. Le choix principal des composants et des éléments est basé sur leur capacité à s'interconnecter facilement entre eux pour se concentrer sur les objectifs attendus. La figure (V.12) montre l'architecture globale du système avec

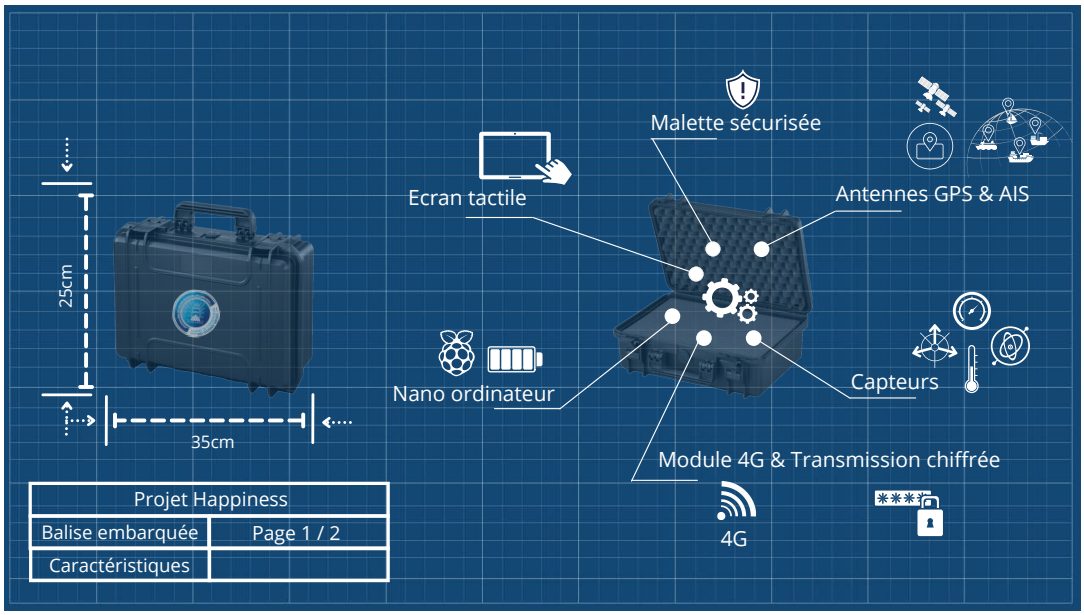


FIGURE V.12 – Caractéristiques de la balise embarquée HAPPINESS.

ses différents composants. La figure (V.13) représente l'architecture fonctionnelle du prototype en y détaillant les liaisons entre les différents sous-systèmes ainsi que la cartographie des flux (les plus importantes). La figure (V.14) montre quelques unes des IHM développées afin d'interagir facilement avec la balise "HAPPINESS". Ainsi, la liste complète des éléments est décrite comme suit :

— Un **mini ordinateur**. Les Mini-ordinateurs sont bien implantés sur le marché des cartes électroniques de développement. En termes de performances, alors que de nombreuses cartes seraient plus adaptées aux besoins opérationnels, le mini-ordinateur Raspberry Pi 4 reste facile à utiliser, possède une communauté très active et croissante et est d'un prix abordable (avant la crise COVID-19).

— Un **RTL-SDR (Software Defined Radio) dongle** qui peut être utilisé comme un scanner radio sur ordinateur pour recevoir des signaux radio en direct, idéal pour la réception de données

GPS et AIS. Il est branché sur l'un des ports USB du Raspberry Pi 4.

— Un **Récepteur GPS** avec son antenne déportée pour augmenter la précision, qui est connectée par USB au Raspberry Pi 4 ;

— Une **Antenne AIS** permettant la réception de la VHF maritime sur les fréquences AIS (161, 975 et 162, 025 MHz) connectée au dongle RTL-SDR ;

— Une **USB 4G stick** permettant de disposer d'une couverture côtière 4G suffisamment large dans les zones de navigation et d'un abonnement SIM pour envoyer des informations en temps réel, via Internet, sur la plate-forme. Cette transmission est réalisée de manière sécurisée, via l'utilisation d'un réseau privé virtuel, le tout chiffré de bout en bout avec le serveur de réception ;

— Un **écran tactile** permettant aux opérateurs de bord de visualiser rapidement l'état des systèmes et d'effectuer des opérations de maintenance au besoin (Fig. V.14) ;

— Des **capteurs traditionnels** : Accéléromètre *MMA8451*, Gyroscope *GYR03b* (représentant la centrale inertielle) et un capteur *BMEE680*, pour mesurer les valeurs d'humidité, de pression et de température (représentant les capteurs météorologiques). Tous ces capteurs ont une faible consommation d'énergie et sont connectés aux broches I2C (*Circuit Intégré* sur le GPIO (*Entrée/Sortie à usage général*) de la carte Raspberry Pi 4 ;

— Une **batterie externe de 20 000 MAh**, qui fournit l'énergie nécessaire à la carte Raspberry et à ses composants de manière continue. Elle permet au système d'avoir une autonomie d'environ 24 heures. La batterie externe est également branchée en permanence sur une prise de courant de 220V à bord du navire, ce qui garantit un niveau élevé de résilience de l'alimentation, qui est utile lors des opérations de maintenance quand le bateau est à quai et qu'il ne délivre plus de courant par exemple.

— Tous les éléments sont intégrés dans une **petite mallette hermétique, sous clé et électriquement isolée**.

Si l'intérêt de collecter des données issues de systèmes GNSS et AIS a été motivé en amont de cette section, il en est tout autrement pour les données de capteurs traditionnels (accéléromètre, gyroscope, etc.). Dans notre cas, l'obtention des données issues d'une centrale inertielle peut permettre d'ajouter un degré de précision supplémentaire aux données reçues afin d'établir la cinématique du bateau dans lequel le système embarqué HAPPINESS se trouve. Cela permet d'ajouter des métriques de détection d'anomalies. Si par exemple le système est victime de leurrage GPS changeant drastiquement sa position, la centrale inertielle, qui ne changera pas aussi brutalement, pourrait éventuellement servir de référence. Quant aux données météorologiques, elles peuvent servir à alimenter les autres systèmes industriels présents dans la plate-forme Naval Cyber-Range avec des variations réalistes, évitant de devoir simuler de tels capteurs et donc de limiter au possible les effets des biais de simulation.

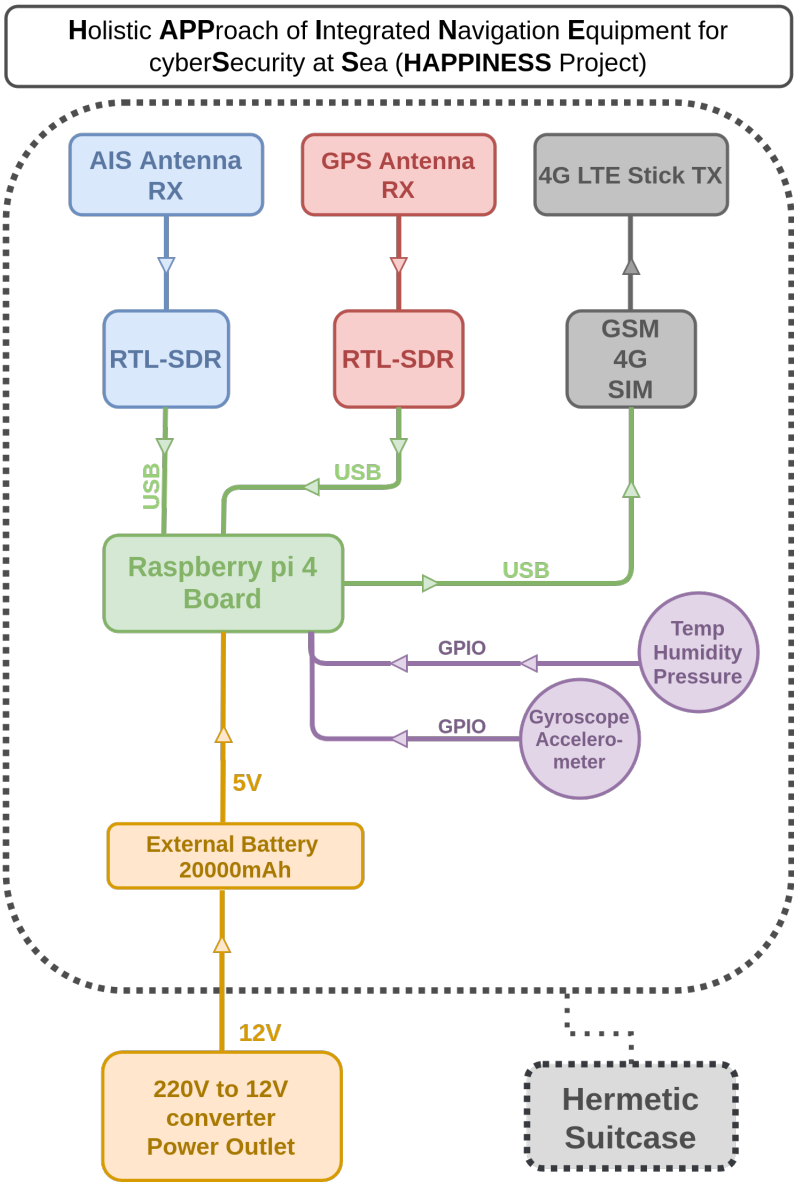


FIGURE V.13 – Architecture fonctionnelle de la balise embarquée HAPPINESS.

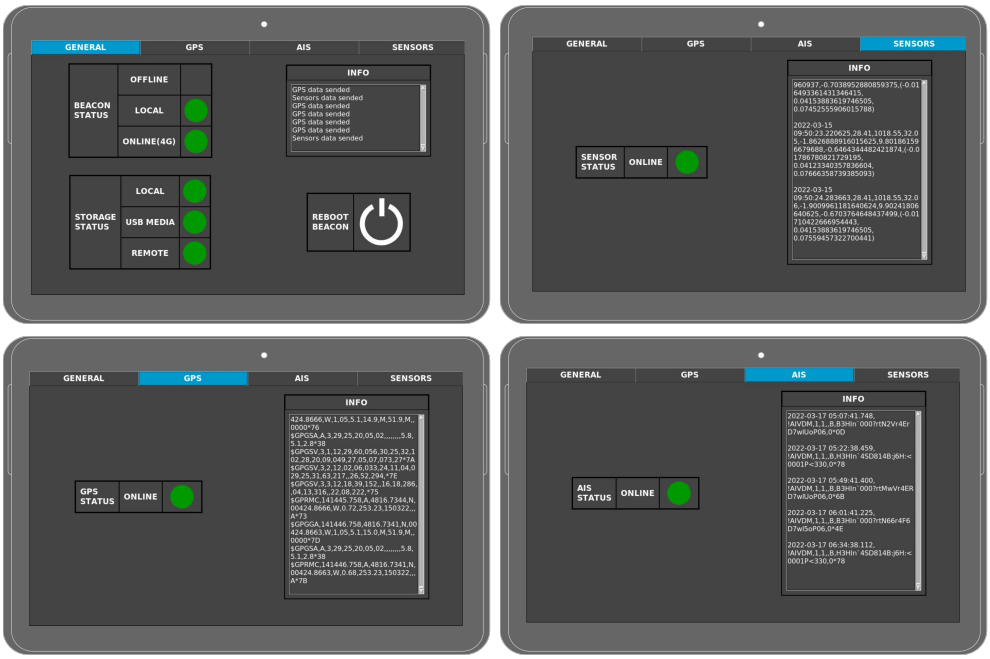


FIGURE V.14 – Exemples d'IHM développées et dédiées aux opérations à bord pour la balise embarquée HAPPINESS.

V.4.2 Méthodologie de collecte des données

Une fois l'ensemble des éléments du système définis, une étude approfondie des processus de collecte et de visualisation a été nécessaire au regard du volume de données susceptible d'être collecté. Les données provenant des différents capteurs et récepteurs sont d'abord enregistrées sur le système embarqué via un stockage local, puis envoyées à terre vers un serveur distant par connexion 4G sécurisée. Le principe étant de pouvoir recevoir, collecter et interpréter les données en temps réel, mais aussi de pouvoir les sauvegarder dans une base de données. Cette base de données peut servir à rejouer des scénarios en se basant sur les données reçues dans lesquelles auront été injectées des anomalies liées à l'exploitation de cyberattaques (section V.5). Le principe de fonctionnement de la balise HAPPINESS et celui de la collecte des données sont illustrés respectivement par la figure (V.15)

Afin de valider le concept et de collecter des données provenant d'un véritable navire, la compagnie maritime "*Morlenn Express*" a été sollicitée afin d'installer le système sur un de leurs bateaux. Les bateaux de cette compagnie, spécialisée dans le transport local de passagers, peuvent accueillir en moyenne 200 à 250 personnes pour des déplacements entre différents ports de Bretagne, notamment entre les villes de Brest et de Lanvéoc, sur la côte ouest-française. Ces bateaux (Transrade), d'une longueur de 35 mètres et d'une largeur de 7 mètres, effectuent des manœuvres simples et régulières tout au long de la journée, réalisant 4 allers-retours par jour avec une durée moyenne de 1 heure

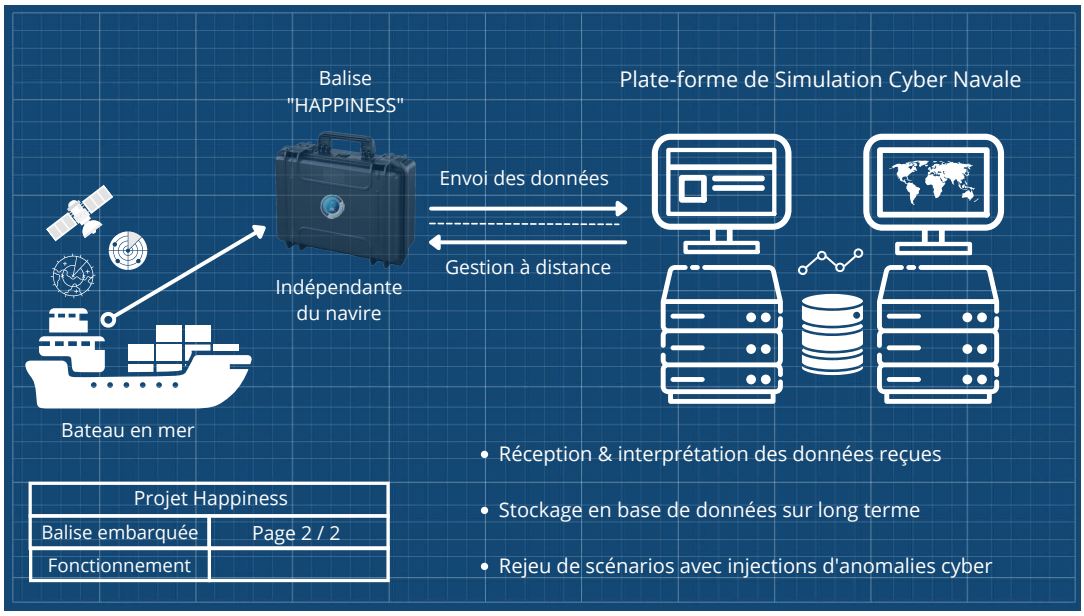


FIGURE V.15 – Principe de fonctionnement de la balise embarquée HAPPINESS.

par trajet.

Lors des campagnes de mesures, il était question d'installer la valise à bord du navire pour qu'il soit alimenté électriquement (prise 220V classique) et qu'il soit facilement accessible sans encombrer l'équipage. Une fois le système en place, la connexion 4G LTE permet d'envoyer les données au Naval Cyber-Range pour enrichir les analyses ultérieures. Les données, qu'elles proviennent de capteurs, du GPS ou de l'AIS, sont stockées au sein du système embarqué au format "*.csv*", étiquetées, horodatées et exploitables par la suite.

À terre, les données sont triées, analysées et nettoyées en temps réel (c'est-à-dire que les données ont été amputées de tout décodage raté ou de format anormal pour les rendre intelligibles) avant d'être stockées sur le serveur distant de la plate-forme. La réception des données de navigation est conforme à la norme NMEA-0183 (Tab. V.4). Lors de la campagne, il est possible d'envoyer les données à un ECS (système de cartes électroniques) open source (OpenCPN) afin de visualiser l'évolution en temps réel du navire ainsi que son environnement GNSS et AIS (Fig. V.16). Grâce à ce système, la plate-forme gagne alors en réalisme en considérant que les différentes boucles du navire interagissent en fonction des données perçues.

V.4.3 Déploiement d'HAPPINESS sur des navires

Une fois les phases de conception et de test finalisées, l'opportunité de pouvoir embarquer le prototype sur des bateaux exerçant des activités différentes s'est présentée. Tout d'abord, pendant toute la phase d'expérimentation, le système d'acquisition a été placé pendant plusieurs mois sur différents navires de la société *Morlenn Express* : *TIBIDY*, *LOUARN*, *DERVENN* et *TERENEZ*.

TABLE V.4 – Exemples de données collectées par le système embarqué HAPPINESS (enregistrées le 7 Mars 2022).

Exemples de données reçues
Données provenant de l'antenne AIS (format NMEA-0183)
21 :32 :39, !AIVDM,1,1,,B,13I5h2gP00OcJwHKco>Gngwp0pG5,0*6D
21 :32 :57, !AIVDM,1,1,,B,13I3 :M ?P00OcJsNKckOa@ ?wj06R0,0*75
21 :32 :58, !AIVDM,1,1,,B,13I5h2gP00OcJwPKco>upgwp0l0R,0*55
21 :33 :19, !AIVDM,1,1,,B,13I5h2gP00OcK02Kco@BNgwp0W3h,0*04
21 :33 :39, !AIVDM,1,1,,B,13I5h2gP00OcK0@Kco@=Jgwp0l0R,0*0F
Données provenant de l'antenne GPS (format NMEA-0183)
21 :32 :50,$GPGGA,203251.440,4823.2864,N,00430.3154,W,1,04,4.9,50.3,M,52.1,M,,0000*71
21 :32 :51,$GPGSA,A,3,27,10,32,22,,,,,,,,,5.7,4.9,2.9*33
21 :32 :51,$GPRMC,203251.440,A,4823.2864,N,00430.3154,W,0.82,277.01,070322,,,A*77
21 :32 :51,$GPGGA,203252.440,4823.2863,N,00430.3154,W,1,04,4.9,50.3,M,52.1,M,,0000*75
21 :32 :52,$GPGSA,A,3,27,10,32,22,,,,,,,,,5.7,4.9,2.9*33
Données capteurs (Température, Pression, Humidité, Accélération, Gyration)
21 :32 :50,8.37,1006.62,39.675,-1.7908,9.0883,3.7110,(-0.0155, 0.0259, 0.1194)
21 :32 :51,8.37,1006.61,39.681,-1.790,9.131,3.715,(-0.0128, 0.0293, 0.1183)
21 :32 :52,8.37,1006.61,39.686,-1.819,9.121,3.797,(-0.0171, 0.0293, 0.1191)
21 :32 :54,8.37,1006.6,39.698,-1.786,9.126,3.754,(-0.01324, 0.0305, 0.1207)
21 :32 :55,8.37,1006.6,39.709,-1.795,9.093,3.797,(-0.0160, 0.0290, 0.1212)

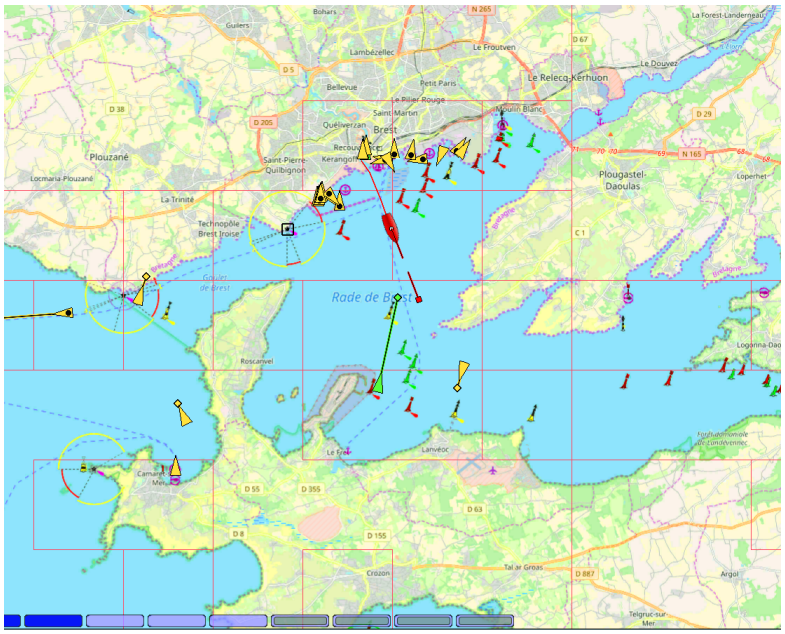


FIGURE V.16 – Exemple de visualisation de message AIS (en vert et jaune) ainsi que la trajectoire du bateau (en rouge) produite à partir de la balise embarquée HAPPINESS.

Il s'agit d'une compagnie professionnelle de transport de passagers effectuant plusieurs navettes par jour dans la Rade de Brest. D'autant plus qu'environ 4 aller-retours par jour sont effectués par chaque navire de transport. Ces navires sont presque tous de taille identique (jusqu'à 35m de long pour 7m de large) et pouvant transporter environ 250 passagers par voyage. Ils effectuent des traversées presque tous les jours de l'année et chacune dure approximativement $1h30$ aller-retour, assurant un réel apport en termes de données générées. Le prototype serait également accessible pour toute opération de maintenance (Fig. V.17).

FIGURE V.17 – Photo de l'extérieur du *TERENEZ*, navire de transport de passagers de la compagnie *Morlenn Express* (à gauche). Photo de l'intérieur du navire avec la balise embarquée HAPPINESS (à droite).

Dans un second temps (mars 2022), après quelques mois d'expérimentation et de premiers retours d'expérience, nous avons eu l'opportunité d'embarquer une deuxième version du prototype sur le *CELADON*, un navire de tests et d'essais technologiques en haute mer appartenant à la plate-forme associative *Sea Test Base*[7]. C'est un navire non disponible sur le marché, fabriqué sur mesure et dédié aux expérimentations comme celle-ci. Outre l'instrumentation de bord classique (système de navigation, pilote automatique, AIS, GNSS, compas, etc.), ce navire dispose également d'instrumentation spécifique pour les essais en mer. Il peut par exemple intervenir jusqu'à 300m de profondeur avec un robot sous-marin pour réaliser des cartes sous-marines à haute résolution avec un sondeur multifaisceaux. Le système informatique du bord est en permanence connecté à Internet en haut débit et offre des services de retransmission vidéo, de téléassistance et de téléopérations. De par tous ces aspects, ce type de navire représentait une opportunité tout aussi intéressant pour exploiter notre système (Fig. V.18).

7. inaugurée en 2011, elle met à disposition de ses adhérents différents types de moyens à terre (notamment sur le site de l'École Navale à Lanvéoc) et en mer. Cette association propose divers services offrant un espace de travail dédié en mettant par exemple à disposition de l'instrumentation marine et sous-marine telle que des drones sous-marins de type AUV ou des robots sous-marins de type ROV

FIGURE V.18 – Photo de l'extérieur du *CELADON*, navire d'essais technologiques en haute mer (à gauche). Photo de l'intérieur du navire avec la balise embarquée HAPPINESS (à droite).

V.4.4 Traitement et analyse des données HAPPINESS

Ainsi, depuis le mois de mars 2021, un volume important de données a été collecté, quasiment quotidiennement, sous la forme de traces GNSS, de trames NMEA et de données de capteurs (Figs. V.19 et V.20). Pour avoir une idée plus précise du volume de données, ci-dessous le nombre de trames pouvant être collectées en une heure via les différents systèmes d'HAPPINESS :

— environ **5750** trames NMEA-0183 GPS par heure,

— environ **2200** trames NMEA-0183 AIS par heure,

— environ **3250** trames de capteurs par heure.

La différence du nombre de trames s'explique simplement par des fréquences d'acquisition différentes entre les capteurs (GPS : environ 4 trames par seconde ; AIS : très fluctuant, dépend énormément de la densité du trafic maritime ; cela peut aller de 10 trames par seconde à 1 trame tous les 3 à 5 secondes ; capteurs : environ 1 trame (pression, température, humidité, gyroscope, etc) tous les 500 ms). Pour rendre exploitables les données, l'horodatage (synchronisation des données entre elles) s'est avéré primordial.

Pour une moyenne de 10 heures d'acquisition de données par jour sur 5 jours par semaine sur une période de 2 mois (les moments où le bateau navigue), une base de données de plus de **19,738,300** données brutes totalisant environ **10 Gb** est obtenue. Une fois ces données nettoyées (comme précisé dans la sous-section V.4.2) et analysées, il a été identifié environ une vingtaine d'attributs (*features*) simplement en exploitant directement les données AIS ou GPS comme : *"Latitude", "Longitude", "Reception Quality", "Speed Over Ground", "Track Angle, "GPS Quality", "Number Of Satellites In View", "Orthometric Height", "Horizontal Dilution Of Precision (HDOP)", "Ver-*

tical Dilution Of Precision (VDOP)", "Positions Dilution Of Precision (PDOP)", "Satellite ID", "Satellite Elevation", "Satellite Azimuth", "SNR", "Maritime Mobile Service Identity (MMSI)", "AIS Status", "Course"," Heading", "Raim", "Radio", etc. Ces différents attributs sont suffisamment riches en informations que l'on peut facilement corréler et comparer. Par exemple toutes les *features* se rapportant à des informations satellitaires sont intéressantes à observer puisque lorsqu'une fausse constellation satellite sera générée par un système de leurrage, par exemple les champs "HDOP", "VDOP", "Satellite ID", "Satellite Elevation", "Satellite Azimuth", "SNR", changeront de paradigme, car les faux satellites simulés n'auront pas la même précision que les vrais. Ce qui peut affecter les autres types de champs comme "Number Of Satellites In View","GPS Quality" et "Orthometric Height" qui seront brutalement différents pendant la période d'attaque.

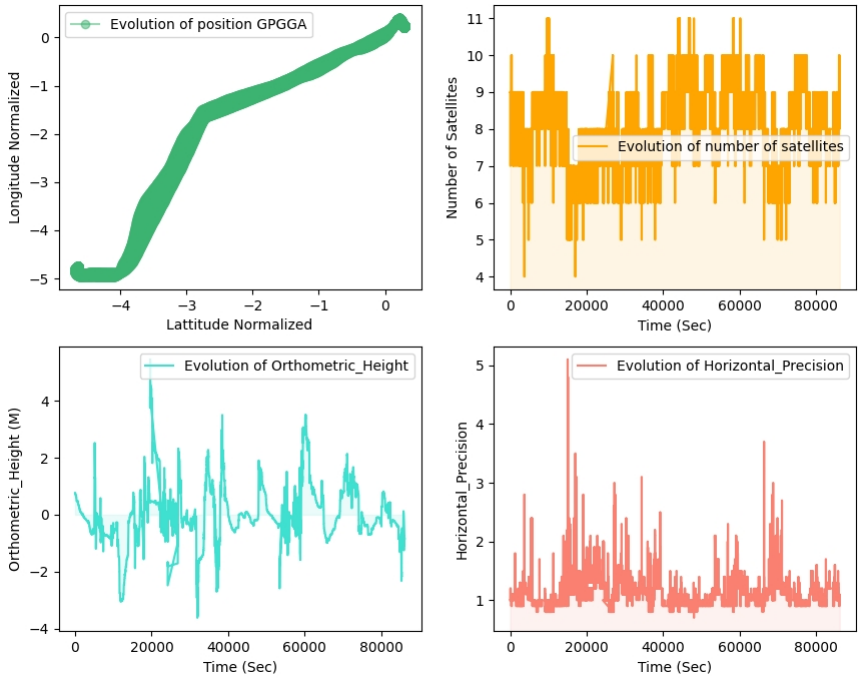


FIGURE V.19 – Évolution des données GPGGA (sur 5 jours).

De plus, pour améliorer l'analyse de la situation, plusieurs tableaux de bord de supervision (via OpenCPN et Grafana [8]) intégrés à la plate-forme du Naval Cyber-Range ont été développés de sorte à pouvoir suivre en temps réel l'évolution des données issues des balises embarquées "HAPPINESS" (Fig. V.21, V.22, V.23).

Ces données permettent par la suite d'élaborer un modèle représentant le comportement normal du navire en prenant en compte l'ensemble de ses manœuvres (sorties des ports, accostages, accélérations, etc.). Ces attributs ou caractéristiques sont ceux qui sont susceptibles de changer

8. Grafana est un outil open source de monitoring informatique orienté data visualisation permettant de manipuler d'importants volumes de données pouvant provenir de plusieurs sources. Il est conçu pour générer des tableaux de bord sur la base de métriques et données temporelles.

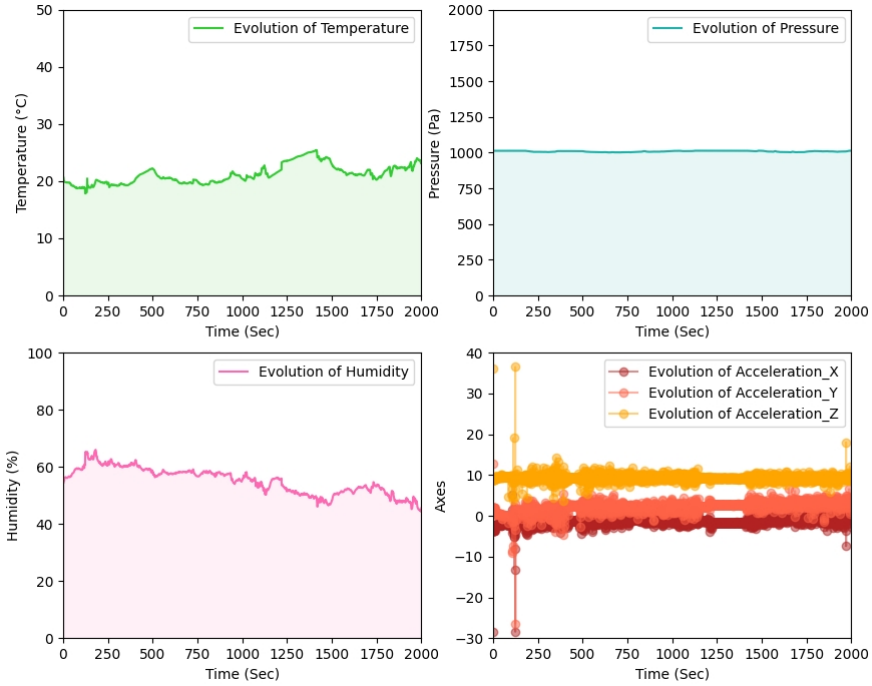


FIGURE V.20 – Évolution des données des trames des capteurs.

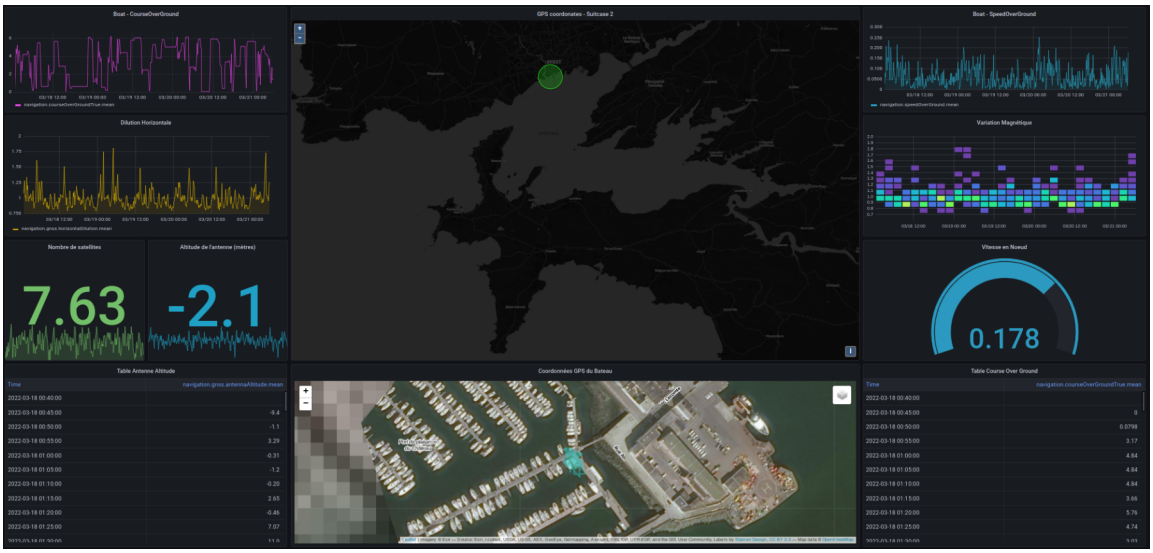


FIGURE V.21 – Dashboard représentant l'évolution des données GNSS du prototype HAPPINESS embarqué sur le *CELADON*.

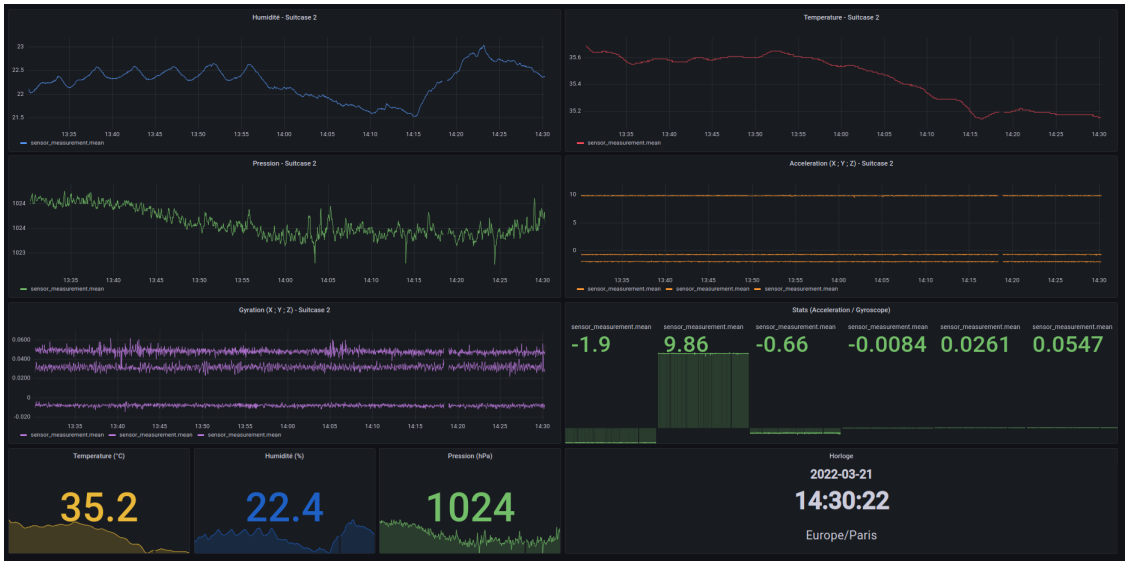


FIGURE V.22 – Dashboard représentant l'évolution des données de capteurs du prototype HAPPINESS embarqué sur le *CELADON*.

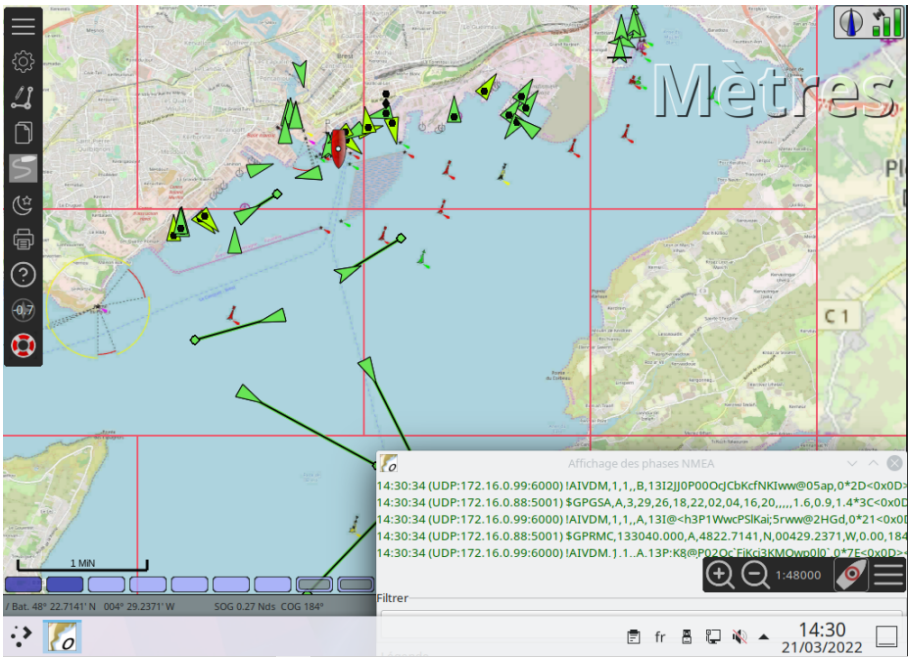


FIGURE V.23 – Dashboard représentant l'évolution des données AIS du prototype HAPPINESS embarqué sur le *CELADON*

lorsque les systèmes GNSS sont victimes de cyberattaques (leurrage, brouillage). Par la suite, une analyse à long terme de l'évolution de ces caractéristiques permet, potentiellement, de déterminer les comportements normaux du navire et ainsi aider à détecter les valeurs aberrantes (*outliers*) synonymes d'une possible attaque cyber.

V.5 Développement de l'outil NAGE

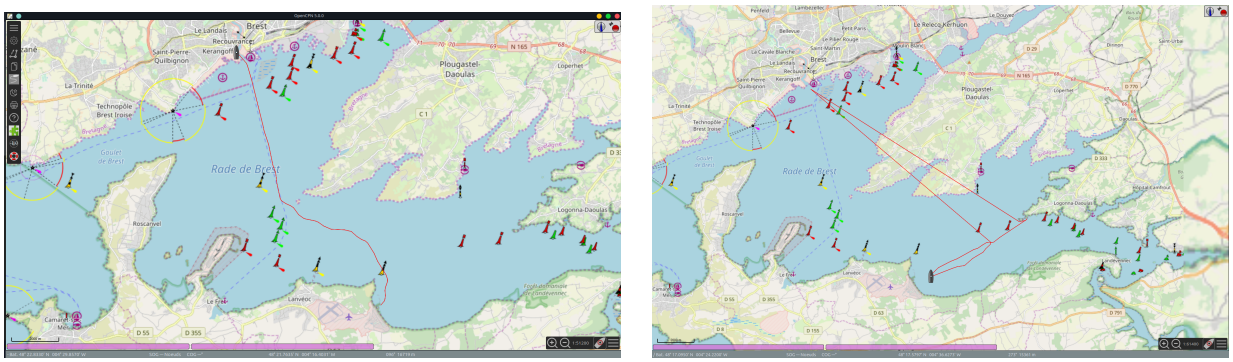
Ainsi, grâce au système embarqué d'acquisition de données HAPPINESS, permettant de collecter des données réalistes de navigation issues de véritables navires en conditions réelles, il est possible d'améliorer la capacité de la plate-forme du Naval Cyber-Range à générer des scénarios réalistes de cyberattaques notamment sur les données GNSS et AIS. Il est aisé d'injecter des anomalies spécifiques sur les systèmes de navigation sans pour autant impacter de quelque manière que ce soit les vrais systèmes desquels sont issus les données. Il est en effet nécessaire de pouvoir falsifier intelligemment les données NMEA acquises précédemment avec l'aide de la balise HAPPINESS.

Pour cela, il s'agit d'exploiter les vulnérabilités identifiées dans la section IV.4 sur les trames NMEA 0183 en y développant un logiciel de simulation spécifique d'attaques : NAGE pour "**N**MEA **A**ttack **G**eneration **E**ngine" installée sur la plate-forme du Naval Cyber-Range. Pour mémoire, la réalisation d'attaques GPS en conditions réelles nécessite des mesures de sécurité très élevées pour s'assurer que l'attaque n'a aucun impact sur les navires ou les aéronefs à proximité. Il n'est donc pas envisageable d'utiliser une telle approche pour générer un volume important de données d'attaques afin de constituer une base pertinente en vue de faire des analyses et des traitements complémentaires dans le cadre d'étude cyber (détection d'intrusion, modélisation de comportements anormaux, résilience, etc.).

Ainsi, nous avons pu reproduire différents scénarios d'attaques GPS sans avoir d'impact sur les navires environnants et l'environnement RF. NAGE permet de prendre les données d'entrée d'un simulateur de navigation générant des trames NMEA réalistes, mais aussi les données NMEA d'un vrai récepteur GPS (Fig. V.24(a)). Une fois les données obtenues, il est possible de transmettre les données réelles à travers NAGE afin qu'il puisse générer des attaques sur cette même base (Fig. V.24(b)).

V.5.1 Description fonctionnelle

Sur la base des attaques réelles générées (section IV.4), l'outil NAGE a été développé afin de pouvoir simuler des falsifications de trames NMEA (dans notre cas 0183) synonymes d'attaques GPS à partir de données réelles. Il s'agit d'imiter au mieux le comportement des véritables systèmes d'attaques GNSS et AIS étudiés précédemment (Fig. V.25). Pour cela, après avoir identifié avec des



(a) (b)

FIGURE V.24 – Comportement normal d'un navire réel obtenu à partir de la balise HAPPINESS (à gauche). Suivi d'un navire victime de leurrage GPS via NAGE à partir de données initiales HAPPINESS (à droite).

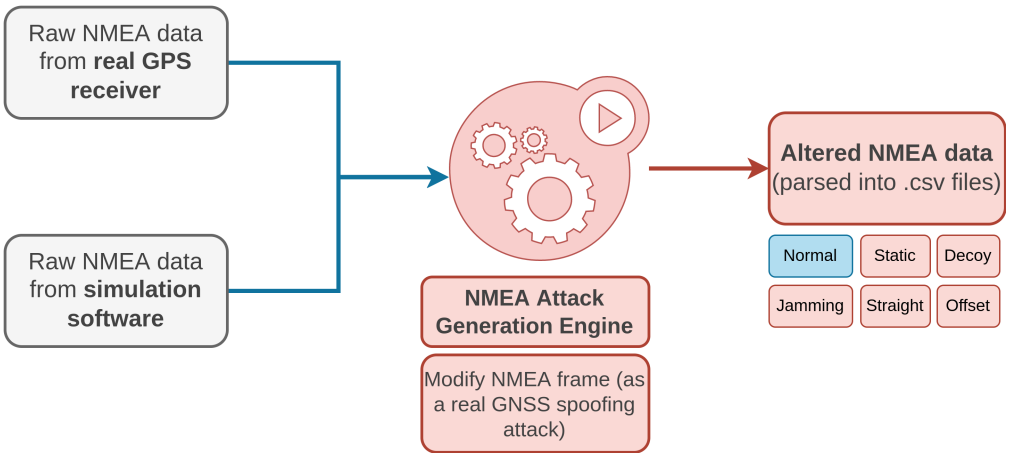


FIGURE V.25 – Principe de fonctionnement de NAGE pour générer des trames NMEA corrompues lors de cyberattaques.

attaques RF réelles les caractéristiques NMEA changeant significativement lorsqu'une attaque de Spoofing (ou Jamming) est perpétrée (section IV.4), il a été possible de recréer ces variations en simulation (Fig. V.26). Par exemple, si on observe l'évolution de chaque champ de données NMEA, en particulier les trames GPGGA et GPRMC, il est possible de voir quels sont ceux qui peuvent être impactés par une attaque de leurrage GPS. À noter que chaque champ ne varie pas de la même manière selon le type d'attaque réalisée et il est apparu que certains champs sont plus pertinents que d'autres pour permettre de mesurer l'impact d'une attaque sur l'ensemble du système (cela sera abordé dans le prochain chapitre VI). Les figures (V.27) et (V.28) montrent l'évolution de la trame NMEA de GPGGA et GPRMC pour deux scénarios.

Incidemment, à partir de cette analyse, il est parfaitement possible de générer une multitude de scénarios d'attaques. Dans ce manuscrit, il ne s'agit pas de tous les décrire, mais plutôt d'en retenir

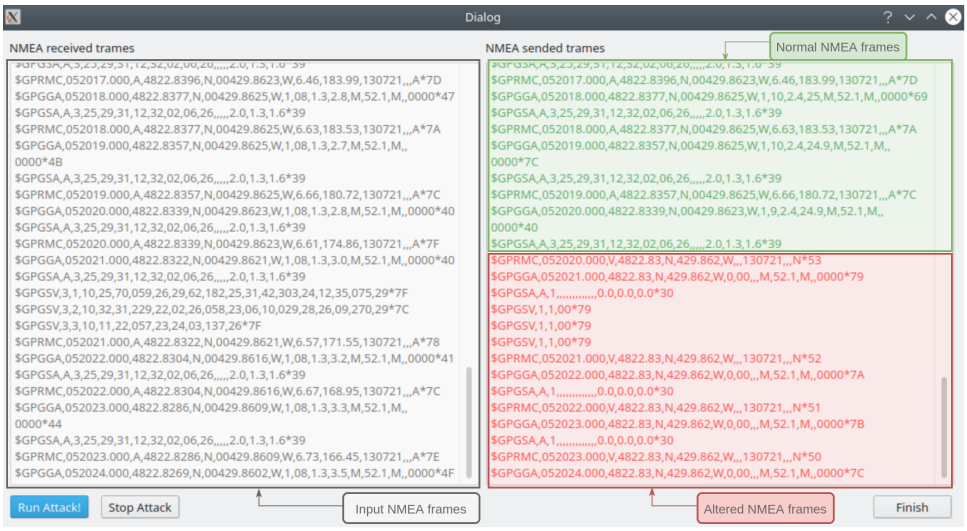


FIGURE V.26 – Exemple de visualisation de données NMEA falsifiées générées par NAGE.

quelques-uns qui sont courants (voir section V.5.2 pour une description plus fine de 4 scénarios d'attaques). La figure (V.29) montre quelques interfaces développées pour faciliter la génération des scénarios d'attaques. Tous les scénarios d'attaque décrits ci-dessous peuvent être réalisés facilement par NAGE grâce à des préconfigurations spécifiques présentes sur la plate-forme Naval Cyber-Range. NAGE a la particularité de s'intégrer facilement et de manière transparente à la plate-forme via l'utilisation de sockets UDP spécifique aussi bien en entrée qu'en sortie. En plus de limiter l'impact de ces expériences, le principe de cet outil est de pouvoir effectuer autant de simulations que nécessaire sans les contraintes expérimentales des expériences réelles qui nécessitent parfois beaucoup de processus d'installation et de nombreuses précautions.

V.5.2 Scénarios d'attaques générés par NAGE

Par la suite, il a été possible de générer cinq scénarios différents via NAGE :

1. Scénario normal (la référence) ;
2. Scénario de brouillage (*GNSS Jamming*) ;
3. Scénario de falsification statique (*GNSS Spoofing Static*) ;
4. Scénario de falsification dynamique en ligne droite (*GNSS Spoofing Dynamic - Straight Line*) ;
5. Scénario de falsification dynamique par décalage (*GNSS Spoofing Dynamic - Offset Trajectory*).

***Scénario normal* (Fig. V.30)**

Le navire navigue normalement, les systèmes sont pleinement opérationnels et fonctionnels et les systèmes cybernétiques ne présentent aucune anomalie. La réception GPS est bonne, le bateau peut

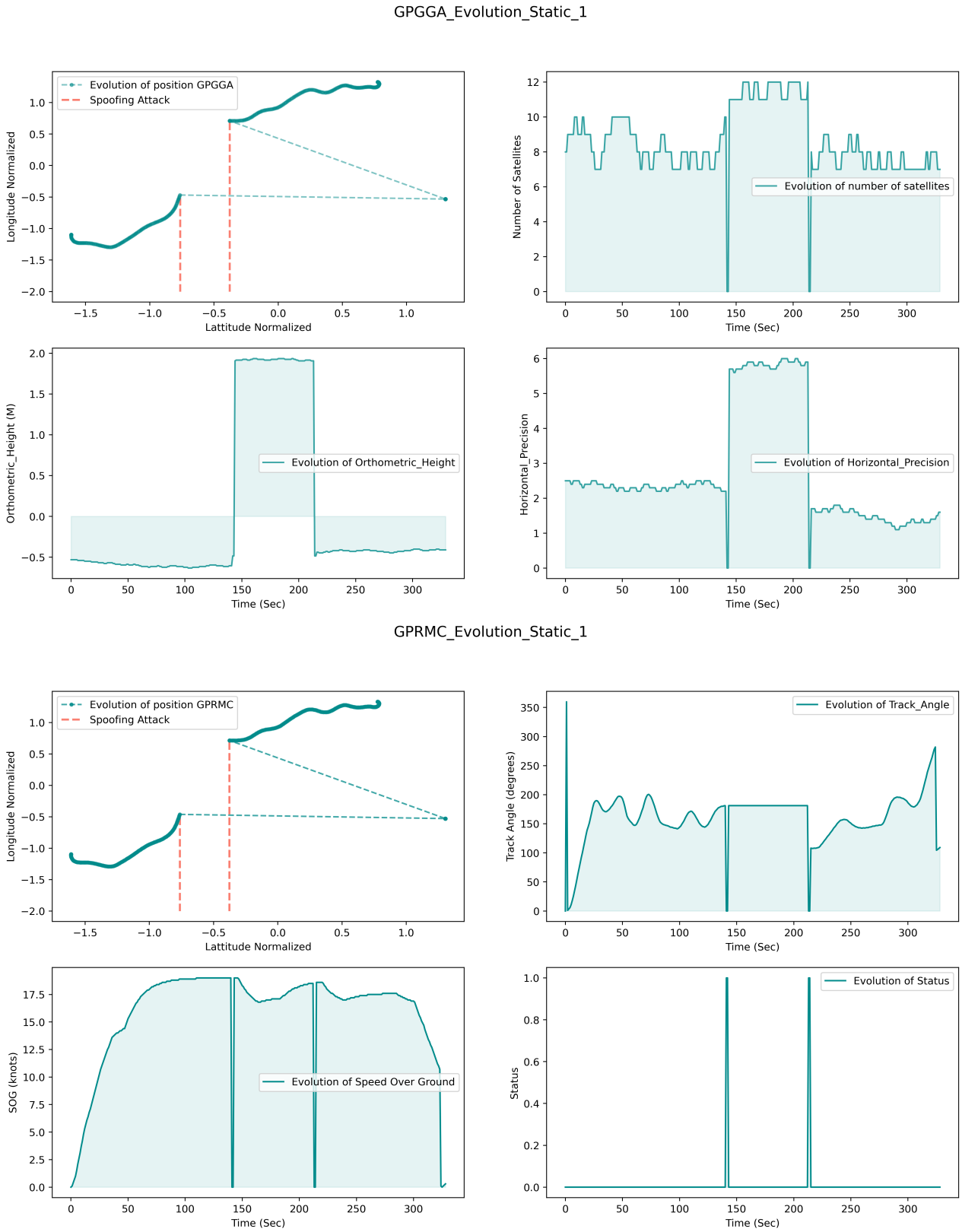


FIGURE V.27 – Évolution des champs GPGGA et GPRMC pendant une attaque par leurrage GPS dit "Statique" via NAGE.

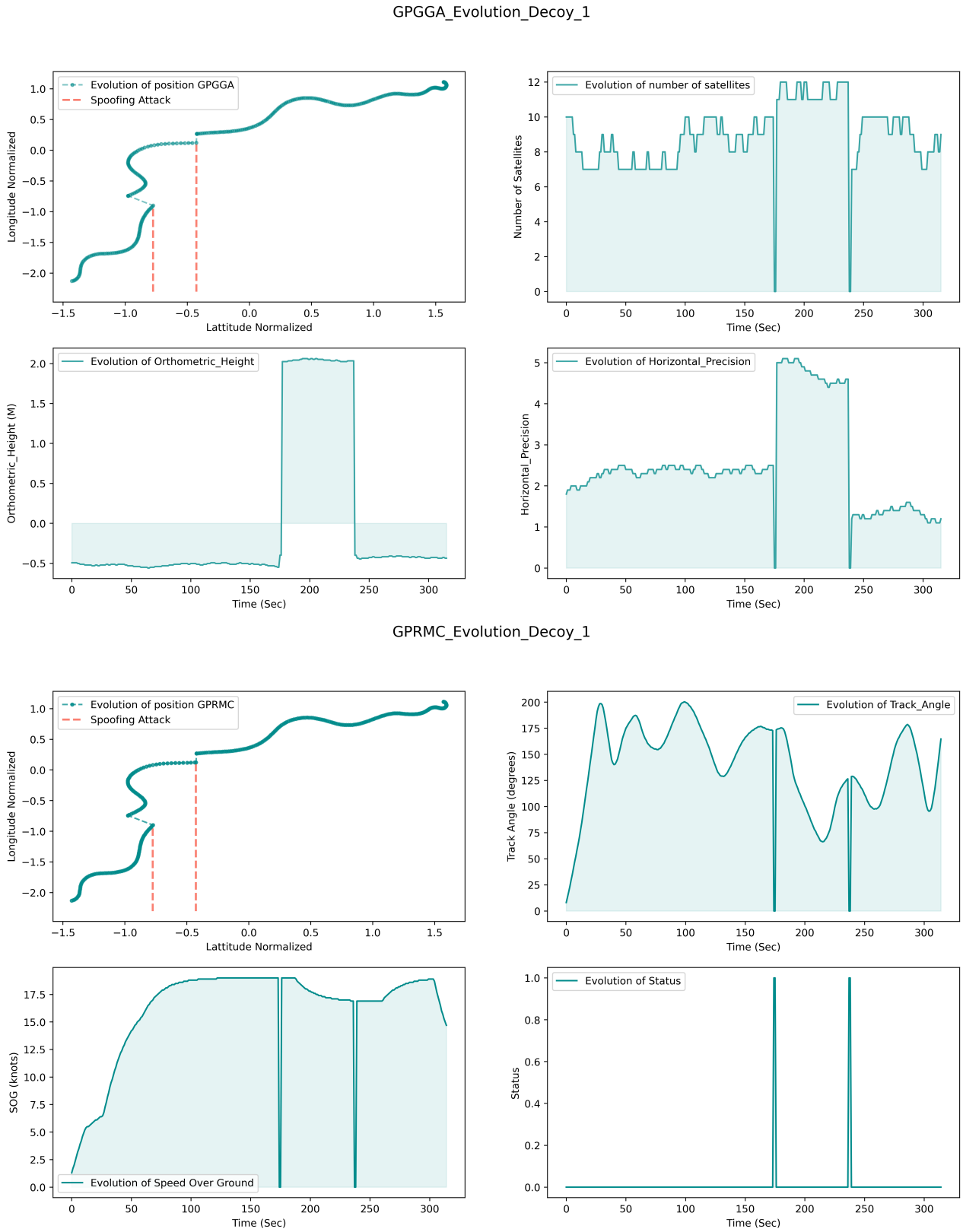


FIGURE V.28 – Évolution des champs GPGGA et GPRMC pendant une attaque par leurrage GPS dit "Décalé" via NAGE.

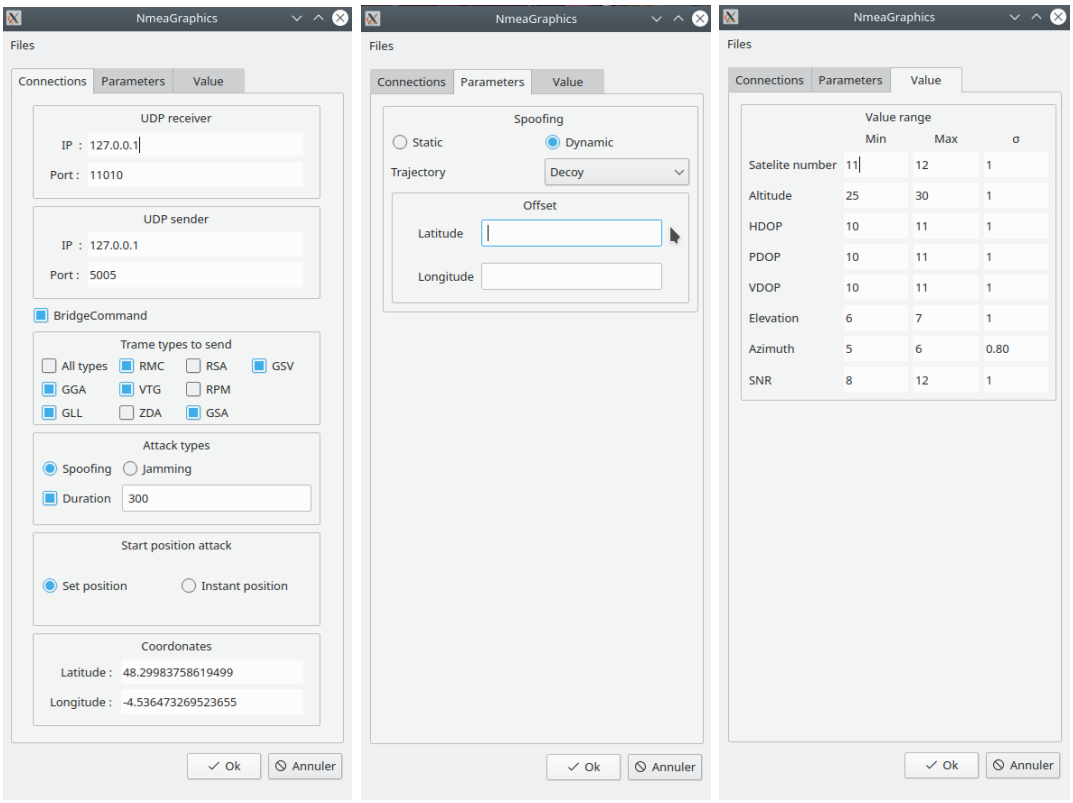


FIGURE V.29 – Exemple d'interface IHM de NAGE pour la génération des scénarios d'attaques.

naviguer en ayant la bonne connaissance de sa position et de son environnement. Le signal NMEA peut être une véritable version représentative d'une vraie trajectoire d'un navire (ou non dans un cas simulé).

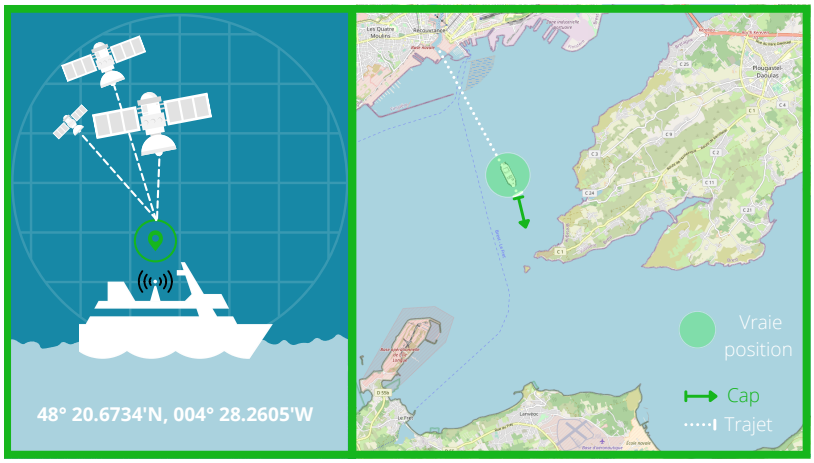


FIGURE V.30 – Comportement normal du navire.

***Scénario de brouillage* (Fig. V.31)**

Ce scénario est le plus basique, car il modifie artificiellement les trames NMEA des phrases GPGGA, GPRMC afin de passer les champs à zéro. Ce scénario (*GNSS Jamming*) correspond à une perte de réception classique qui peut également se produire lorsque la qualité de réception des satellites est faible, déclenchant généralement une alerte d'affichage sur le GPS (de type "*Signal Loss*").

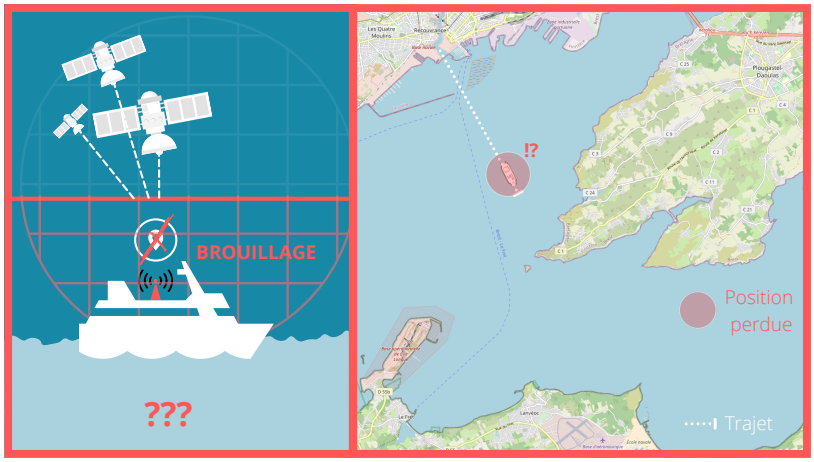


FIGURE V.31 – Comportement anormal du navire : attaque par brouillage via NAGE.

***Scénario de falsification statique* (Fig. V.32)**

Ce scénario d'attaque met en pratique une attaque relativement classique et basique de falsification GNSS qui consiste à faire croire au récepteur GPS qu'il se trouve à une position différente de sa réelle position (*GNSS Spoofing*). Pendant toute la durée de l'attaque, le récepteur GPS considère qu'il est à une position unique (c'est une attaque de type statique).

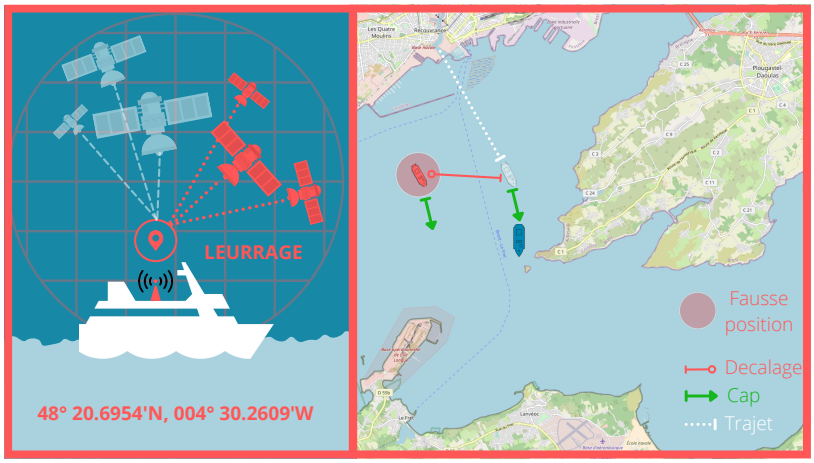


FIGURE V.32 – Comportement anormal du navire : attaque par falsification statique via NAGE.

***Scénario de falsification dynamique en ligne droite* (Fig. V.33)**

Dans le cas de ce scénario de falsification, une fois l'attaque lancée, les trames NMEA modifiées

indiquent au navire qu'il continue en ligne droite alors que l'angle de barre change. Cette attaque peut être similaire à un scénario d'attaque statique, mais dont la position est décalée dans le temps de manière à simuler une trajectoire rectiligne. Ce type de scénario d'attaque peut être très dangereux s'il est exploité alors que le navire réalise des manœuvres de giration (à proximité d'autres navires ou encore de récifs, accostages, etc.).

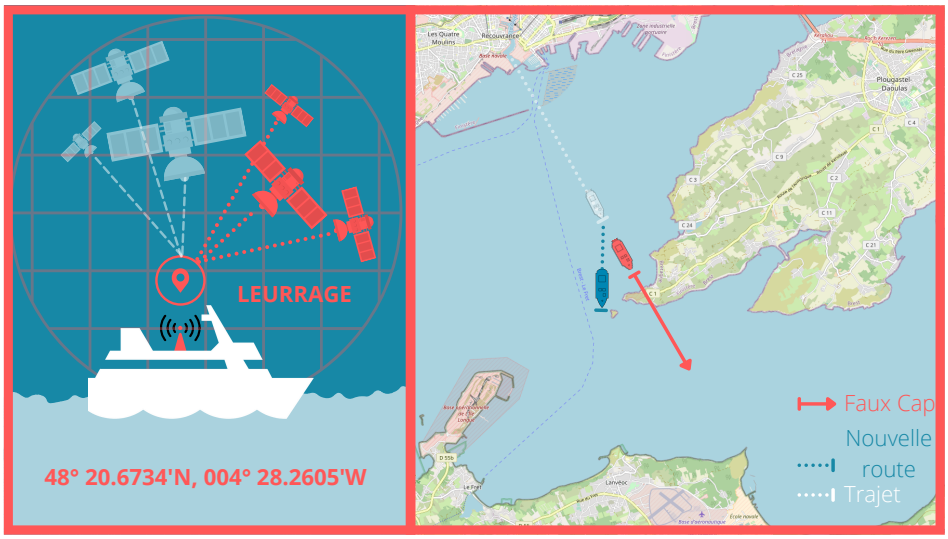


FIGURE V.33 – Comportement anormal du navire : attaque par falsification dynamique en ligne droite via "NAGE".

Scénario de falsification dynamique par décalage **(Fig. V.34)**
Ce dernier scénario implique une translation des données de latitude et de longitude du navire. L'angle de barre n'est pas modifié par rapport à la réalité. Cette attaque peut être similaire à un scénario d'attaque dynamique, mais dont la position subit une translation tout en dépendant de la vraie route du navire.

Grâce à l'outil NAGE, il est possible d'élaborer plusieurs simulations de scénarios d'attaques à partir des données collectées. Il est possible de générer des jeux de données réalistes de plusieurs heures de transferts NMEA, mélangeant des comportements normaux et anormaux avec des attaques de Spoofing et/ou de Jamming. Tous ces jeux de données générés permettent d'élaborer des modèles de référence de comportement normal et de comportement anormal exploité dans le prochain chapitre VI.

V.6 Conclusion

Dans ce chapitre nous avons décrit comment améliorer les données et les scénarios générés par la plate-forme de simulation. Différentes expérimentations ont été menées pour mieux comprendre

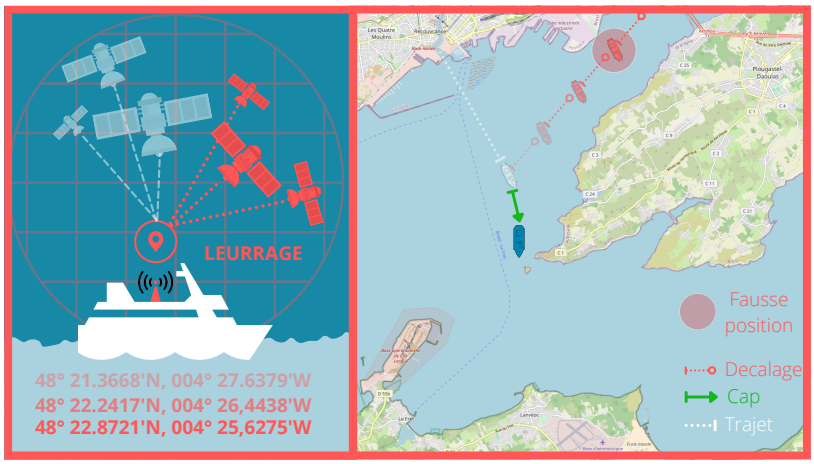


FIGURE V.34 – Comportement anormal du navire : attaque par falsification dynamique par décalage via NAGE.

le fonctionnement de vraies cyberattaques sur des systèmes de navigation. Nous avons développé des outils autour de cette plate-forme, AEGIS et NAGE, dédiés respectivement à la génération d'attaques dans les données industrielles et sur les données de navigation et facilitant ainsi la génération de scénarios. L'élaboration de ces scénarios s'est basée sur des incidents réels et documentés qui se sont produits pour ce genre d'architecture avec les spécificités des systèmes maritimes et portuaires. De plus, nous avons décrit le développement de la balise embarquée HAPPINESS permettant de collecter des données de navigation réalistes tout en alimentant la plate-forme de simulation. Finalement, le système d'acquisition de données à même pu être embarqué en mer. À l'heure où ces lignes sont écrites, deux systèmes sont placés dans deux types de navires totalement différents et alimentent en continu la plate-forme. Cela combiné aux outils de génération d'attaque, cela permet de revenir simuler par rejeu des comportements réels et non pas une vue de ce qui pourrait peut-être se passer en cas d'attaque, validant les simulations qui ne sont pas essentiellement théoriques, mais réalistes. Ce chapitre permet d'apporter la suite des éléments de réponse pour la question de Recherche **QR2**, mais également de répondre à la question de développement **QD1**.

Le chapitre suivant portera sur l'exploitation des outils présentés précédemment. L'objectif étant l'exploitation et l'analyse des données collectées ainsi que des scénarios d'attaques proposés dans le cadre de deux problématiques cybernétiques spécifiques à savoir : l'apport du traitement du signal dans l'analyse et la détection d'anomalie sur les ICS ; l'apport du "Machine Learning" dans la modélisation du comportement normal / anormal de la cinétique d'un navire à travers l'étude de la falsification des trames NMEA dans les systèmes de navigation.

Chapitre VI

Analyse et Détection d'Anomalies dans les Systèmes Cybernétiques Navals

Sommaire

VI.1 Introduction

Ce chapitre a pour objectif de mettre à profit les données navales générées, pour les valoriser via l'analyse et la détection d'anomalies d'un système cybernétique naval. Le but est également de valider le concept de la balise embarquée HAPINESS, et les outils logiciels développés AEGIS et NAGE, suite à l'expérimentation en condition réelle BELAMY. Pour ce faire, dans un premier temps, nous nous intéressons au problème de la vulnérabilité d'un ICS spécifique : la propulsion (une partie spécifique de la boucle de mobilité). Nous décrivons cette première application en précisant le contexte de l'étude, puis en décrivant l'extraction (génération) des données cybernétiques (avec

ou sans attaque), suivie par la mise en œuvre et l'analyse d'une méthode de détection d'anomalies originale. Cette étude peut être étendue et réalisée, de manière identique, sur les trois autres grandes boucles du navire (décrites dans la section IV.2.3.1). Dans un deuxième temps, nous étudions comment détecter les attaques exploitant les vulnérabilités des systèmes de navigation et plus spécifiquement ceux des trames NMEA générées par les systèmes de localisation de type GPS.

La question de recherche **QR3** sera assurée dans ce Chapitre comme le montre la Fig.VI.1.

Correspondance : Question de Recherche / Chapitre					
	Chap. II	Chap. III	Chap. IV	Chap. V	**Chap. VI**
QR I					
QR II					
QD I					
QR III					

FIGURE VI.1 – Tableau de correspondances entre les Questions de Recherche et les Chapitres.

VI.2 Cas d'étude des ICS

Comme cela a été présenté précédemment, les navires modernes sont composés de systèmes complexes destinés à garantir les exigences fonctionnelles et opérationnelles. Parmi eux, les systèmes embarqués présentent des vulnérabilités spécifiques qui peuvent compromettre le bon fonctionnement du navire. Récemment, l'analyse des systèmes comme les SCADA, l'AIS, l'ECDIS et les VDR a mis en lumière leur vulnérabilité [113]. Cette analyse a révélé plusieurs failles numériques qui doivent être corrigées, car ces systèmes sont sensibles aux cyberattaques [127, 123]. Dans ces systèmes, il existe différentes couches, chacune ayant un rôle spécifique à jouer (chapitre IV, section IV.2.1). Une architecture succincte de la partie automatique du navire illustrée par la figure (VI.2) permet de bien cerner le premier scénario d'étude qui concerne essentiellement la couche automatique du navire. Cette partie gérant le PLC et l'ICS permet la gestion physique des capteurs et des actionneurs ainsi que les systèmes SCADA. Elle représente l'ensemble des serveurs, stations de travail et applications du ICS qui supervisent les processus industriels via des ordinateurs et des IHM.

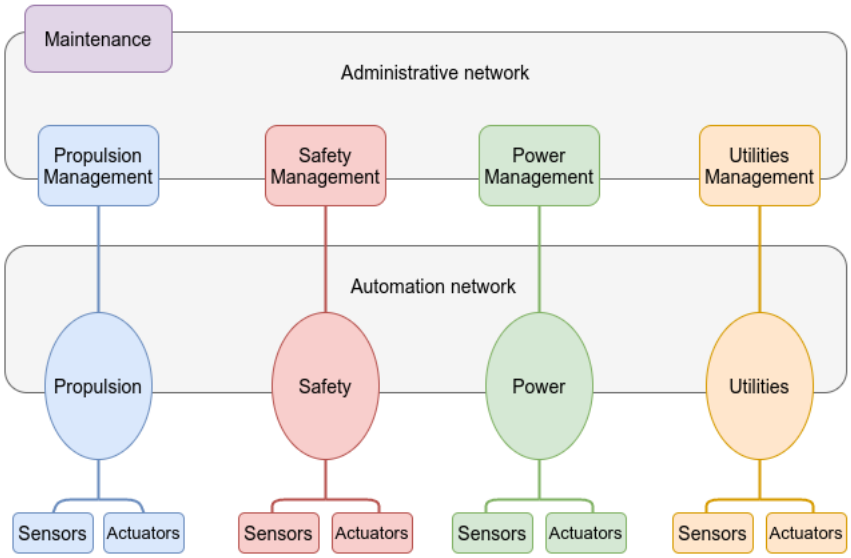


FIGURE VI.2 – Architecture simplifiée de la partie réseau et automatique de la plate-forme.

VI.2.1 Description de la méthode

Dans ce travail, une stratégie d'extraction du trafic réseau est proposée pour illustrer les performances des algorithmes de détection d'anomalies basés sur l'alerte cyber physique. Nous nous concentrons sur le système de gestion de la propulsion (la boucle verte sur la figure (VI.2)).

VI.2.1.1 Extraction du flux cybernétique de gestion de la propulsion

Dans ce type de système, il y a de nombreux équipements tels que des PLC et des IHM, connectés avec des commutateurs et contrôlables à distance par le réseau. Plusieurs cartes d'Entrée/Sorties gèrent les capteurs et les actionneurs qui permettent d'assurer efficacement la navigation. L'architecture proposée pour le système de gestion de la propulsion pour l'extraction de données est représentée dans la figure (VI.3).

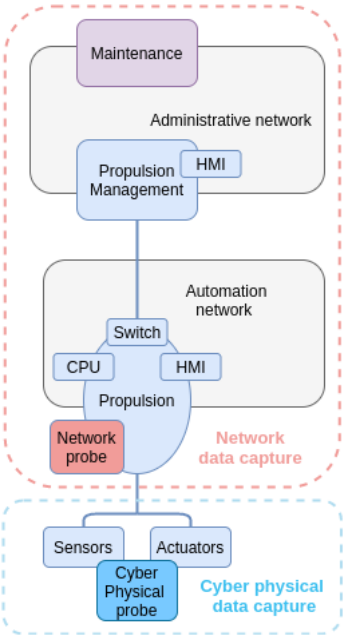


FIGURE VI.3 – Modèle d'extraction de données pour le système de gestion de la propulsion.

Après configuration de l'ensemble du réseau administratif, nous avons installé l'outil de collecte de flux réseau *Tcpdump* [1] pour extraire le trafic réseau. Une autre sonde est utilisée pour collecter l'ensemble des flux physiques (trafic des capteurs et des actionneurs) afin de les comparer au trafic réseau. Les capteurs et actionneurs sont simulés par des cartes microcontrôleur (directement connectées au PLC) pour générer le trafic physique. L'ensemble des sondes est synchronisé pour mettre en évidence la corrélation des anomalies et des attaques. L'ensemble des attaques sur les PLC est réalisé à l'aide de l'outil PAGE présenté dans le chapitre IV à la section V.2. Le scénario (i), correspondant au comportement normal de l'ensemble du système, est représenté par la courbe reportée sur la figure VI.4. Nous simulons le comportement normal du navire sur une durée de 5 minutes avec une accélération croissante suivie d'une décélération. La figure VI.4 montre l'évolution du nombre de paquets ainsi que les valeurs de sortie des capteurs/actionneurs sous forme de séries temporelles sur 5 minutes. Comme indiqué, le nombre de paquets est constant et correspond au flux net de trois CPU, envoyant et recevant du trafic réseau au sein de l'architecture. L'analyse de la courbe de variation du nombre de paquets (Fig. VI.4) ne montre aucune perturbation sur le trafic réseau. Le système de propulsion fonctionne normalement (scénario sans attaque), comme le montrent les figures VI.4, VI.5, VI.6 et VI.7.

1. Cet outil est un analyseur de paquets permettant de récupérer le détail du trafic réseau. Voir le lien https ://www.tcpdump.org/

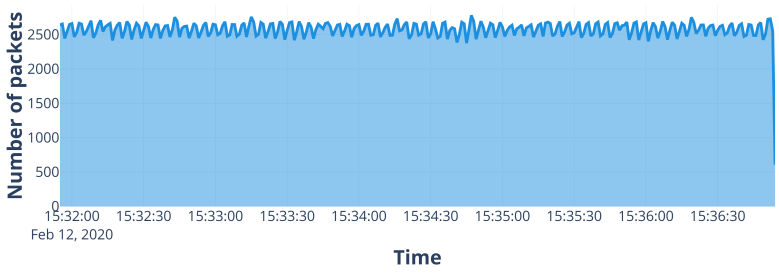


FIGURE VI.4 – Évolution normale du trafic réseau (Boucle Propulsion).

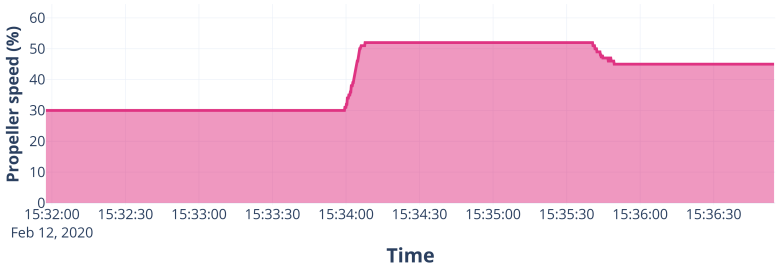


FIGURE VI.5 – Évolution normale de la vitesse de propulsion (Boucle Propulsion).

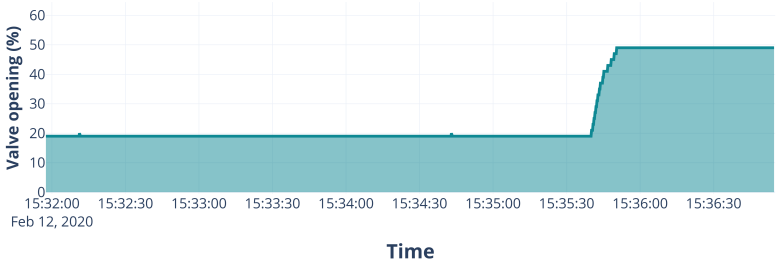


FIGURE VI.6 – Évolution normale d'ouverture de vanne (Boucle Propulsion).

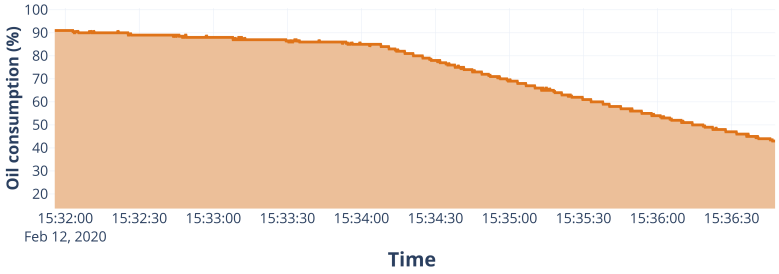


FIGURE VI.7 – Évolution normale de la consommation d'huile (Boucle Propulsion).

VI.2.1.2 Configuration et scénarios d'attaques

Les expériences qui ont été réalisées concernent l'analyse fonctionnelle d'un système de propulsion. Les capteurs et actionneurs simulés, gérés par les cartes d'E/S et l'IHM, génèrent des mesures telles que la vitesse de l'hélice de la ligne d'arbre, l'ouverture des vannes pour diminuer la température, les consommations de carburant et d'huile. Chaque quantité est simulée en fonction d'une autre, ce qui leur permet d'évoluer dans le temps. La consommation d'huile est représentée par un réservoir réel avec un niveau d'eau. Une électrovanne fait varier cette valeur en fonction des commandes de vitesse envoyées à l'IHM via le microcontrôleur connecté à l'automate. Grâce à cette configuration, nous pouvons simuler un comportement normal de l'ensemble du système et des cyberattaques sur le système de gestion de la propulsion. Pour mettre en évidence cette configuration, trois scénarios ont été définis :

(1) Un comportement normal de l'ensemble du système ;

(2) Une attaque de reconnaissance *Port scan* et *DoS* ;

(3) Une attaque *CPU stop and start*.

Le scénario (3) exploite une faille de sécurité permettant à l'attaquant de prendre le contrôle à distance de l'automate. Toutes les attaques qui sont perpétrées dans ces scénarii ont été générées par l'outil "AEGIS" présenté dans la section V.2 du chapitre V.

Scénario (2)

Ce scénario est une attaque en deux étapes : un balayage de ports suivi d'une attaque par DoS. Dans un premier temps, un ordinateur attaquant relié à la couche numérique de l'automate réalise un balayage de ports afin de détecter ceux qui sont libres. La majorité des attaques impliquant un réseau de communication sont initiées par une étape de reconnaissance rendue possible par le manque de compartiments réseau au sein de l'architecture. L'une des méthodes les plus utilisées est l'analyse de ports utilisés par le système visé. La détection de ces balayages de ports est l'un des sujets majeurs de la sécurité des réseaux. Différentes méthodes de détection basées sur l'analyse des statistiques du trafic réseau, ou encore l'utilisation de réseaux de neurones pour classifier les échanges dans le réseau ont été proposées. Dans notre cas, l'identification des ports ouverts est réalisée en utilisant l'outil open source : "Nmap" (*NEtwork Mapping*). La confidentialité des paramètres du système est ainsi impactée, les ports ouverts détectés sont autant de points d'entrée potentiels pour effectuer des attaques supplémentaires sur l'automate. La seconde partie du scénario consiste à réaliser une attaque par DoS pour inonder de requêtes l'automate tout en saturant les connexions possibles (comme présenté dans la section V.2) et ainsi altérer sa disponibilité. Cette attaque est possible grâce à l'identification en amont des ports ouverts associés à l'adresse IP de l'automate. Pour la réaliser, nous avons utilisé un autre outil open source : "hping" ("hping" [2]) permettant de générer en abondance des requêtes ICMP (*Internet Control Message Protocol*) pour

2. http ://www.hping.org/

inonder le réseau et tester la disponibilité de systèmes informatiques. Les automates étant équipés de cartes réseau, ils sont tout à fait sensibles à ce type d'attaque, les rendant indisponibles. Toute commande de contrôle envoyée depuis le SCADA vers l'automate ne devrait avoir aucun effet sur les actionneurs puisqu'elle ne sera pas prise en compte même si les connexions se retrouvent "libérées" par l'attaquant. On comprend que lorsque l'on a besoin de réagir dans un temps imparti, ce type d'attaque peut être problématique.

Scénario (3)

Dans ce scénario une cyberattaque altère une fois de plus la disponibilité des informations transmises dans le système en exploitant une vulnérabilité de l'automate pour forcer son arrêt à partir d'une fausse commande de contrôle. Cette commande de PLC stop arrête automatiquement l'automate et le rend indisponible jusqu'à sa remise en marche. Tout comme dans le premier scénario, l'attaquant récupère la cartographie réseau à partir de l'outil Nmap. En partant du principe que l'attaquant connaît la marque et la gamme de l'automate via des renseignements antérieurs, celui-ci peut alors exploiter une vulnérabilité associée pour injecter une charge utile (payload) et générer l'arrêt de l'automate. Cette approximation sur les connaissances de l'attaquant sur l'automate est réaliste puisque les signatures réseau de ces dispositifs sont aisément reconnaissables dès lors que l'on analyse les échanges dans le réseau concerné. On peut très aisément identifier le type de protocole utilisé et le type d'automate. Pour choisir et configurer la charge utile visant à générer la commande d'arrêt de l'automate, l'attaquant utilise un module spécifique de l'outil Metasploit, une infrastructure logicielle dédiée le plus souvent aux tests de pénétration des systèmes informatiques. Le module utilisé permet de générer les commandes PLC start et PLC stop adapté pour arrêter l'automate et le redémarrer continuellement ou bien le rendre totalement indisponible. En conséquence, les actionneurs ne devraient plus recevoir de commandes de contrôles transmises par le PLC. De même, les valeurs mesurées par les capteurs devraient être transmises à l'automate, mais non lues ou non interprétées par celui-ci, et donc non prises en compte dans l'architecture de contrôle. Si l'on combine à cela une attaque par saturation de connexion empêchant toute connexion légitime de se faire ainsi que la modification d'un bloc fonctionnel (comme présenté dans la Fig. V.8 Section V.2) l'intégrité fonctionnelle se retrouve alors altérée. Par la suite, l'automate est remis en service par une commande PLC start. Avec ce genre d'outil et parce que l'automate ne fait qu'interpréter une commande qu'on lui donne sans s'assurer que la source est fiable, l'attaquant a la main mise complète sur le système.

Un exemple d'attaques est reporté dans la figure (VI.8) à savoir Reconnaissance (scan du réseau) et DoS. Un pic correspondant à une attaque de type scan ("Nmap") est mis en évidence dans cette figure et se situe à $(t + 2)$ minutes, suivi d'une attaque de type DoS ("hping" [3]) qui commence à

3. http ://www.hping.org/

$(t + 2)$ minutes et 30 secondes. Un autre type d'attaque est illustré dans la figure (VI.9). Après le scan de port (Fig. VI.8), l'attaquant contrôle à distance l'automate et réalise deux commandes d'arrêt de l'automate à $(t + 2)$ minutes et $(t + 3)$ minutes. Les graphiques présentés sur les figures (VI.4) et (VI.8) montrent que l'évolution dans le temps des capteurs et du trafic réseau est en partie constante et qu'elle présente également des changements rapides.

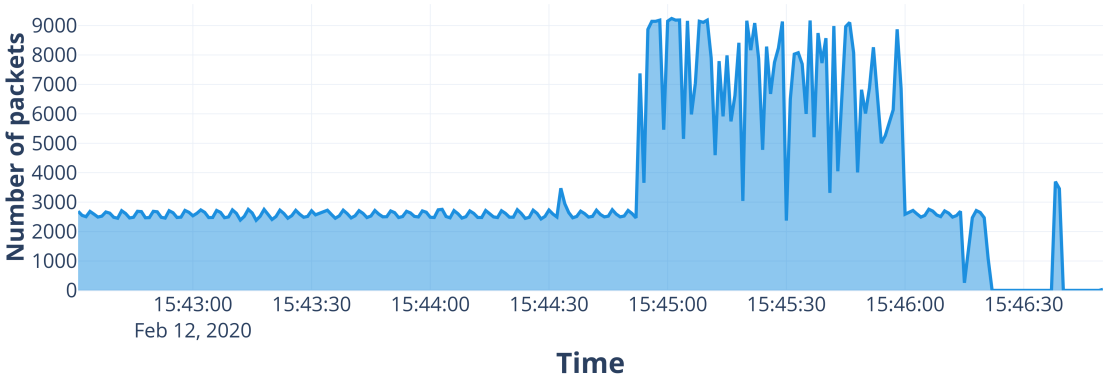


FIGURE VI.8 – Évolution anormale du trafic réseau (Boucle propulsion) - Nmap et DoS.

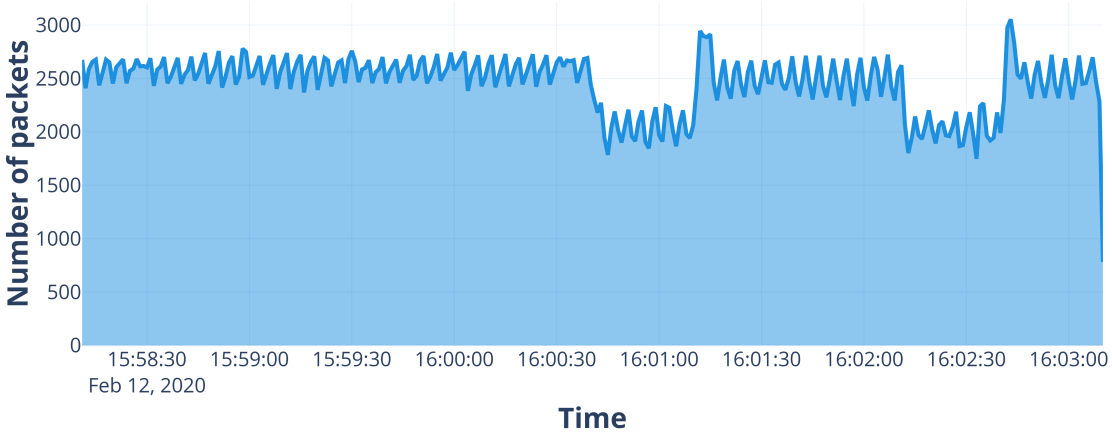


FIGURE VI.9 – Évolution du trafic réseau - PLC STOP (Boucle propulsion).

L'analyse de ces variations abruptes nécessite des outils de détection efficaces pour mettre en évidence les discontinuités, comme les filtres basés sur les dérivées. Pour détecter ces discontinuités, nous proposons une stratégie basée sur l'opérateur d'énergie de Teager-Kaiser (TK), qui est un filtre quadratique basée sur les dérivées du signal [68], et comparons les résultats de détection à ceux de l'opérateur de dérivation classique. La détection des attaques est effectuée en analysant les changements locaux et les discontinuités dans les données, considérées comme des séries temporelles.

VI.2.1.3 Détection d'anomalies avec l'opérateur d'énergie de Teager-Kaiser

L'opérateur d'énergie de TK est une méthode bien établie pour la détection des changements dans les séries temporelles ou les signaux [68]. Cet opérateur a trouvé de nombreuses applications en analyse des signaux et des images [31, 14]. Cet outil est un estimateur d'énergie du point de vue d'un système oscillatoire [68]. Appliqué à une série temporelle continue ou à un signal $x(t)$, la sortie de l'opérateur d'énergie TK est donné par :

$$\Psi_c[x(t)] = \dot{x}^2(t) - x(t)\ddot{x}(t) \tag{VI.1}$$

où $\dot{x}(t)$ et $\dot{x}(t)$ sont les dérivées de premier et second ordre de $x(t)$ par rapport au temps t respectivement. Ainsi l'opérateur Ψ_c peut être vu comme un opérateur dérivatif d'ordre deux. En utilisant l'approximation arrière des dérivées temporelles, la contrepartie en temps discret mise à l'échelle et centrée de Ψ_c devient :

$$\Psi_d[x(n)] = x^2(n) - x(n-1)x(n+1) \tag{VI.2}$$

L'opérateur $\Psi_d[x(n)]$ offre une excellente résolution temporelle, car seuls trois échantillons sont nécessaires pour le calcul de l'énergie à chaque instant, il a donc une bonne adaptabilité aux changements instantanés du signal. En raison de sa sensibilité à ces changements de l'énergie, qui dépendent du contenu fréquentiel du signal, l'opérateur d'énergie TK est considéré comme un outil efficace pour détecter les signaux en forme de pointes. Une version multirésolution de cet opérateur a été initialement proposée par Lin *et al.* [83] mais pour résoudre deux tones très rapprochées :

$$\Psi_{d_m}[x(n)] = x^2(n) - x(n-m)x(n+m) \tag{VI.3}$$

où l'entier m désigne le paramètre de décalage, et représente également l'échelle ou la résolution d'analyse. Une grande valeur de m indique une plus grande échelle puisque les échantillons intervenant dans l'équation (VI.3) sont plus éloignés les uns des autres et la pertinence entre eux diminue. Pour $m = 1$, Ψ_{d_m} est réduit à l'opérateur d'énergie de TK classique Ψ_d (Eq. (VI.2)), qui est d'ordre deux. L'idée est d'utiliser les propriétés multi-échelles des séries temporelles pour identifier les anomalies en utilisant toutes les observations à travers les échelles de temps. À titre de comparaison nous utilisons l'opération de dérivation :

$$\mathcal{D}_m(x(t)) = \frac{\mathrm{d}^m x(t)}{\mathrm{d}t^m} \tag{VI.4}$$

où m est l'ordre de la dérivation.

Remarque

Comme l'opérateur Ψ_{d_1} est d'ordre 2, nous comparons Ψ_{d_m} à l'opérateur de dérivation $\mathcal{D}_{m+1}$.

VI.2.2 Analyse des résultats

Le scénario normal (1) est représenté par la courbe reportée sur la figure VI.4. Cette courbe montre l'évolution du nombre de paquets ainsi que les valeurs de sortie des capteurs/actionneurs sous forme de séries temporelles sur 5 minutes. Comme indiqué, le nombre de paquets est constant et correspond au flux net de trois CPU, envoyant et recevant du trafic réseau au sein de l'architecture. L'analyse de la courbe de variation du nombre de paquets (Fig. VI.4) ne montre aucune perturbation sur le trafic réseau. Le système de propulsion fonctionne normalement, comme le montrent les figures VI.4, VI.5, VI.6 et VI.7. Le scénario normal est résumé par la figure VI.10. Le scénario

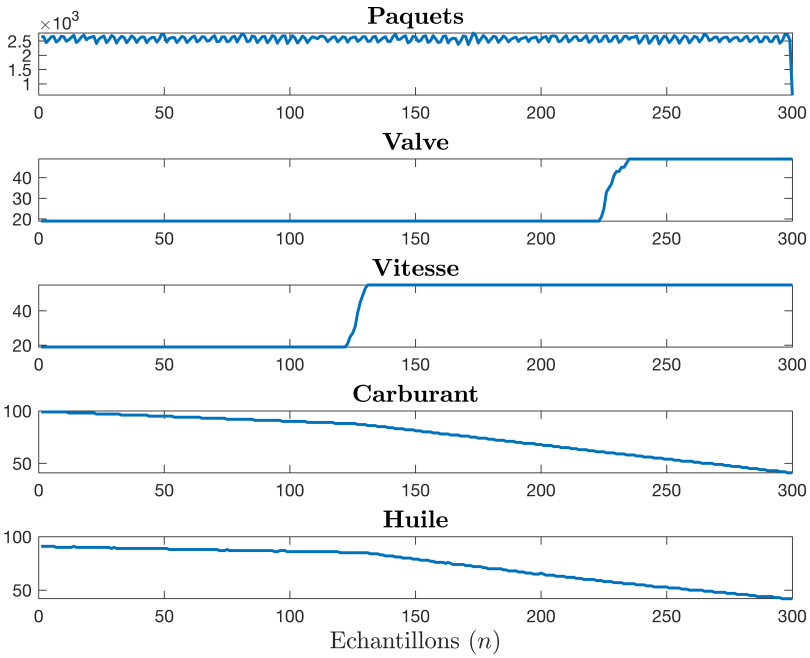


FIGURE VI.10 – Scenario normal : sans attaque PLC-Stop (Boucle propulsion).

(2) correspondant à une reconnaissance et à des attaques DoS est illustré dans la figure VI.8. Ces deux attaques n'ont pas d'effets évidents sur les comportements des capteurs et des actionneurs. Le scénario (3), correspondant à l'arrêt et au démarrage du PLC, illustré sur les figures VI.9, VI.11, VI.12 et VI.13, montre un impact significatif tel qu'une attaque d'*arrêt et démarrage du PLC* peut avoir sur les comportements des capteurs et des actionneurs. Cette attaque exploite une vulnérabilité spécifique de l'équipement qui permet à un attaquant de contrôler à distance les commandes de marche/arrêt de l'automate. Le scénario d'attaque PLC-Stop généré est bruité avec un bruit additif blanc Gaussien de RSB=20dB est résumé par la figure VI.14.

La détection des différentes attaques perpétrées dans les scénarios (2) et (3) montrant l'altération de la disponibilité avec les attaques par saturation de connexion, de DoS et l'attaque PLC-Stop (Boucle Propulsion) sont étudiées via l'analyse des variations locales rapides associées. On part

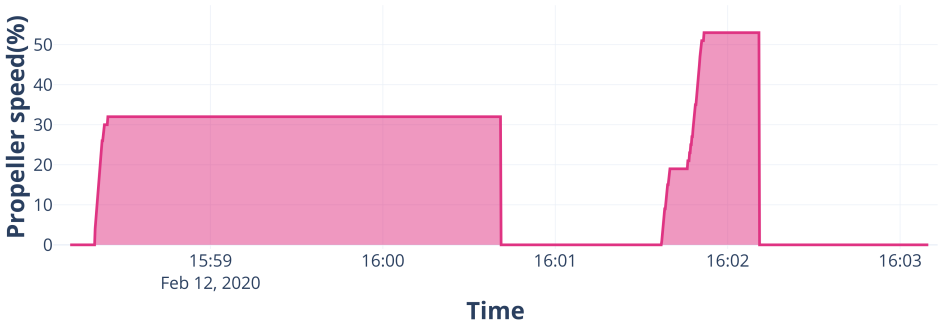


FIGURE VI.11 – Évolution de la vitesse de propulsion - PLC STOP (boucle propulsion).

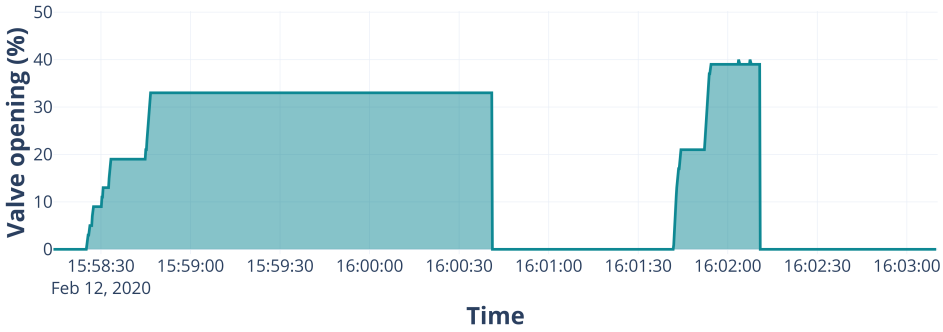


FIGURE VI.12 – Évolution de l'ouverture de vanne - PLC STOP (boucle propulsion).

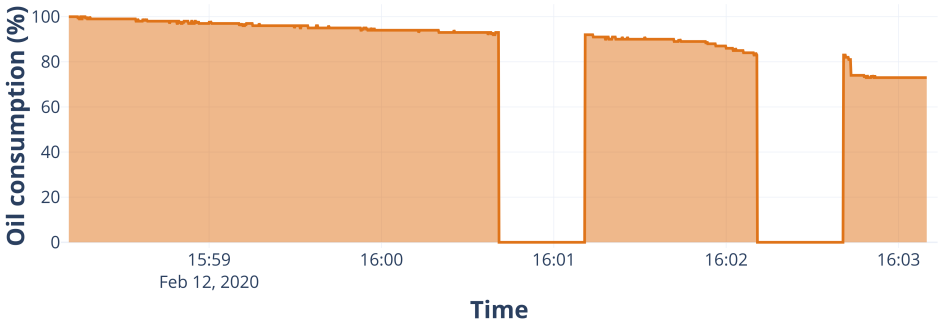


FIGURE VI.13 – Évolution de la consommation d'huile - PLC STOP (boucle propulsion).

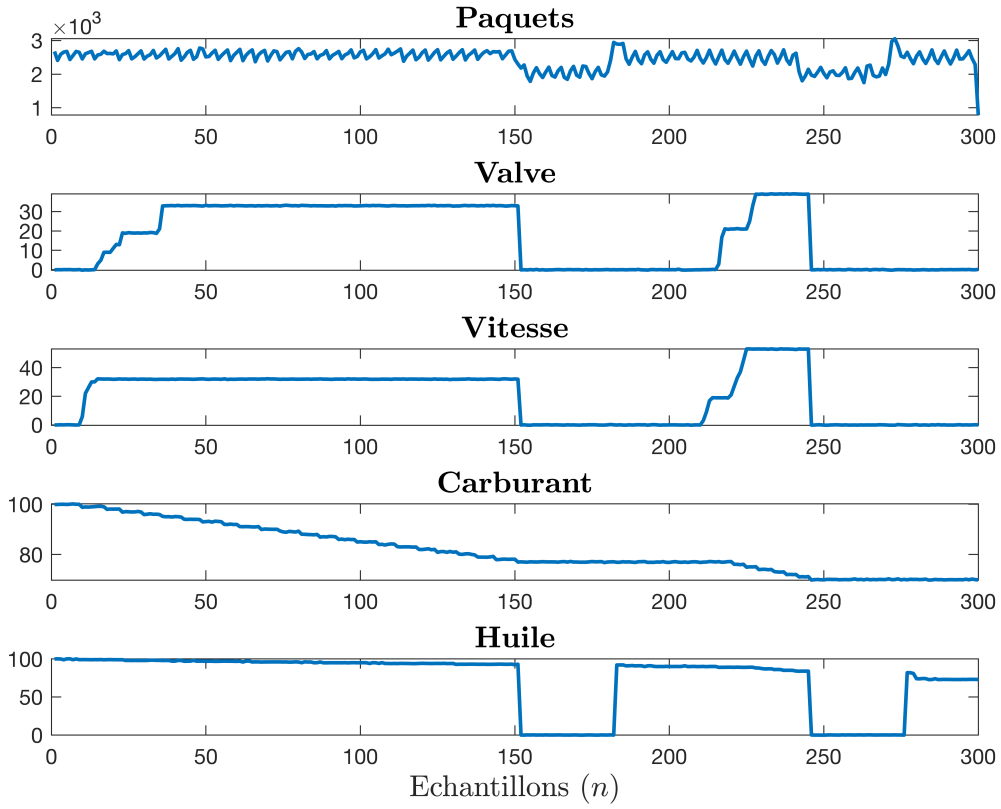


FIGURE VI.14 – Attaque PLC-Stop (Boucle propulsion).

de l'idée que si anomalie il y a, elle doit persister à plusieurs résolutions de la série temporelle. L'idée est d'exploiter les propriétés multiéchelle des données de cette série temporelle pour identifier les anomalies associées en utilisant toutes les observations à travers l'échelle de temps. L'analyse multiéchelle est réalisée en utilisant l'opérateur d'énergie de TK, Ψ_{d_m}, et les résultats sont comparés à ceux de l'opérateur dérivé $\mathcal{D}_{m+1}$. Nous illustrons l'analyse de l'attaque sur quatre niveaux de résolution des séries temporelles : $(m = 2 - 5)$. Nous comparons les résultats des deux opérateurs comme suit : $(\mathcal{D}_2, \Psi_1)$, $(\mathcal{D}_3, \Psi_2)$, $(\mathcal{D}_4, \Psi_3)$ et $(\mathcal{D}_5, \Psi_4)$. Les résultats sont représentés par les figures VI.15, VI.16, VI.17, VI.18, VI.19, VI.20, VI.21 et VI.22. Dans l'ensemble ces résultats montrent que les arrêts et les démarrages du PLC sont identifiés et confirment l'approche multirésolution de la détection d'anomalie. Ces événements sont identifiés sur les quatre échelles et en particulier par l'analyse basée sur l'opérateur d'énergie TK (Figs. VI.16, VI.18, VI.20 et VI.22). De plus, ces résultats montrent que plus l'échelle augmente, plus les anomalies sont mises en évidence par l'opérateur d'énergie de TK, comparé à l'opérateur dérivatif $\mathcal{D}_m$ (Figs. VI.15, VI.17, VI.19 et VI.21). Globalement, toutes les signatures de la série temporelle (transitions et anomalies) sont conservées par l'opérateur d'énergie TK. Cependant, le nombre optimal d'échelles à utiliser pour la détection des anomalies reste un problème ouvert.

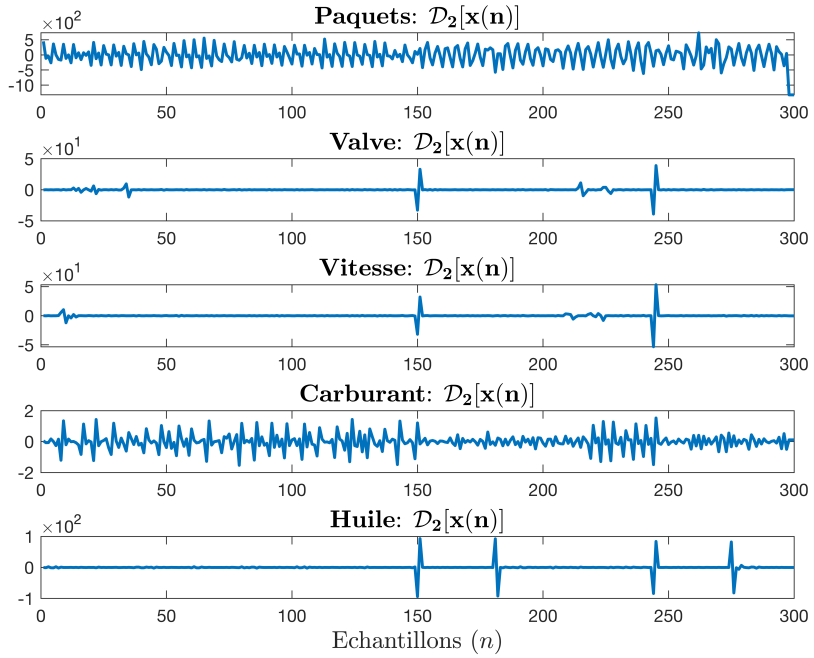


FIGURE VI.15 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur dérivatif : $m = 2$.

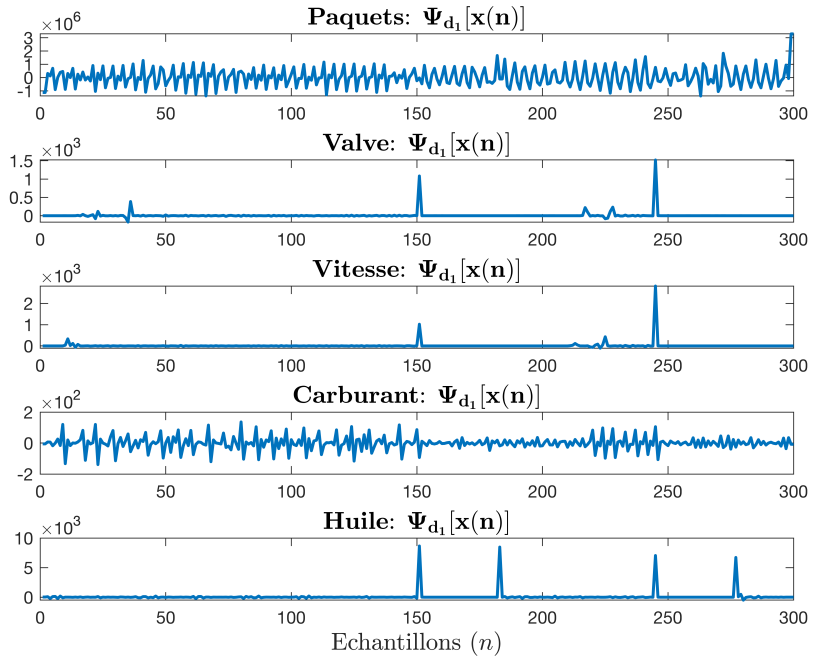


FIGURE VI.16 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur d'énergie de TK : $m = 1$.

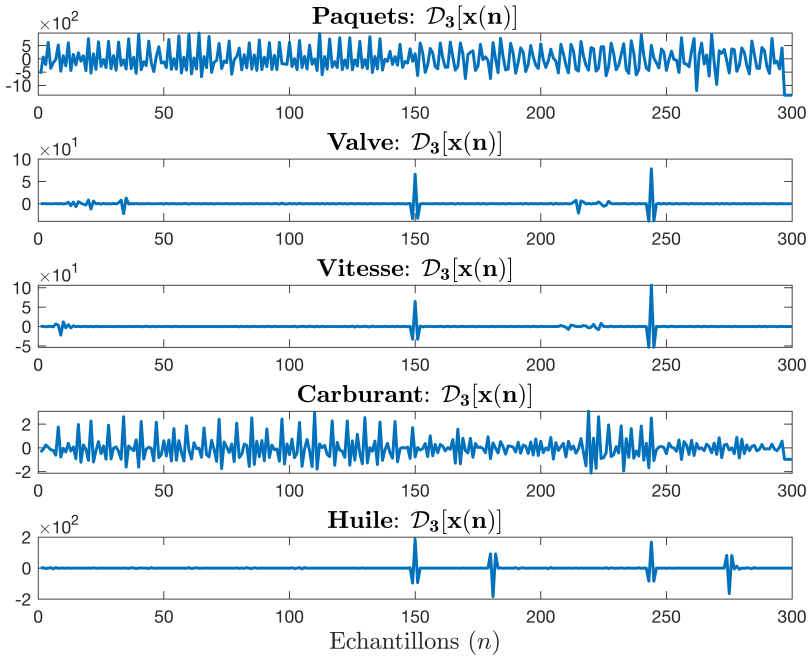


FIGURE VI.17 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur dérivatif : $m = 3$.

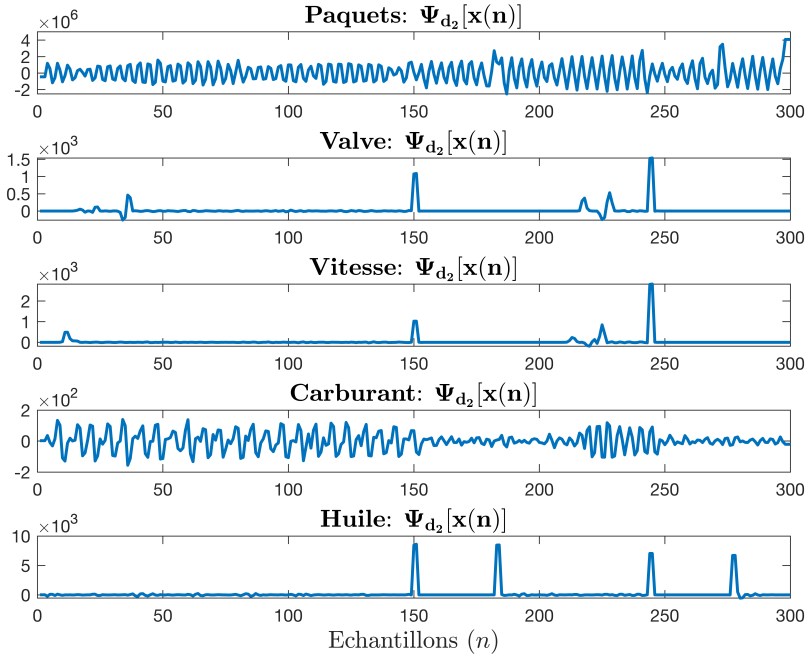


FIGURE VI.18 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur d'énergie de TK : $m = 2$.

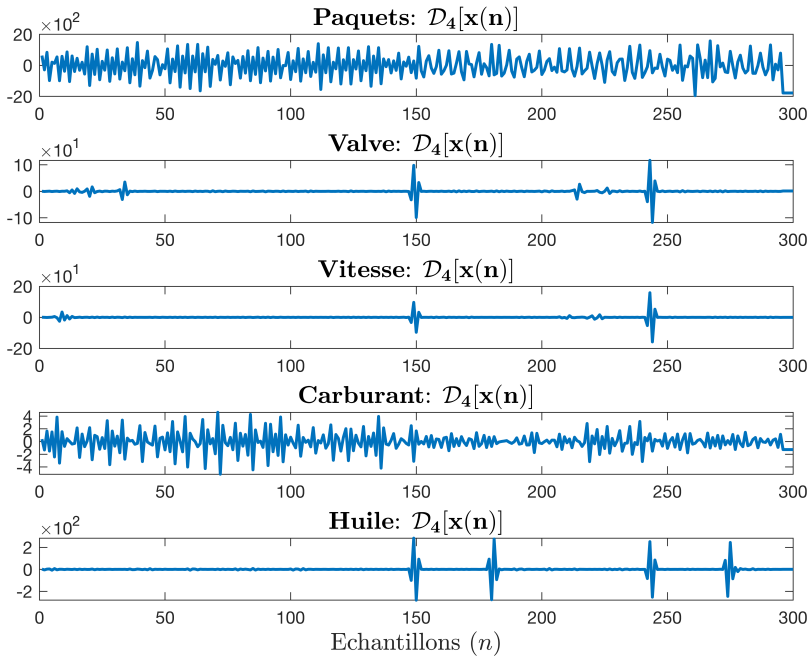


FIGURE VI.19 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur dérivatif : $m = 4$.

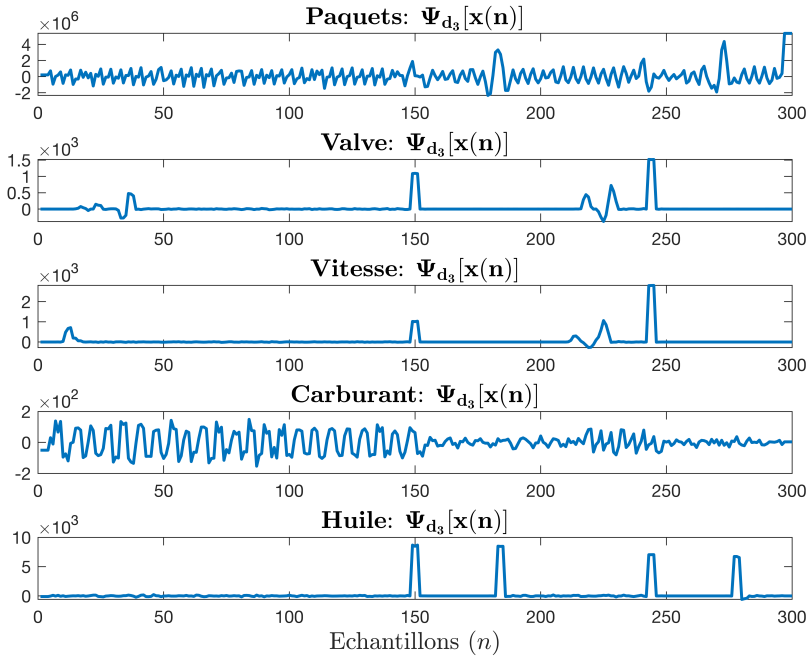


FIGURE VI.20 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur d'énergie de TK : $m = 3$.

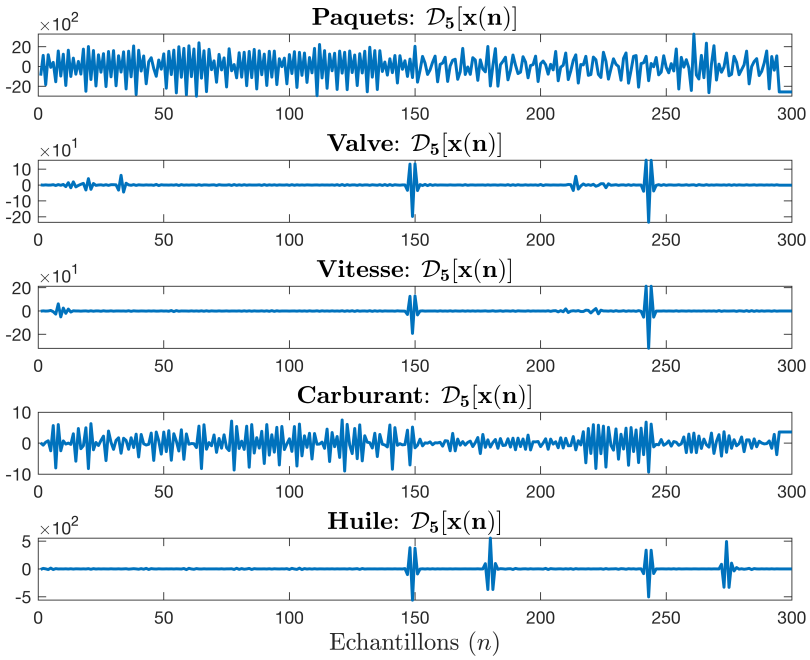


FIGURE VI.21 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur dérivatif : $m = 5$.

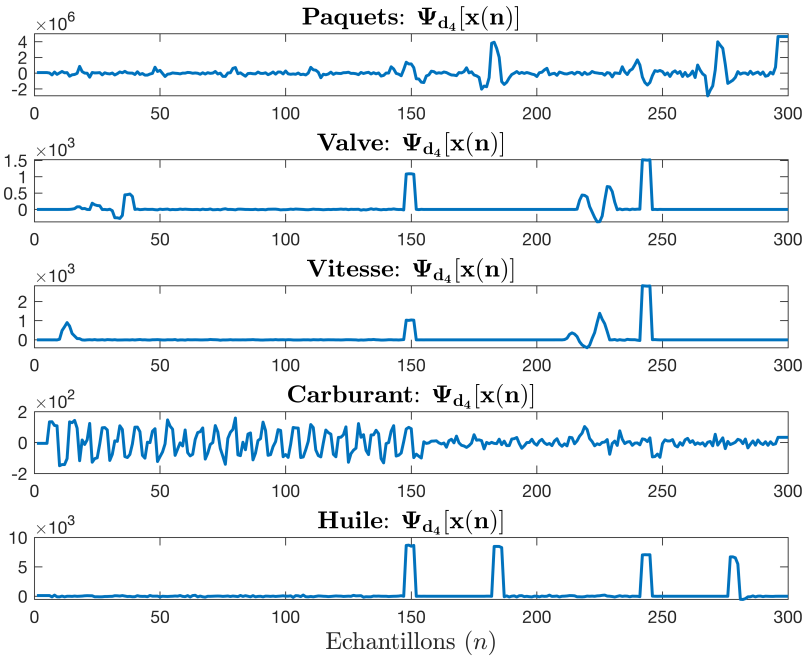


FIGURE VI.22 – Analyse multirésolution de l'attaque d'arrêt de l'automate avec l'opérateur d'énergie de TK : $m = 4$.

VI.2.3 Amélioration de la cybersécurité des systèmes industriels

Dans ce premier cas d'étude, nous avons élaboré une nouvelle stratégie d'extraction de données qui est décrite pour améliorer la gestion des alertes à bord du navire. Les résultats montrent que les alertes des capteurs et des actionneurs sont pertinentes pour assurer la cybersécurité des systèmes navals. Les expériences réalisées révèlent l'impact des attaques sur le système de gestion de la propulsion du navire. La méthode de détection d'anomalies proposée utilisant l'analyse multirésolution, basée sur l'opérateur d'énergie de TK, permet d'identifier efficacement les anomalies injectées. Cette analyse montre l'intérêt d'exploiter la structure multiéchelle des séries temporelles pour une meilleure identification des anomalies. Pour confirmer les résultats obtenus, des analyses de données supplémentaires sont nécessaires.

VI.3 Cas d'étude : les systèmes de navigations

La détection et la réaction en temps utile à une cyberattaque visant un navire, en particulier au milieu de l'océan, nécessitent des processus de connaissance de la situation efficaces et spécifiques. L'étape la plus importante pour assurer la sécurité maritime et accroître l'efficacité de la planification et de la conduite des opérations est l'amélioration de la connaissance de la situation cybermaritime. L'objectif de cette stratégie est de comprendre efficacement ce qui se passe dans l'environnement maritime et qui pourrait avoir un impact sur la sécurité. En général, la *Cyber Situational Awareness* se construit en trois étapes. Pour évaluer la situation, différents processus doivent être mis en place. La première étape, appelée processus de perception de la situation, nécessite le développement d'une architecture globale adaptée pour collecter les données d'intérêt à bord du navire afin d'être conscient de la situation actuelle [61]. La deuxième étape, appelée compréhension de la situation, comprend l'analyse des tendances et des intentions d'attaque, l'analyse de la causalité et l'évaluation des impacts actuels et futurs. La troisième étape, appelée projection de la situation, consiste à prédire l'évolution de la situation [17]. Certaines études ajoutent également une quatrième étape, appelée résolution de la situation, qui, lorsqu'elle est appliquée à la cybernétique, aiderait les analystes de la sécurité et les décideurs à prendre les mesures appropriées, sur la base de l'expérience, des renseignements sur les menaces, des meilleures pratiques et de la compréhension de l'impact [93].

VI.3.1 Description des méthodes

Il est question, ici, de se focaliser sur la détection d'anomalies dans les messages NMEA pouvant être causée par des acteurs malveillants. Une méthode est mise en œuvre pour détecter les anomalies NMEA dans les systèmes de navigation et appuyés sur MITRE ATTACK [129] pour décrire les techniques d'attaques menées dans les scénarios d'attaques. Cette stratégie a été choisie en raison

de son modèle de menace complet dans la description du comportement contradictoire. Plusieurs types de messages NMEA prennent en charge plusieurs fonctions de navigation. Chaque message se compose de plusieurs champs, chacun connectant des informations spécifiques. Les attaquants mènent des procédures d'attaque pour affecter les fonctions de navigation en ciblant des types ou des champs de messages. Les défenseurs implémentent des algorithmes de détection pour protéger les fonctions de navigation en surveillant les types de messages et les champs pour détecter les procédures d'attaques. Le modèle est de nature générale, en tant que telle, il est pertinent pour tout cas d'utilisation qui utilise les données de capteurs communiquées dans les messages NMEA dédiées aux fonctions de navigation.

Pour procéder à la détection d'anomalies dans ce type de données, l'idée est de réaliser l'identification des modèles anormaux (c'est-à-dire, des valeurs ou des événements inhabituels) qui peuvent apparaître pendant les opérations. Dans cette étape, tous les messages dans la portée et leurs champs sont analysés pour identifier les modèles anormaux en fonction d'une certaine catégorisation des anomalies. Des techniques d'attaque peuvent être mises en œuvre pour invoquer des schémas anormaux dans les types de messages sélectionnés et leurs champs de message. Pour ce faire, des algorithmes appropriés sont utiles pour détecter les modèles anormaux causés par les techniques d'attaque portées contre les messages NMEA. Cette étape est étroitement liée à la précédente, car l'algorithme de détection est continuellement mis à l'épreuve et amélioré avec des techniques d'attaque améliorées jusqu'à ce qu'un niveau d'efficacité suffisant soit atteint. Les figures Fig. VI.23 et Fig. VI.24 schématisent les méthodologies de détection.

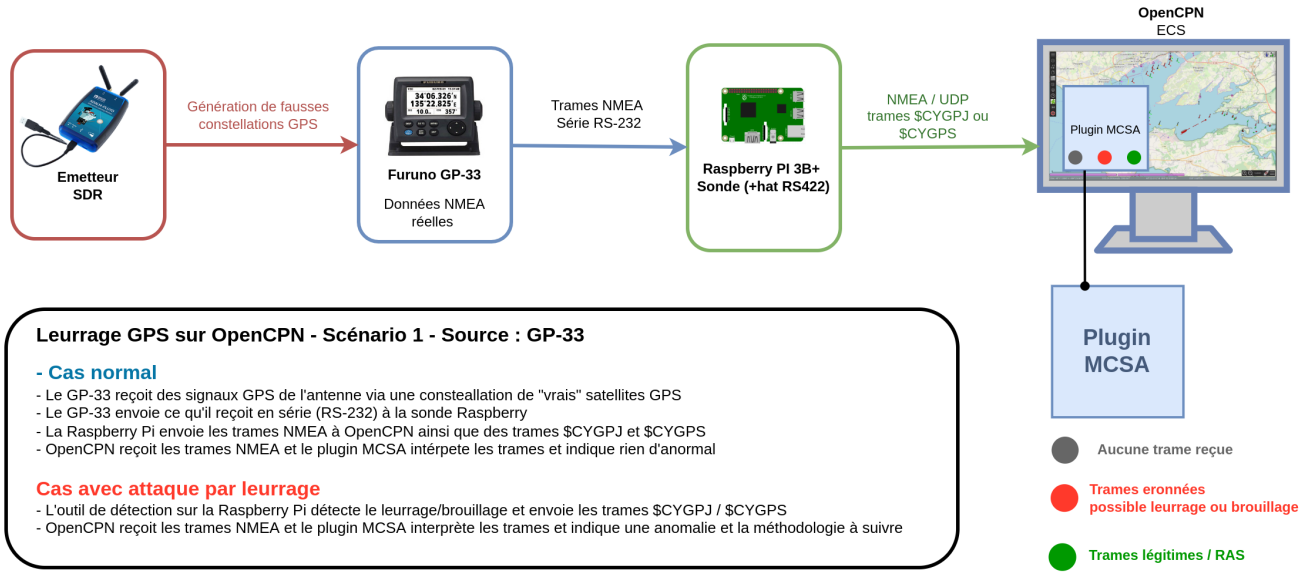


FIGURE VI.23 – Méthodologie de détection cyber dans le cas d'un leurrage GPS.

Dans ce qui suit, la méthodologie conçue pour améliorer la détection des cyberattaques avan-

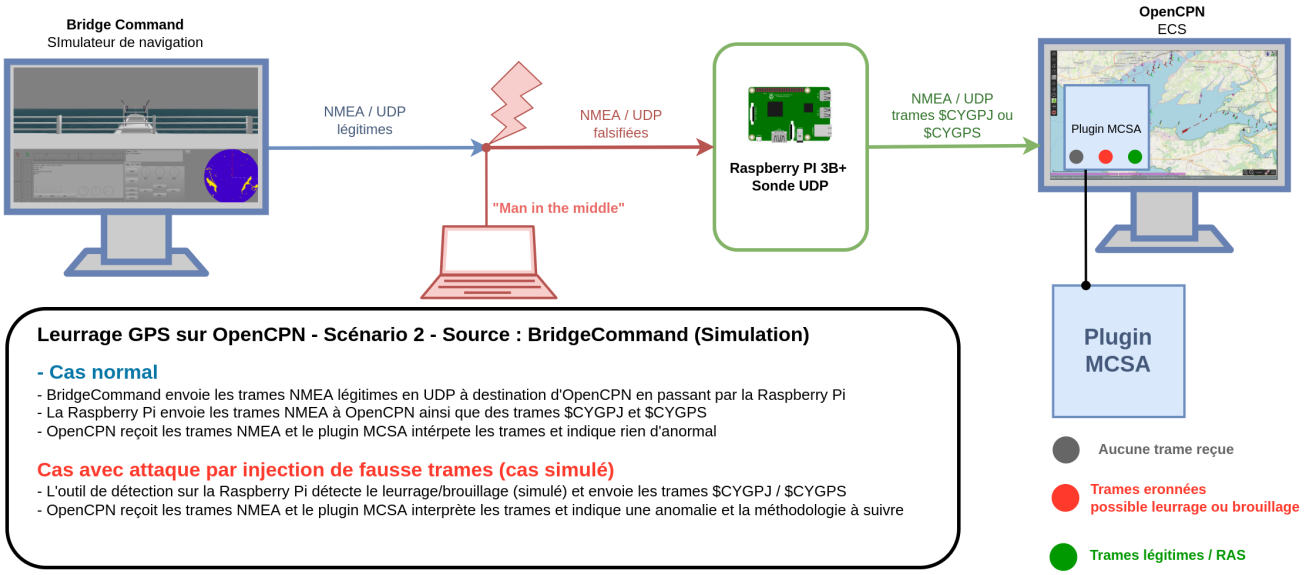


FIGURE VI.24 – Méthodologie de détection cyber dans le cas d'un Man-In-The-Middle sur GPS.

cées sur un système de navigation maritime tel qu'un ECDIS est détaillée. Elle combine les principes de la connaissance de la situation cybernétique pour permettre au décideur de réagir en temps utile. Grâce à l'étude préliminaire que nous avons réalisée dans les chapitres précédents, il a été possible de définir une approche plus complète et précise permettant d'obtenir des résultats décisifs de manière efficace. L'objectif de cette approche est de répondre à des problèmes courants du monde maritime en offrant une solution en temps réel plus simple à mettre en œuvre. Pour assurer une détection efficace des anomalies contre le brouillage et le leurrage, nous avons conçu une méthodologie de détection et une architecture adaptée pour récupérer les données d'un système de navigation maritime et les analyser avant leur envoi vers l'ECDIS (Fig. VI.25). Suivant la progression de nos recherches, l'architecture de notre méthodologie a évolué en plusieurs phases : la première étape (1) représente

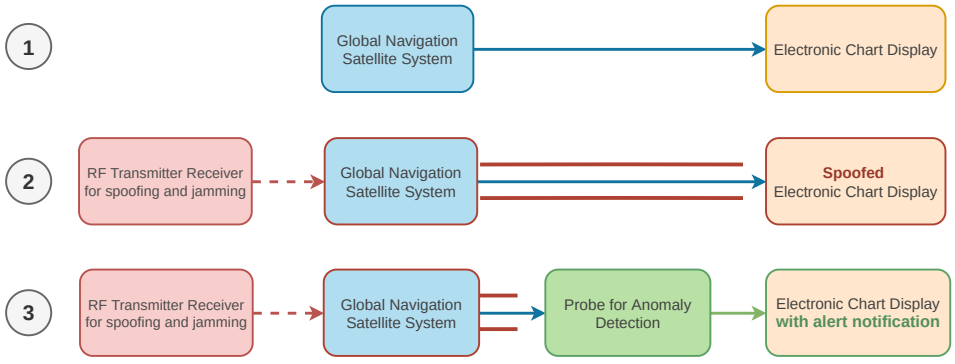


FIGURE VI.25 – Évolution de l'architecture au cours de nos travaux de recherche.

l'architecture la plus couramment rencontrée à bord d'un navire, à savoir une communication directe

entre les équipements de navigation sans aucun composant de cybersécurité. La deuxième étape (2) ajoute une attaque externe de spoofing ou de brouillage via un émetteur RF externe, compromettant le système de navigation. Ce cas se rencontre lorsqu'un navire navigue dans des zones conflictuelles où l'accès aux informations GPS peut être refusé. La troisième étape (3) de cette architecture comprend un système embarqué supplémentaire qui permet l'analyse en temps réel du trafic NMEA grâce à un capteur dédié et renvoie des données qui peuvent être interprétées par un ECDIS ou un ECS. Nous représentons la mise en œuvre de notre architecture avec des dispositifs et des systèmes réalistes pour réaliser toutes nos expériences. Pour réaliser notre stratégie de détection, différents équipements sont utilisés :

— **Software Defined Radio (SDR) RF Transmitter Receiver** : Adalm-Pluto ou HackRF One-SDR utilisés comme dispositif de falsiication et de brouillage ;

— **Récepteur GPS maritime** : un Furuno GP-33 connecté à une antenne de réception ;

— **Une carte Raspberry Pi 3B+** : utilisée comme une sonde pour analyser en temps réel les flux NMEA et assurer la détection des anomalies ;

— **Système de cartes électroniques** : un ordinateur portable avec OpenCPN (un logiciel de cartographie électronique recevant et interprétant les flux NMEA).

Dans notre environnement de recherche sécurisé, le système est configuré pour générer une fausse constellation de satellites GPS en utilisant les données des éphémérides GPS (un fichier contenant les positions des satellites dans le temps à intervalles réguliers). Nous avons commencé à faire de cette façon, mais, pour des raisons pratiques, nous avons procédé de la même manière avec les données de simulation générées par l'outil que nous avons développé. Comme le montre la figure VI.24, on utilise un émetteur / récepteur RF (détaillé dans la section V.3) pour générer une attaque externe sur le réseau NMEA (les données générées par l'outil développé). Ce système est capable de collecter momentanément des éphémérides et de générer une fausse constellation de satellites, en fonction d'une position préalablement définie. Dans cette configuration, le système envoie un message dont le signal associé est plus élevé que celui envoyé par les satellites, brouillant ainsi le système GPS et usurpant ensuite une nouvelle position. Aujourd'hui, les capteurs existants pour la détection des anomalies nécessitent souvent une configuration et une grande expertise technique.

VI.3.1.1 Exploitation de la cinématique du navire pour la détection des anomalies

Un changement de position GPS se traduit par une ou plusieurs variations de position inattendues entre deux trames successives qui peuvent être caractérisées comme un décalage. À partir d'un instant t où la falsification GPS commence, le point GPS sera décalé, caractérisé par une différence entre la position attendue et la position observée comme le détaille la figure VI.26. Le point clé est la détection de falsification de positions GPS en combinant les informations de position données par les caractéristiques de latitude et de longitude des champs NMEA, mais aussi qu'avec d'autres

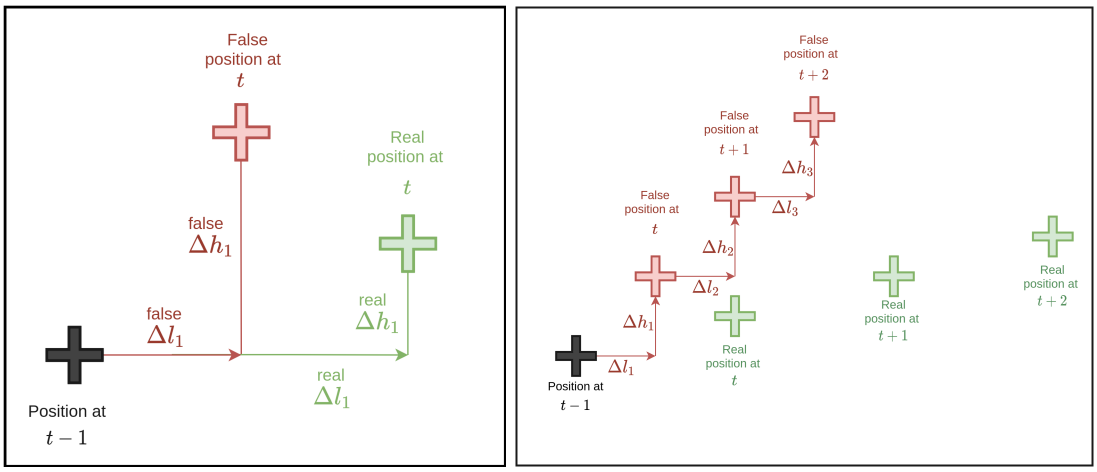


FIGURE VI.26 – Détournement simple et successif des points GPS du au GPS spoofing.

caractéristiques telles que *Speed Over Ground* et *Track Angle*. En effet, il n'est pas pertinent de se limiter uniquement à la comparaison entre les positions GPS, utilisant la latitude et la longitude, car une fausse position peut être cohérente dans l'espace dans lequel évolue le navire même s'il a été modifié. De nouvelles données sont nécessaires qui, combinées aux champs NMEA existants, permettent la détection d'anomalies pour une falsification GPS avancée. La méthode proposée consiste

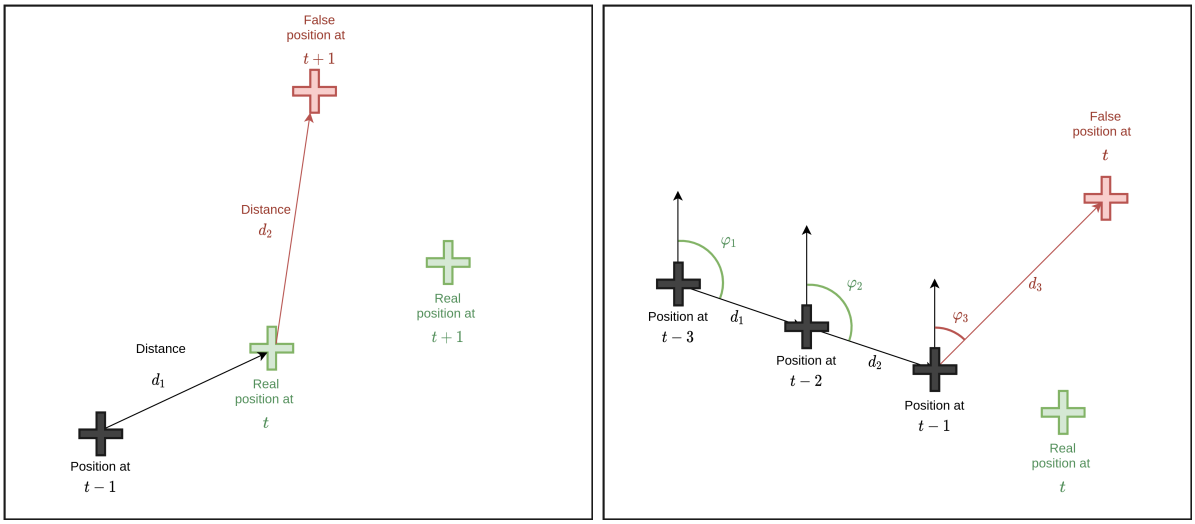


FIGURE VI.27 – Détermination de la distance et du parcours pour la détection des anomalies.

à déterminer la distance et la trajectoire entre deux points consécutifs. En supposant qu'un leurre GPS provoque une discontinuité dans le cap et la distance parcourue par le navire, il sera possible de détecter d'éventuelles anomalies dans l'évolution de ces variables. Dans une situation normale, lorsqu'un navire se déplace dans son propre environnement, nous supposons que la séquence de variation de la distance et du cap est bornée, et donc qu'une attaque peut provoquer des anomalies dans cette séquence. Comme le montre la figure VI.27, une distance trop élevée par rapport à une

vitesse donnée et une variation de cap trop importante par rapport à une situation normale peuvent rendre possible la détection d'anomalies dues à la falsification du GPS.

La combinaison d'une analyse de la variation de la trajectoire et de la distance par rapport à la vitesse du navire permet de construire une zone dans laquelle les points GPS peuvent être identifiés ou non comme des points d'anomalie. La méthode basée sur l'angle de route considère qu'un point est une anomalie lorsqu'il sort d'un cône devant le navire (caractérisé par une trop grande variation). La méthode basée sur la distance considère un point comme une anomalie lorsque ce point sort d'un cercle englobant le navire, dont le diamètre dépend du calcul de la distance définie par la vitesse du navire. Ceci nous permet de modéliser la cinématique du navire, si un point leurre GPS a une trop grande variation d'angle de trace ou de distance et est situé dans une des zones, alors une anomalie sera détectée comme le montre la figure VI.28. Cependant, il existe un angle mort de détection, car si le point GPS modifié est trop proche d'un point cohérent potentiel sur le navire, cela représente une zone non couverte par la détection. Dans cette zone, d'autres caractéristiques utiles à la détection devront être exploitées. Toute la partie concernant la détection d'anomalies a été codée en Python et directement implémentée sur les sondes de détection connectées aux backbones NMEA.

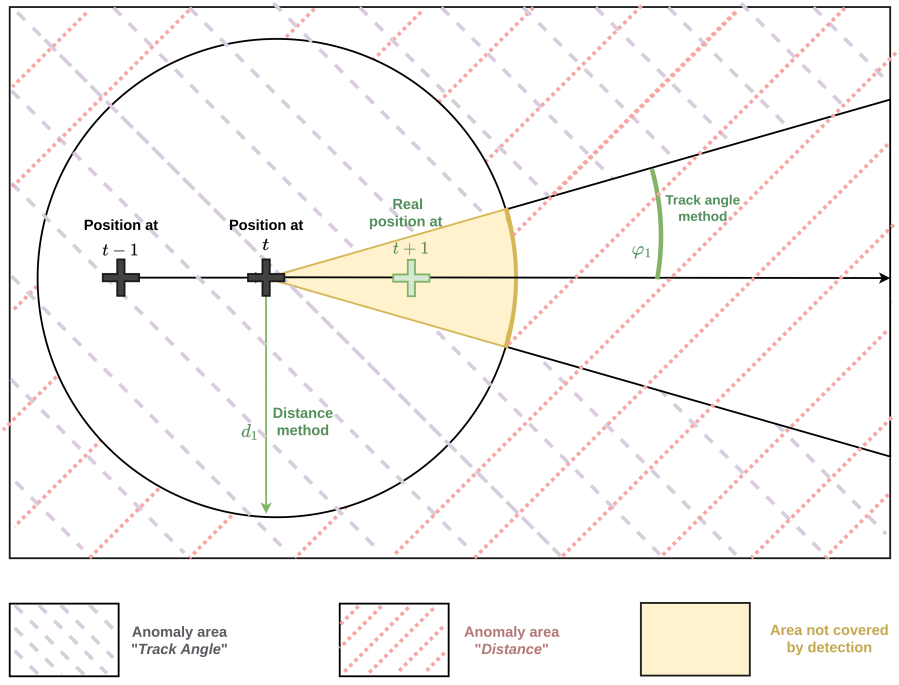


FIGURE VI.28 – Zones de détection des anomalies en fonction de la cinématique du navire.

VI.3.1.2 Attributs navire pour la détection des anomalies

Afin de détecter efficacement les anomalies dans le trafic du réseau NMEA, des caractéristiques pertinentes doivent être utilisées. Différentes caractéristiques sont extraites et normalisées, et sont énumérées ci-dessous :

1. **GPRMC** - *"Lat"* : les coordonnées géographiques sont des valeurs angulaires représentant la position nord-sud d'un point. Combinées à la longitude, elles déterminent la position précise d'un élément sur la terre.
2. **GPRMC** - *"Long"* : coordonnées géographiques sous forme de valeur angulaire représentant la position est-ouest d'un point. Combinée à la latitude, elle détermine la position précise d'un élément sur la terre.
3. **GPRMC** - *"S.O.G"* : vitesse du bateau en nœuds (1 nœud = 1,852 km/h).
4. **GPRMC** - *"C.M.D"* : course Made Good ou Track Angle, direction du bateau en degrés.
5. **GPGGA** - *"GPS_Fix"* : données de localisation et d'ondulation du GPS qui sont les informations de localisation que le système GPS fournit pour un point spécifique.
6. **GPGGA** - *"Number_of_SVs"* : nombre de satellites utilisés.
7. **GPGGA** - *"H.D.O.P"* : dilution horizontale de précision qui est une mesure positionnelle de la précision indiquant la propagation des erreurs de géométrie des satellites de navigation.
8. **GPGGA** - *"Orthemetric_Height"* : altitude de l'antenne au-dessus/au-dessous du niveau moyen de la mer en mètres.

VI.3.1.3 Traitement des données

En général les données réelles sont bruitées et entachées d'incertitude. À cela s'ajoute le fait que les données multicapteurs ou multivariées prennent des valeurs dans des intervalles différents. Le prétraitement de ces données est une étape centrale avant leur analyse, ou l'application de plusieurs algorithmes, pour les transformer dans un format utile et efficace. La normalisation, ou préparation des données, est un exemple de prétraitement qui consiste à modifier les valeurs des données pour utiliser une échelle commune, sans que les différences de plages de valeurs ne soient faussées et sans perte d'informations. Dans nos expérimentations, nous avons utilisé les techniques de normalisation StandardScaler (*Permet de normaliser les caractéristiques en supprimant la moyenne et en mettant à l'échelle la variance unitaire.*), MinMaxScaler (*Permet de trasnformer les caratéristiques en les mettant à l'échelle sur une plage donnée*) et RobustScaler (*Permet d'échelonner les caractéristiques en utilisant des statistiques qui sont robustes aux valeurs aberrantes.*), définies comme suit :

$$\text{MinMaxScaler} = X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}} \tag{VI.5}$$

$$\text{StandardScaler} = X_{scaled} = \frac{X - \mu_X}{\sigma_X} \tag{VI.6}$$

$$\text{RobustScaler} = X_{scaled} = \frac{X - \text{median}}{IQR} \tag{VI.7}$$

MinMaxScaler met à l'échelle toutes les caractéristiques des données dans la plage $[0, 1]$ (VI.5). S'il y a des valeurs négatives dans l'ensemble de données, cette mise à l'échelle comprime toutes les valeurs aberrantes dans une plage étroite. StandardScaler (VI.6) correspond au Z-score qui consiste à centrer (moyenne nulle) et réduire les données (variance unité). RobustScaler (VI.7) est plus robuste que MinMaxScaler et StandardScaler vis-à-vis des valeurs aberrantes. Cette normalisation soustrait la médiane et divise le résultat obtenu par l'intervalle interquartile (IQR pour InterQuartile Range). Ainsi, cette méthode supprime la médiane et met les données à l'échelle entre le 1er quartile et le 3e quartile (IQR).

VI.3.2 Simulations et résultats

Dans cette section, nous présentons les résultats de l'application de quatre méthodes de classification à classe unique, utilisées en Apprentissage automatique, pour la détection des aberrations à savoir les séparateurs à vastes marges à une classe (OCSVM ou OneClass - Support Vector Machine en Anglais), le facteur d'aberration locale (LOF), la forêt d'isolement (IF) et la covariance robuste (RC). La détection de valeurs aberrantes peut être considérée comme un classificateur binaire : une instance est soit normale ou anormale. Il existe plusieurs métriques pour déterminer la performance d'un classificateur binaire pour la détection d'intrusion (réseau industriel, domestique, de bureau mais aussi dans un ensemble de données de navigation). En raison de la grande quantité de trafic, les faux positifs peuvent avoir des effets notables. Tout d'abord, un long délai est nécessaire pour l'enquête. En raison du nombre potentiellement élevé de faux positifs qu'ils génèrent, ils peuvent, cognitivement, rendre les administrateurs négligents, un phénomène appelé fatigue des alarmes. Il ne faut pas oublier non plus qu'il n'y a pas de ressources humaines spécialisées en cybernétique à bord d'un navire pour analyser ces alertes. Enfin, la quantité de trafic normal dans un réseau de navigation dépasse généralement de loin la quantité de trafic malveillant. Cela signifie qu'une classification erronée de 0,1% du trafic normal et malveillant entraîne un nombre élevé d'alarmes.

La qualité de la connaissance de la situation cyber en maritime dépend de la qualité des capteurs et des données collectées. Les métriques d'évaluation telles que la précision (performance globale du modèle) (III.1) et le score F1 (métrique hybride utile pour les classes non équilibrées) (III.1) sont calculées sur la base de l'assurance de détecter de vrais positifs (TP) et des vrais négatifs (TN) avec un niveau de faux positifs (FP) et de faux négatifs (FN) aussi bas que possible. Ces métriques sont utilisées pour évaluer les performances des algorithmes de détection d'anomalies.

Des études récentes ont montré la valeur ajoutée potentielle de l'analyse du trafic à partir

du GPS pour une variété d'applications maritimes [21]. Cependant, des travaux antérieurs ont montré que le GPS peut être sujet à des messages erronés en raison d'une mauvaise configuration du dispositif ou de cyberattaques qui sont critiques à classifier. En observant qu'une approche d'apprentissage axée sur les données s'est avérée être un moyen efficace pour collecter et rassembler l'ensemble du flux NMEA, nous avons mené une étude pour comprendre comment réaliser une détection d'anomalies en temps réel sur les messages GPS. À notre connaissance, il n'existe pas de méthode d'Apprentissage automatique qui combine directement le flux de données maritimes et les principes de la sensibilisation à la cybersécurité maritime (ou connaissance de la situation cybermaritime).

L'Apprentissage automatique étant basé sur les données, il nécessite des données d'entraînement importantes pour être efficace. Les caractéristiques des données utilisées pour la résolution d'un problème dépendent en particulier du nombre et de la diversité des caractéristiques candidates des données et cela a un impact direct sur l'applicabilité d'une approche d'Apprentissage automatique et de ses performances. Par conséquent, nous avons mené une série d'études en utilisant l'ensemble de données générées pour obtenir les informations nécessaires sur les données GPS. Les résultats de détection de nouveauté suite au leurrage GNSS avec les algorithmes OCSVM, LOF, IF et RC sont représentés respectivement par les figures (VI.29), (VI.30), (VI.31) et (VI.32). Ces figures permettent de visualiser les frontières de décision définies par chacun des algorithmes de détection. Les résultats de détection en termes de précision et Score F1 sont reportés dans le Tableau VI.1. L'analyse des résultats du Tableau VI.1, montre que sur les différents types de scénarios, l'algorithme IF donne des résultats légèrement meilleurs que les algorithmes OCSVM et LOF, tandis que l'algorithme RC donne les plus mauvais résultats.

Le matériel dont le prix est modeste, la réduction de la taille des systèmes informatiques relativement performants, et les avancées dans le domaine de détection d'anomalies rendent possible la solution de systèmes compacts et portables pour la détection précoce des anomalies. Ce travail décrit un système portable d'acquisition de données en temps réel et de traitement automatisé basé sur Raspberry Pi qui utilise l'Apprentissage automatique pour identifier et détecter efficacement les attaques par falsification GNSS. Chaque modèle a d'abord été calculé sur un ordinateur offrant des capacités plus puissantes qu'une simple carte Raspberry. Le modèle qui fournit des résultats plus intéressants que les autres a ensuite été implémenté dans le système embarqué pour effectuer une analyse en temps réel. L'idée est de ne pas avoir à recalculer la base d'apprentissage à chaque fois, mais seulement à comparer avec les nouvelles entrées.

VI.3.3 Amélioration de la cybersécurité des systèmes industriels

Nous proposons alors une évolution de le protocole NMEA-0183, mettant en œuvre des phrases de détection d'anomalies. Pour faciliter la prise en compte des cyberattaques sur les données NMEA

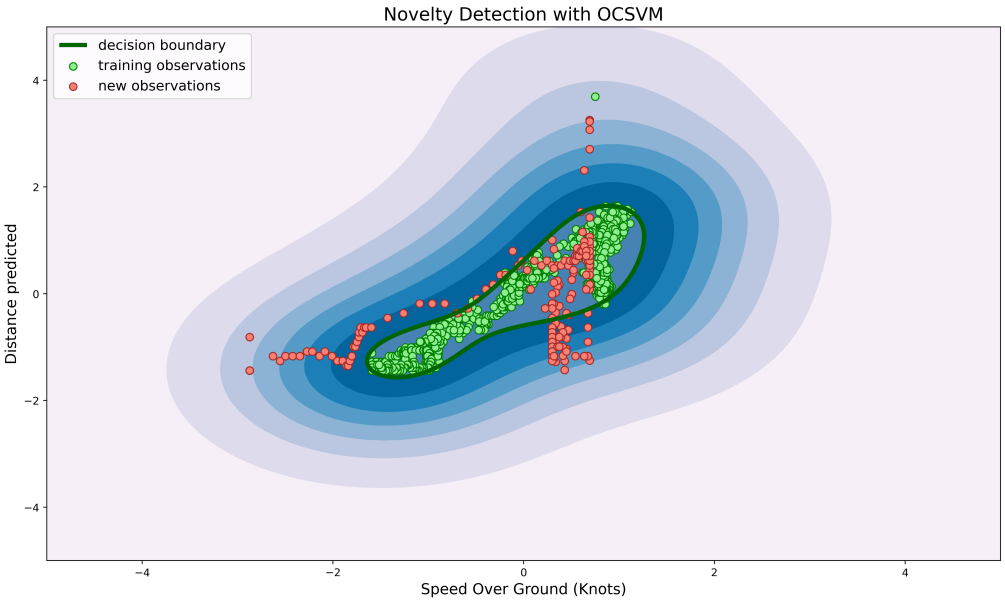


FIGURE VI.29 – Exemple de détection de nouveauté avec le modèle de OCSVM dans un scénario de leurrage GNSS.

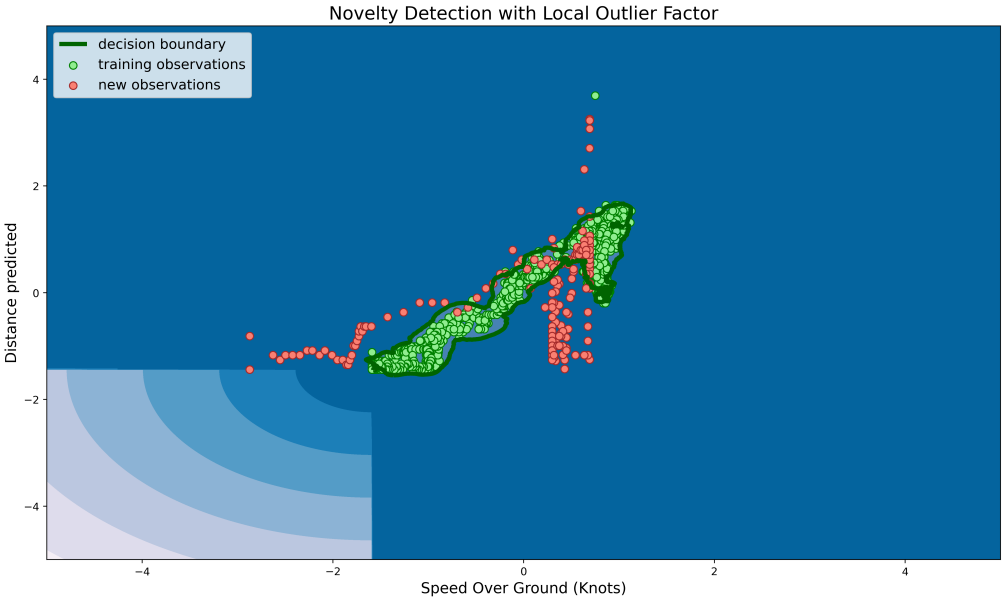


FIGURE VI.30 – Exemple de détection de nouveauté avec le modèle de LOF dans un scénario de leurrage GNSS.

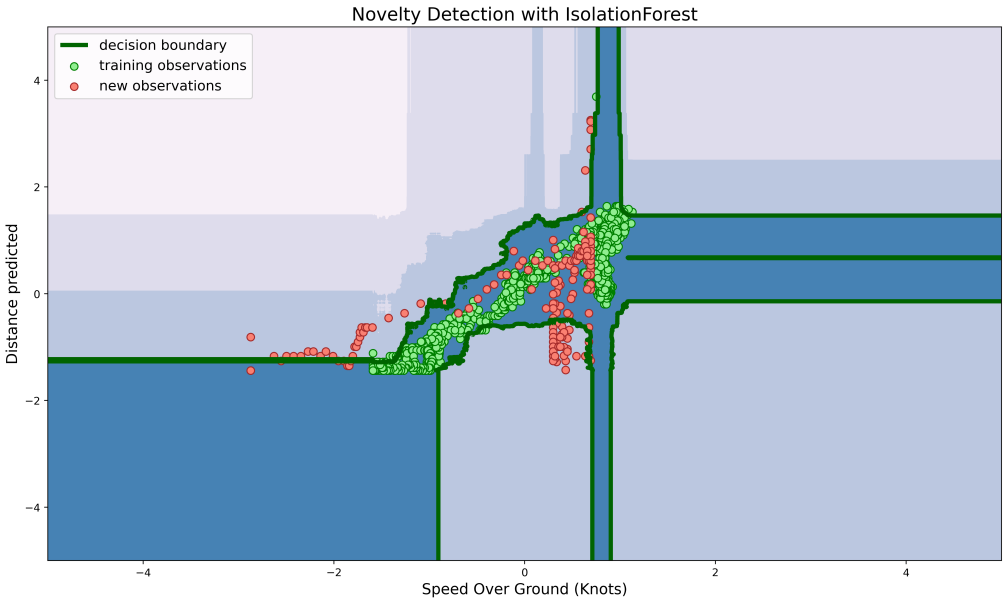


FIGURE VI.31 – Exemple de détection de nouveauté avec le modèle d'IF dans un scénario de leurrage GNSS.

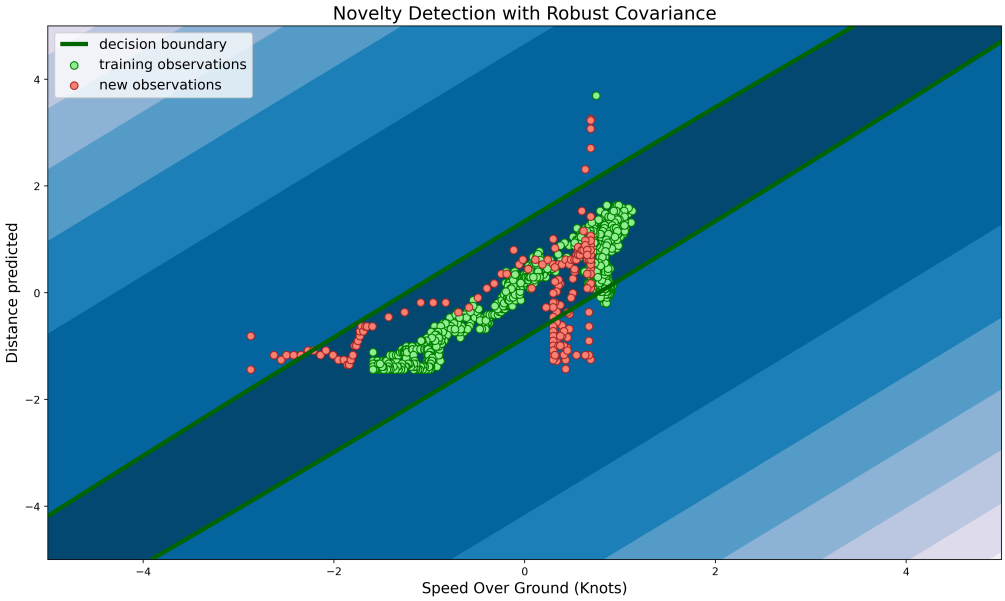


FIGURE VI.32 – Exemple de détection de nouveauté avec le modèle de RC dans un scénario de leurrage GNSS.

Algorithme de détection de nouveauté	Attaque de leurrage GNSS	Précision	Score F1
OCSVM	Static	97.9%	99.0%
LOF	Static	98.4%	99.2%
IF	Static	99.0%	99.5%
RC	Static	89.1%	94.8%
OCSVM	Decoy	95.0%	97.5%
LOF	Decoy	94.0%	96.9%
IF	Decoy	96.9%	98.4%
RC	Decoy	80.1%	88.9%
OCSVM	Straight	98.9%	99.5%
LOF	Straight	97.8%	98.9%
IF	Straight	98.9%	99.5%
RC	Straight	83.0%	90.7%
OCSVM	Offset	97.4%	98.7%
LOF	Offset	96.6%	98.3%
IF	Offset	97.8%	98.9%
RC	Offset	93.1%	96.4%

TABLE VI.1 – Résultats des algorithmes de détection de nouveautés sur les données NMEA.

directement au niveau de l'ECS, nous avons conçu de nouvelles trames NMEA qui peuvent être interprétées par les équipements du réseau NMEA-0183 grâce à un plugin que nous avons développé sur le logiciel Open-CPN ECS. Nous appelons ces nouvelles trames CYGPS car elles effectuent une Cyber analyse du GPS. Une phrase **CYGPS** reçue sur un réseau pourrait être, par exemple :

```
$CYGPS, 120004,1*.64D
```

La phrase **CYGPS** est décrite dans le Tableau VI.2.

TABLE VI.2 – Description de la phrase CYGPS

Field	Comments
$CYGPS	Sentence ID
CY	Talker ID, "cyber" component
120004	time of the fix, here 12 :00 :04 UTC
1-0	Anomaly indicator (1 : an anomaly is detected 0 : NO anomaly detected).
*64D	the checksum of the data

Afin de faciliter la compréhension de ce type d'interactions, nous avons créé un plugin capable d'intercepter les nouvelles trames NMEA et de les interpréter sur un système de navigation. Un statut "vert" indique qu'il n'y a rien d'anormal sur la réception des trames NMEA 0183 : l'opérateur est alors informé qu'il n'y a rien à signaler au niveau de la navigation. Un statut "gris", indique qu'il

y a un problème de réception de trames ou un défaut de réception des systèmes GPS ou AIS avec un message spécifique indiquant à l'opérateur qu'il y a un problème (fonction "watchdog"). Enfin, un statut "rouge" qui indique à l'opérateur qu'il y a une cyberattaque potentielle. Un message d'alerte est affiché pour avertir l'opérateur que quelque chose ne va pas et lui suggère d'utiliser des méthodes de positionnement alternatives. Dans notre cas de figure et par facilité de conception, la sonde qui intercepte les trames, détecte les anomalies dans les données et envoie les trames CYGPS est le même système. Mais dans une architecture plus globale, ce type de système peut être séparé par module pour compartimenter la partie "interception", la partie "détection" et la partie "génération" pour une meilleure étanchéité. Des exemples d'alerte sur un ECS utilisant la fonction de détection d'anomalie proposée sont représentés sur la figure VI.33. Les résultats de classification présentés dans le Tableau VI.1 montrent le potentiel de notre stratégie de détection.

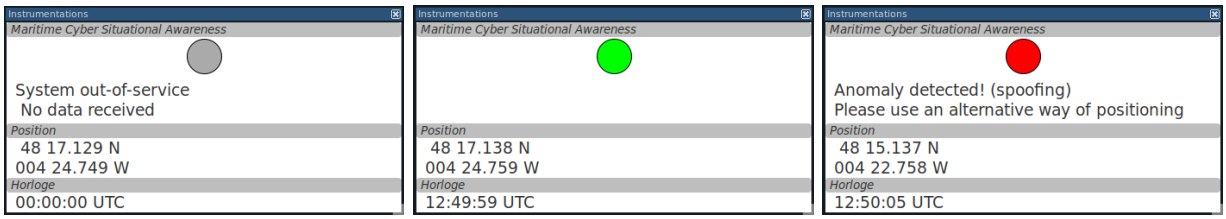


FIGURE VI.33 – Statuts gris, vert et rouge du plugin développé.

Les figures VI.34 et VI.35 représentent des images de capture d'écran de l'ECDIS lors d'une démonstration de manipulation de GPS au large des côtes françaises, près de l'École Navale dans la rade de Brest, encore dans des conditions d'expérimentation sécurisées.

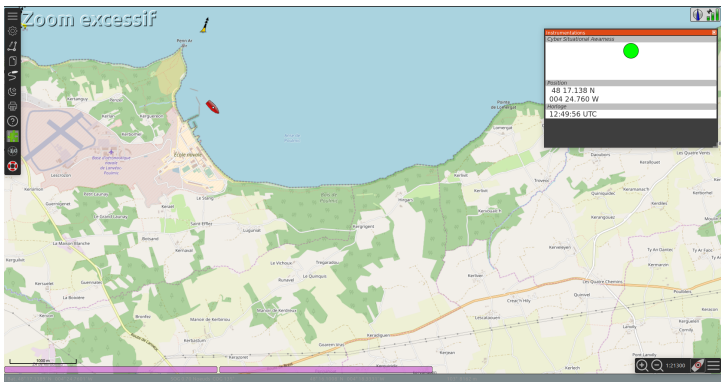


FIGURE VI.34 – Statut vert du plugin, indiquant l'absence de cyber-attaques GNSS.

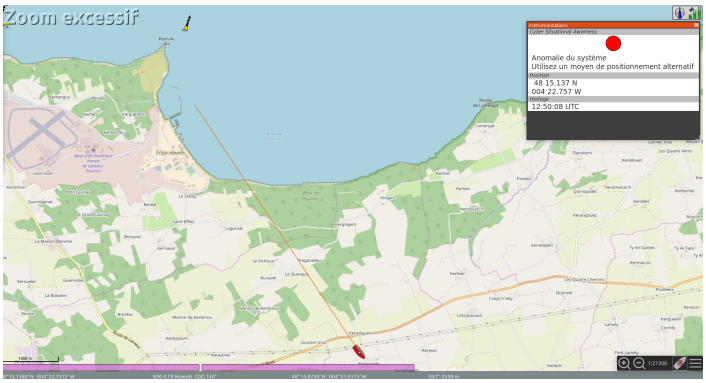


FIGURE VI.35 – Statut rouge du plugin, indiquant la présence de cyber-attaques GNSS.

Nous avons implémenté le plugin que nous avons développé directement dans le logiciel de cartographie open source utilisé pour le système de cartographie électronique appelé "OpenCPN", afin de démontrer notre preuve de concept en bout de chaîne. Ce plugin nous permet de compléter la stratégie complète qui était de combiner la détection d'anomalies via des méthodes d'algorithmes d'apprentissage d'automatique et le respect des principes de la sensibilisation à la cybersécurité maritime (ou connaissance de la situation cybermaritime). Cette preuve de concept présente de nouveaux types de trames interprétables par un plugin tactique sur un système de cartes de navigation électroniques.

VI.4 Conclusion

Dans ce chapitre, plusieurs contributions ont été proposées. Pour commencer, une approche multirésolution basée sur des méthodes de détection de discontinuités et de changements locaux des données au cours du temps, qui sont attribuées aux cyberattaques sur les systèmes de contrôles industriels. Les résultats de détection sur des données issues des ICS, obtenus par l'opérateur d'énergie de Teager-Kaiser (TK) et de l'opérateur de dérivation. Ces résultats montrent aussi l'intérêt de l'analyse multirésolution des attaques. Ensuite, une approche d'Apprentissage automatique pour la détection d'anomalies GPS basée sur le comportement des navires a été proposée. Avec un contrôle total sur les données NMEA-0183 générées et avec un équipement opérationnel imitant celles générées à bord des navires, nous avons créé un dissecteur de protocole adapté à la norme NMEA 0183 afin d'extraire des caractéristiques pertinentes pour l'analyse des données.

Une stratégie de détection axée sur les données a ensuite été développée, basée sur des systèmes de sondes embarquées et portables pour analyser les flux de données NMEA en direct transitant dans les systèmes de navigation. Des algorithmes de détection de nouveauté tels que les One-Class Support Vector Machine, Local Outlier Factor, Isolation Forest et Robust Covariance ont été utilisés et comparés. Ensuite, en respectant les principes de sensibilisation à la cybersécurité maritime (ou

connaissance de la situation cybermaritime) les anomalies détectées sont transmises en utilisant les nouvelles phrases proposées pour la norme NMEA-0183 afin d'être affichées sur les systèmes de navigation tels que l'ECDIS et l'ECS.

Enfin une séquence d'analyse disséquante des messages collectés sur les flux de trafic GPS a été imaginée en proposant un moyen d'alerter les opérateurs de potentielles cyberattaques sur les systèmes de navigation. L'exemple de l'utilisation d'un appareil portable et peu coûteux pour mettre en évidence une stratégie de détection d'anomalies a démontré que les étapes de mise en œuvre et d'amélioration de la cybersécurité à bord du navire et aux systèmes existants peuvent être réalisées de manière efficace en temps réel. Ce chapitre répond à la suite de la question de recherche **QR3**. Le Chapitre suivant (Chap. VII) décrit les différentes conclusions et les perspectives de recherches associées.

Chapitre VII

Conclusion générale et perspectives

Sommaire

VII.1 Rappel de la problématique

Si le transport maritime représente aujourd'hui à lui seul une très grande part de la totalité du commerce mondial, c'est en partie grâce aux progrès de numérisation et d'automatisation des systèmes qui composent les navires. Et si ce domaine réunit des acteurs et des organisations de taille, de maturité, de complexité et de portée opérationnelle différentes, il est devenu indispensable dans le rouage du développement économique. Malheureusement, ces mutations ont rendu ces systèmes vulnérables et augmenté le risque aux attaques cyber. De plus, la connectivité accrue et la convergence des systèmes navals et plus particulièrement les systèmes IT et les OT engendrent un élargissement de la surface d'attaque exposant par conséquent plus que jamais les opérations maritimes à de nouvelles menaces.

VII.2 Contributions

Dans cette thèse, nous nous sommes focalisés sur deux objectifs majeurs à savoir l'identification des vulnérabilités des systèmes ainsi que l'élaboration de méthodologies de génération de données et de détection d'anomalies dans les systèmes cybernétiques navals.

Les deux premiers chapitres ont proposé des réponses à la première partie de la question **QR1** : "*Comment générer des données crédibles et mener des attaques réalistes permettant de valider les travaux connexes ?*". Au deuxième chapitre un état de l'art est présenté sur les systèmes navals dans leur ensemble en détaillant certains liens entre les systèmes, leur fonctionnement ainsi que les vulnérabilités associées. Cela nous a permis d'identifier la criticité de chaque système en fonction de son exploitation au sein de l'architecture globale d'un navire ou bien d'un environnement portuaire. Nous avons également identifié quels sont les systèmes à mettre en place et à développer permettant d'avoir une architecture fiable, et surtout proche de celle d'un navire disposant de systèmes de télécommunications spécifiques. Ensuite nous avons détaillé quelques exemples d'incidents de cybersécurité dans les secteurs les plus critiques pour faire le parallèle avec la criticité du monde maritime, notamment ses composantes industrielles fortement touchées de par leurs vulnérabilités. Après la présentation de nombreux exemples de cyberattaques spécifiques relatives au monde maritime, nous avons évoqué en quoi la prise de conscience de ces vulnérabilités permet d'instaurer au fur et à mesure une certaine politique de cybersécurité dans le domaine maritime comme détaillé dans le troisième chapitre.

Pour répondre à la deuxième partie de la question **QR1** et la question **QR2** "*Quels sont les marqueurs significatifs des d'attaques générées par rapport à la réalité ?* ", nous avons d'abord présenté l'environnement dans lequel se situe l'ensemble des travaux de cette thèse à savoir la plate-forme de simulation d'un navire situé à l'École Navale, le Naval Cyber-Range. Cette nouvelle plate-forme numérique de simulation est unique en son genre dans le domaine, de par ses spécifications techniques et combinant systèmes numériques et physiques. Nous avons participé activement à l'élaboration de cette plate-forme pour générer, collecter, simuler et synthétiser des données réalistes en vue d'études cybernétiques (attaque, défense, sécurité, résilience, modélisation,...). Nous avons notamment proposé un environnement permettant d'élaborer des scénarios pertinents d'attaques réalistes par rapport aux incidents déjà produits dans ce type d'infrastructure. Nous avons élaboré des scénarios basés sur de vrais incidents qui se sont produits ou qui peuvent potentiellement se produire avec les spécificités des systèmes maritimes et portuaires.

Pour répondre à la question **QD1** "*Quels outils informatiques et matériels à développer pour faciliter la génération de données et de scénarios ainsi que la détection d'anomalies ?*", le développement et la conception d'outils spécifiques permettant d'alimenter la plate-forme de simulation en données réalistes couplés à des scénarios d'attaques étaient nécessaires. La réponse à cette question est donnée par le développement d'outils comme AEGIS et NAGE qui permettent respectivement de simuler des scénarios d'attaques dans des données provenant de systèmes industriels pour l'un et des systèmes de navigation (et notamment le récepteur GPS) pour l'autre. L'outil HAPPINESS, faisant également partie de ces contributions, est un système autonome de collecte de données de navigation installé sur de vrais navires et alimentant en continu la plate-forme de simulation avec des données réalistes. Ces outils développés ont été motivés par l'expérience BELAMY pendant laquelle de vraies

attaques sur des GNSS ont été perpétrées dans un environnement contrôlé, permettant de mieux imaginer le comportement des attaques sur ce type de systèmes et de valider la théorie des scénarios imaginés. Pour répondre à la **QR3** "*Quelle est la meilleure façon pour détecter les anomalies dans ce contexte maritime ?* ", nous avons identifié quelques solutions bien connues et issues de récents travaux de la littérature, comme les méthodes de détection d'anomalies, permettent d'améliorer la cybersécurité maritime. Il est notamment présenté des méthodes de détection d'intrusion basées sur l'apprentissage automatique, exploitées et évaluées dans ce manuscrit. Différentes propositions sont faites et chacune des méthodes est illustrée directement sur les données générées par les outils et systèmes de la plate-forme.

La figure Fig. VII.1 suivante représente d'ailleurs la stratégie globale de collection de données issues de la plate-forme. Cependant cette fois-ci, il sera indiqué les liens entre les différentes questions de recherches correspondantes aux différentes portions de l'architecture combinées avec les contributions directes et tous les systèmes imaginés et développés au cours de cette thèse.

VII.3 Perspectives

Dans cette thèse nous avons proposé des solutions permettant de répondre aux problématiques identifiées, qui peuvent bien évidemment prolonger les travaux de cette thèse par des perspectives qui sont variées. Les résultats obtenus sont dépendants des limitations des méthodologies utilisées pour la génération de données et ainsi que celles des techniques de détection d'anomalies exploitées. Ces limitations constituent des perspectives qu'il serait intéressant d'explorer.

La plate-forme de simulation exploitée tout au long de cette thèse a permis de tirer profit directement des systèmes très spécifiques propes au monde maritime et de pouvoir générer des données, qui, à notre connaissance n'existent pas dans la littérature de manière accessible. Cependant, même si la plate-forme permet un large panel d'expérimentations autour du navire, il est important de garder à l'esprit la présence de biais évoqués tout au long du manuscrit, comme le fait que certains systèmes ne sont que simulés malgré des appareillages physiques (à bas coût), et donc forcément ne représentent que sommairement les vrais systèmes d'un navire. Si la partie automatique avec les IHM et les ICS est la plus aboutie, la partie de la plate-forme représentant la passerelle de navigation mériterait d'être davantage développée avec d'autres types de systèmes. De la même manière, la connectivité entre les systèmes industriels et les systèmes de navigation mériterait d'être améliorée, même si les premiers essais d'interactions ont déjà vu le jour.

Les méthodologies de collecte et d'analyse de données nous ont permis d'identifier les caractéristiques propres à chaque type de données issues de systèmes navals avec leurs protocoles de communication spécifiques. En revanche, quand bien même un certain nombre d'outils ont permis d'élaborer et de visualiser l'évolution en temps réel des données sur toute la plate-forme, il serait

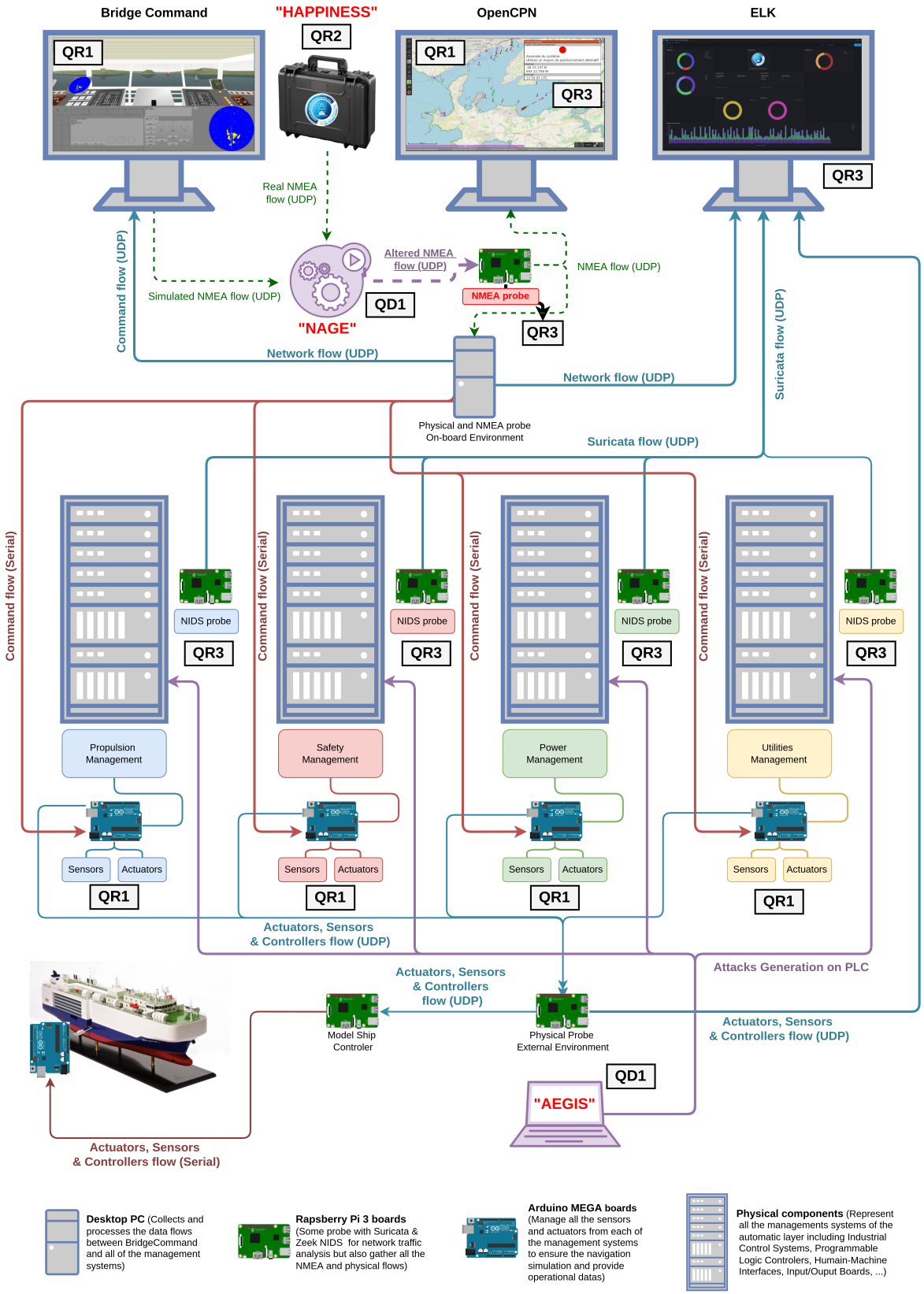


FIGURE VII.1 – Ajout des contributions sur l'architecture globale de la plate-forme Naval Cyber-Range.

intéressant de corréler davantage les données issues des ICS, les données des capteurs et les données issues des systèmes de navigation. Analyser et comparer ces différents flux de données pourrait être une façon intéressante de détecter les anomalies. Des attaques sur les systèmes de navigation peuvent faire émerger des prémisses d'attaques potentielles sur les ICS et inversement. L'un des points initiés a été notamment de placer des points de sondes à plusieurs niveaux pour observer l'évolution de différents flux de données à travers toute la plate-forme. Ce point mériterait d'être davantage exploré et peut représenter une perspective intéressante pour de futurs axes de recherches dans le domaine.

Pour analyser les flux de données issues des ICS, nous nous sommes focalisés sur les flux réseau provenant des automates en les comparant à des sondes capteurs placés directement sur les modules entrées-sorties des automates. Il a été observé que les flux réseau présents sur les IHM sont tous aussi déterministes (en termes de variations de séries temporelles) que ceux sur les systèmes à automates. Analyser l'évolution de ces flux pourrait être intéressant pour globaliser la détection d'anomalies et placer d'autres sondes réseau. En ce qui concerne les données de navigation, notamment les données propres aux protocoles NMEA-0183, nous avons réussi à gérer plusieurs types de données issues de ces protocoles grâce à un outil de simulation et d'analyser quels champs étaient plus pertinents que d'autres pour réaliser la détection d'anomalies. De la même manière, pour enrichir les différentes bases de données de la plate-forme avec des données réalistes, la balise embarquée a permis d'obtenir d'autres types de trames directement issues de navires en activité. Nous avons par ailleurs analysé des types de trames spécifiques aux informations satellitaires comme les trames GPRMC, GPGGA, GPGSV et GPGSA, mais d'autres trames du format NMEA peuvent être exploitées pour une analyse plus poussée [1]. Par exemple, une analyse approfondie sur les trames provenant plus spécifiquement des systèmes intégrés permet d'avoir des informations sur l'utilisation des moteurs et du gouvernail. Ces données étant toutes aussi vulnérables que les autres, elle peuvent-être exploitées pour leurrer les systèmes de cartographie sur la direction et la vitesse du navire de la même façon que les autres données.

Pour l'une de nos preuves de concept, il était question de proposer une approche pour alerter les opérateurs de bord lorsqu'une attaque par leurrage ou brouillage GNSS était en cours. Cette approche se base sur l'analyse de trames NMEA spécifiques et de nouvelles trames sont générées pour alerter l'opérateur via une extension de l'ECDIS qu'une attaque est justement en cours. En guise d'amélioration, l'un des points à développer serait notamment d'explorer d'autres trames indiquant que d'autres types d'attaques sont perpétrées.

Concernant les algorithmes utilisés tout au long des différentes phases de détection d'anomalies, il serait intéressant de proposer d'autres d'approches de détection qui seraient adaptés à ce type de données. L'utilisation des algorithmes d'apprentissage automatique non supervisés spé-

1. https ://opencpn.org/wiki/dokuwiki/doku.php ?id=opencpn :opencpn_user_manual :advanced_features :nmea_sentences

cifiquement utilisés pour la classification à une classe est selon nous une partie intéressante. Les données recueillies et utilisées pour les expériences ne sont pas équilibrées (en termes de comportement normal/anormal, avec une grande proportion de données dites "normales") c'est-à-dire que l'emploi de méthodes d'apprentissage automatique avec des algorithmes supervisés ne serait pas adapté au risque de faire du surapprentissage biaisant les résultats. Il serait avantageux de rendre les données collectées plus exploitables avec des analyses plus poussées au niveau algorithmique. Cela étant, l'utilisation de certains algorithmes d'apprentissage non supervisés à une classe ont été adaptés à cette problématique, mais il serait bon d'explorer d'autres algorithmes en optimisant de façon identique les hyperparamètres pour une comparaison équitable. Pour une diversité de systèmes tous interconnectés à des niveaux différents, l'utilisation de méthodes émergentes comme le Federated Learning [23] pourrait être judicieux sur ce type d'architecture en termes de stratégie de détection plus globalisée.

Pour la détection d'anomalies, nous avons également proposé une approche multirésolution basée sur des méthodes de détection de discontinuités et de changements locaux des données au cours du temps, qui sont attribuées aux cyberattaques. Nous partons du fait que ces événements, s'ils sont le résultat d'attaques, doivent persister à plusieurs niveaux de résolution des séries temporelles associées aux données à analyser. Les résultats de détection sur des données issues des ICS, obtenues par l'opérateur d'énergie de Teager-Kaiser (TK) et de l'opérateur de dérivation sont prometteurs et en particulier ceux de l'opérateur TK. Également, ces résultats montrent aussi l'intérêt de l'analyse multirésolution des attaques, mais aussi soulèvent le problème, qui reste ouvert, celui du choix du nombre optimal pour l'analyse des anomalies. Ainsi, une méthode d'estimation du nombre optimal de résolutions (échelles) adaptée aux données, pour automatiser le processus de détection, mériterait d'être développée.

Comme cela a été identifié dans nos travaux, il n'y a pas réellement d'IDS qui soit spécifique aux systèmes cybernétiques navals, car ces derniers, en termes de fonctionnement, sont de plus en plus semblables aux systèmes IT. Les NIDS actuels ne prennent pas vraiment en compte à leur conception des règles de détection dédiées aux attaques sur les ICS et les systèmes de navigation (même si des projets émergent, surtout pour la partie industrielle qui est plus connue, car elle ne se cantonne pas qu'au monde maritime et se trouve bien présente tous secteurs confondus). En revanche des projets pour mettre en place des règles spécifiques basées sur des sondes open source sont en cours de développement dans le domaine des automates industriels. En effet, le problème ne vient pas réellement des NIDS mais plutôt du manque d'éditeurs de signatures de détection qui se fait cruellement sentir (à l'heure actuelle, seules des règles concernant le protocole industriel ModBus existent en sources ouvertes). Par ailleurs des NIDS spécialisés comme la sonde Nozomi [2] ont une politique orientée OT mais celles-ci sont realtivement coûteuses et donc peu accessibles. Concernant les données NMEA, il n'y a pas, à notre connaissance, de règles de détection spécifiques

2. https ://www.nozominetworks.com/

mettant en avant les caractéristiques des données NMEA tous standards confondus et encore moins de sondes dédiées. C'est une piste de recherche qui mériterait aussi d'être prospectée.

En guise de conclusion et d'un point de vue pratique, toutes les expérimentations, développements d'outils et conceptions de systèmes embarqués peuvent être améliorés. Par exemple, si l'expérience BELAMY a permis de comprendre et d'identifier l'évolution des données de navigation basées sur le protocole NMEA-0183 lors d'une attaque par leurrage GNSS, nous n'avons pu réaliser que quelques scénarios d'attaque. Par ailleurs, les systèmes expérimentaux employés ne prenaient en compte que certains types de données NMEA-0183. Une version évoluée de ce type d'attaques, notamment avec du matériel plus récent utilisant le standard NMEA-2000, serait plus ambitieuse. Concernant les outils de génération d'attaques, s'ils ont suffi à générer un nombre d'attaques pendant nos expérimentations sur la plate-forme, il serait intéressant de poursuivre leur développement pour prendre en compte davantage d'attaques. Par exemple, nous n'avons pas automatisé via AEGIS la génération d'attaques sur les différentes IHM des systèmes industriels. Concernant la partie navigation, l'outil NAGE pourrait, dans une version future, prendre en compte d'autres types de trames comme celles concernant les équipements intégrés à la navigation. La génération d'attaques plus subtiles pourrait permettre de tester davantage les systèmes de détection. Enfin, l'un des projets réalisés fut la conception du système embarqué HAPPINESS (qui se trouve être aujourd'hui en plusieurs exemplaires sur différents bateaux). Le développement de ce système mériterait d'être encore amélioré avec des capacités de collecte de données plus puissantes permettant ainsi leur installation sur des navires de grandes dimensions. Même si à l'heure actuelle, ce projet permet de rendre mobile la plate-forme et de collecter facilement et en quantité suffisante des données de navigation, il y a de toute évidence une liste non exhaustive de points à perfectionner comme la portée des systèmes de réception, la qualité des capteurs, l'augmentation de l'autonomie ou l'ajout de caméras.

L'ensemble de ces pistes ont été autant de défis très stimulants dans ce parcours de thèse au sein d'une équipe soudée et dynamique. Participer à un pan, aussi petit soit-il, de ce grand challenge que représente la sécurisation cyber du secteur maritime a montré que le travail est colossal à l'échelle du jeune chercheur et reste immense à l'échelle de la première industrie du monde, le transport maritime. Et cela sans même aborder la question des navires militaires. Pour l'ensemble des navires, et cela dans un contexte géopolitique propice à ces attaques, l'enjeu pour les marins qui risquent leur vie quotidiennement, qu'ils soient de commerce ou militaires, est d'aider à la meilleure compréhension de leur environnement immédiat, le navire et de leur environnement élargi, la mer. Et même en mer, nous l'avons vu, la cybersécurité n'est qu'à son début.

VII.4 Acronymes

Voici les différentes abréviations utilisées tout au long du manuscrit : :

AEGIS : *Attack and Exploit Generator on Industrial control Systems.*

AI : *Artificial Intelligence.*

AIS : *Automatic Identification System.*

ANSSI : *Agence Nationale de la Sécurité des Systèmes d'Information.*

AUV : *Autonomous Underwater Vehicles - Robot sous-marins autonomes.*

BELAMY : *Basic Experimentation of Light spoofing Attack on Maritime sYsteme.*

BIMCO : *Baltic and International Maritime Council.*

CAN : *Controller Area Network.*

CCTV : *Closed-Circuit Television.*

COSCO : *China Ocean SHipping COmpagny.*

CMS : *Combat Management SYstem.*

CPS : *Cyber-Physical System.*

C4ADS : *Center for Advanced Defence Studies.*

DCS : *Distributed Control System.*

DDoS : *Distributed Denial of Service.*

DoS : *Denial of Service.*

ECDIS : *Electronic Chart Display Information System.*

ECS : *Electronic Chart System.*

EW : *Electronic Warfare.*

FCS : *Fire Control System.*

FTP : *File Transfer Porotocol.*

GRU : *direction générale des renseignements de Russie.*

GPIO : *General Purpose Input Ouput.*

GNSS : *Global Navigation Satellite System.*

GNL : *Gaz Naturel Liquefié.*

GPS : *Global Positioning System.*

HIDS : *Host Intrusion Detection System.*

HAPPINESS : *Hollistic APProach of Integreted Equipment for cyberSecurity at Sea.*

HDOP : *Horizontal Dilution of Precision.*

IAEA : *International Atomic Energy Agency.*

IARPA : *Intelligence Advanced Research Projects Activity.*

I2C : *Inter Integrated Circuit.*

ICMP : *Internet Control Message Protocol.*

IDES : *Intrusion Detection Expert System.*

IDS : *Intrusion Detection System.*

IEC : *International Electrotechnical Commission.*

IETM : .

IF : *Isolation Forest.*

IHM : *Interface Homme-Machine.*

IMO : *International Maritime Organisation.*

INS : *Integrated Navigation Systems.*

IoT : *Internet of Things.*

IP : *Internet Protocol.*

IPS : *Intrusion Prevention System.*

ISO : *International Organization for Standardization.*

IT : *Informationnal Technology.*

IRNSS : *Indian Regional Navigation Satellite System.*

LOF : *Local Outlier Factor.*

M-CERT : *Maritime Computer Emergency Response Team.*

MICA : *Maritime Information, Cooperation and Awareness center.*

NAGE : *NMEA Attack Generator Engine.*

NIDS : *Network Intrusion Detection System.*

NMAP : *Network Mapper.*

NMEA : *National Marine Electronics Association.*

MMSI : *Maritime Mobile Service Identity.*

MITM : *Man In The Middle.*

NSA : *National Security Agency.*

NIDS : *Network INtrusion Detection System.*

NIST : *National Institute of Standards and Technology.*

OMI : *International Maritime Organization.*

OT : *Operationnal Technology.*

PLC : *Programmable Logic Controller.*

PNT : *Positioning Navigation Timing.*

QZSS : *Quasi-Zenith Satellite System.*

RC : *Robust Covariance.*

RF : *Radio Fréquence.*

ROV : *Remotely Operated Vehicle.*

RSB : *Rapport Signal sur Bruit.*

SCADA : *Supervisory Control and Data Acquisition.*

SNMP : *Simple Network Management Protocol.*

SQL : *Structured Query Language.*

SIEM : *Security Information and Event Management.*

SSAS : *Ship Security Alert System.*

SVM : *Support Vector Machine.*

UAV : *Unmanned Aerial Vehicle.*

VDR : *Voyage Data Recorder.*

VDOP : *Vertical Dilution of Precision.*

VHF : *Very High Frequency.*

VPN : *Virtual Private Network.*

VSAT : *Very Small Aperture Terminal.*

Bibliographie

[1] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shiang, Johari Abdullah, and Farhan Ahmad. Network intrusion detection system : A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1) :e4150, 2021.

[2] Nurkhodzha Akbulaev and Gadir Bayramli. Maritime transport and economic growth : Interconnection and influence : an example of the countriesin the caspian sea coast ; russia, azerbaijan, turkmenistan, kazakhstan and iran. *Marine policy*, 118 :104005, 2020.

[3] Frank Akpan, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis, and Michalis Michaloliakos. Cybersecurity challenges in the maritime sector. *Network*, 2(1) :123–138, 2022.

[4] Sumayah Al-Rabiaah. The "stuxnet" virus of 2010 as an example of a "apt" and its "recent" variances. In *2018 21st Saudi Computer Society National Computer Conference (NCC)*, pages 1–5. IEEE, 2018.

[5] Amaal Al Shorman, Hossam Faris, and Ibrahim Aljarah. Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for iot botnet detection. *Journal of Ambient Intelligence and Humanized Computing*, 11(7) :2809–2825, 2020.

[6] W Laftah Al-Yaseen. Improving intrusion detection system by developing feature selection model based on firefly algorithm and support vector machine. *IAENG International Journal of Computer Science*, 46(4) :534–540, 2019.

[7] Emin Aleskerov, Bernd Freisleben, and Bharat Rao. Cardwatch : A neural network based database mining system for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)*, pages 220–226. IEEE, 1997.

[8] Omar Alghushairy, Raed Alsini, Xiaogang Ma, and Terence Soule. Improving the efficiency of genetic-based incremental local outlier factor algorithm for network intrusion detection. In *Advances in Artificial Intelligence and Applied Cognitive Computing*, pages 1011–1027. Springer, 2021.

[9] Tejasvi Alladi, Vinay Chamola, and Sherali Zeadally. Industrial control systems : Cyberattack trends and countermeasures. *Computer Communications*, 155 :1–8, 2020.

[10] James P Anderson. Computer security technology planning study. Technical report, ANDER-

SON (JAMES P) AND CO FORT WASHINGTON PA FORT WASHINGTON, 1972.

[11] James P Anderson. Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Company*, 1980.

[12] Andrej Androjna, Tanja Brcko, Ivica Pavic, and Harm Greidanus. Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10) :776, 2020.

[13] Andrej Androjna, Marko Perkovič, Ivica Pavic, and Jakša Mišković. Ais data vulnerability indicated by a spoofing case-study. *Applied Sciences*, 11(11) :5015, 2021.

[14] A.O. Boudraa and F. Salzenstein. Teager–Kaiser energy methods for signal and image analysis : A review. *Dig. Sig. Proc.,*, 78 :338–375, 2018.

[15] Amin Azmoodeh, Ali Dehghantanha, and Kim-Kwang Raymond Choo. Big data and internet of things security and forensics : Challenges and opportunities. *Handbook of Big Data and IoT Security*, pages 1–4, 2019.

[16] Urvashi Bansal et al. A review on ransomware attack. In *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, pages 221–226. IEEE, 2021.

[17] P. Barford, M. Dacier, T.G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, S. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen. Cyber sa : situational awareness for cyber defense. In *Cyber situational awareness*, pages 3–13. Springer, 2010.

[18] Zachry Basnight, Jonathan Butts, Juan Lopez Jr, and Thomas Dube. Firmware modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, 6(2) :76–84, 2013.

[19] Mohamed Amine Ben Farah, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. Cyber security in the maritime industry : a systematic survey of recent advances and future trends. *Information*, 13(1) :22, 2022.

[20] Michael W Berry, Azlinah Mohamed, and Bee Wah Yap. *Supervised and unsupervised learning for data science*. Springer, 2019.

[21] D. Blauwkamp, T.D. Nguyen, and G.G. Xie. Toward a deep learning approach to behavior-based ais traffic anomaly detection. In *DYNAMICS Workshop, San Juan.*, pages 1–10, 2018.

[22] Nor Afiq Bonandir, Norziana Jamil, Md Nabil Ahmad Nawawi, Razali Jidin, Mohd Ezanee Rusli, Lam Kwok Yan, and Loviana Lenyu Anak Dunstan Maudau. A review of cyber security assessment (csa) for industrial control systems (ics) and their impact on the availability of the ics operation. In *Journal of Physics : Conference Series*, volume 1860, page 012015. IOP Publishing, 2021.

[23] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingerman, Vladimir Ivanov, Chloe Kiddon, Jakub Konečnỳ, Stefano Mazzocchi, Brendan McMahan, et al. Towards federated learning at scale : System design. *Proceedings of Machine Learning and Systems*, 1 :374–388, 2019.

[24] Clet Boudehenn, Olivier Jacq, Maxence Lannuzel, Jean-Christophe Cexus, and Abdel Bou-

draa. Navigation anomaly detection : An added value for Maritime Cyber Situational Awareness. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–4. IEEE, 2021.

[25] Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, and Jörg Sander. Lof : Identifying density-based local outliers. In *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data*, SIGMOD '00, page 93–104, New York, NY, USA, 2000. Association for Computing Machinery.

[26] Scott Steele Buchanan. Cyber-attacks to industrial control systems since stuxnet : A systematic review. 2022.

[27] Joe Burton. Cyber attacks and maritime situational awareness evidence from japan and taiwan. In *2016 International Conference on Cyber Situational Awareness, Data analytics and Assessment (CyberSA)*, pages 1–4. IEEE, 2016.

[28] N. A. Campbell. Robust procedures in multivariate analysis i : Robust covariance estimation. *Journal of the Royal Statistical Society : Series C (Applied Statistics)*, 29(3) :231–237, 1980.

[29] Steven L Caponi and Kate B Belmont. Maritime cybersecurity : a growing threat goes unanswered. *Intellectual Property & Technology Law Journal*, 27(1) :16, 2015.

[30] Brent Carrara and Carlisle Adams. A survey and taxonomy aimed at the detection and measurement of covert channels. In *Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security*, pages 115–126, 2016.

[31] Jean-Christophe Cexus, AO Boudraa, Alexandre Baussard, FH Ardeyeh, and EHS Diop. 2d cross-ψ b-energy operator for images analysis. In *2010 4th International Symposium on Communications, Control and Signal Processing (ISCCSP)*, pages 1–4. IEEE, 2010.

[32] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection : A survey. *ACM Computing Surveys*, 41(3) :1–58, 2009.

[33] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection : A survey. *ACM computing surveys (CSUR)*, 41(3) :1–58, 2009.

[34] Samrat Chatterjee and Shital Thekdi. An iterative learning and inference approach to managing dynamic cyber vulnerabilities of complex systems. *Reliability engineering & system safety*, 193 :106664, 2020.

[35] J Csorba and N Husteli. Securing your control systems : overcoming vulnerabilities. *Proceedings of the Marine Safety and Security Council, Coast Guard Journal of Safety and Security at Sea*, 71(4), 2014.

[36] Moritz Schulze Darup. Verschlüsselte regelung in der cloud–stand der technik und offene probleme. *at-Automatisierungstechnik*, 67(8) :668–681, 2019.

[37] Dorothy E Denning. An intrusion-detection model. *IEEE Transactions on software engineering*, (2) :222–232, 1987.

[38] Joseph DiRenzo, Dana A Goward, and Fred S Roberts. The little-known challenge of maritime cyber security. In *2015 6th International Conference on Information, Intelligence, Systems*

and Applications (IISA), pages 1–5. IEEE, 2015.

[39] Georg Disterer. Iso/iec 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2), 2013.

[40] Jose R Dorronsoro, Francisco Ginel, C Sgnchez, and Carlos S Cruz. Neural fraud detection in credit card operations. *IEEE transactions on neural networks*, 8(4) :827–834, 1997.

[41] Wenli Duo, MengChu Zhou, and Abdullah Abusorrah. A survey of cyber attacks on cyber physical systems : Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5) :784–800, 2022.

[42] Francis Ysidro Edgeworth. Xli. on discordant observations. *The london, edinburgh, and dublin philosophical magazine and journal of science*, 23(143) :364–375, 1887.

[43] Oliver Fitton, Daniel Prince, Basil Germond, and Mark Lacy. The future of maritime cyber security. 2015.

[44] Jean-Marie Flaus. *Cybersecurity of industrial systems*. John Wiley & Sons, 2019.

[45] Antoine Frémont. Maritime transport : The threat of de-globalization ? *Futuribles*, 445(6) :63–86, 2021.

[46] Michael G Frodl. Pirates exploiting cybersecurity weaknesses in maritime industry. *National Defense*, 96(702) :22–23, 2012.

[47] Ryohei Fujimaki, Takehisa Yairi, and Kazuo Machida. An approach to spacecraft anomaly detection problem using kernel feature space. In *Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining*, pages 401–410, 2005.

[48] Rose George. *Ninety percent of everything : Inside shipping, the invisible industry that puts clothes on your back, gas in your car, and food on your plate*. Macmillan, 2013.

[49] Anup K Ghosh, Aaron Schwartzbard, Michael Schatz, et al. Using program behavior profiles for intrusion detection. In *Proceedings of the SANS Intrusion Detection Workshop*. Citeseer, 1999.

[50] Dennis Göge and Hans-Christof Enge. Look-out 2016 maritime domain cyber : Risks, threats & future perspectives. *Lampe & Schwartze KG*, 2015.

[51] Alan Grant, Paul Williams, Nick Ward, and Sally Basker. Gps jamming and the impact on maritime navigation. *Journal of Navigation*, 62(02) :173–187, 2009.

[52] Alan Grant, Paul Williams, Nick Ward, and Sally Basker. Gps jamming and the impact on maritime navigation. *The Journal of Navigation*, 62(2) :173–187, 2009.

[53] Adam Hahn. Operational technology and information technology in industrial control systems. In *Cyber-security of SCADA and other industrial control systems*, pages 51–68. Springer, 2016.

[54] David Hambling. Gps fail : how a little black box could cause chaos. *New Scientist*, 209(2803) :44–47, 2011.

[55] Song Han, Miao Xie, Hsiao-Hwa Chen, and Yun Ling. Intrusion detection in cyber-physical systems : Techniques and challenges. *IEEE systems journal*, 8(4) :1052–1062, 2014.

[56] Christopher R Hayes. *Maritime cybersecurity : the future of national security*. PhD thesis,

Monterey, California : Naval Postgraduate School, 2016.

[57] Hongxing He, Jincheng Wang, Warwick Graco, and Simon Hawkins. Application of neural networks to detection of medical fraud. *Expert systems with applications*, 13(4) :329–336, 1997.

[58] Hui Hu and Na Wei. A study of gps jamming and anti-jamming. In *2009 2nd international conference on power electronics and intelligent transportation system (PEITS)*, volume 1, pages 388–391. IEEE, 2009.

[59] Mamoona Humayun, NZ Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. Internet of things and ransomware : Evolution, mitigation and prevention. *Egyptian Informatics Journal*, 22(1) :105–117, 2021.

[60] L Ingham. Drones at sea : automated cargo ships to set sail by 2035, 2014.

[61] O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, and J. Simonin. Detecting and hunting cyberthreats in a maritime environment : Specification and experimentation of a maritime cybersecurity operations centre. In *2nd Cyber Security in Networking Conference, IEEE (CSNet)*, pages 1–8, 2018.

[62] Olivier Jacq. *Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la Cyber Situational Awareness du monde maritime.* PhD thesis, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire, 2021.

[63] Lars Jensen. Challenges in maritime cyber-resilience. *Technology Innovation Management Review*, 5(4) :35, 2015.

[64] Wang Jia, Yang Xiao, Tieshan Li, and C. Chen. Impacts of gps spoofing on path planning of unmanned surface ships. *Electronics*, 11 :801, 03 2022.

[65] Anita K Jones and Robert S Sielken. Computer system intrusion detection : A survey. *Computer Science Technical Report*, pages 1–25, 2000.

[66] Kevin D Jones, Kimberly Tam, and Maria Papadaki. Threats and impacts in maritime cyber security. 2016.

[67] Leslie Pack Kaelbling, Michael L Littman, and Andrew W Moore. Reinforcement learning : A survey. *Journal of artificial intelligence research*, 4 :237–285, 1996.

[68] J.F. Kaiser. On a simple algorithm to calculate the 'energy' of a signal. In *Proc. ICASSP*, pages 381–384, 1990.

[69] A Karaś. Smart port as a key to the future development of modern ports. *TransNav : International Journal on Marine Navigation and Safety of Sea Transportation*, 14(1), 2020.

[70] Anastasis Keliris, Charalambos Konstantinou, Nektarios Georgios Tsoutsos, Raghad Baiad, and Michail Maniatakos. Enabling multi-layer cyber-security assessment of industrial control systems through hardware-in-the-loop testbeds. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 511–518, 2016.

[71] Omera Khan and Daniel A Sepúlveda Estay. Supply chain cyber-resilience : Creating an agenda for future research. *Technology Innovation Management Review*, 5(4), 2015.

[72] Seung Hyun Kim, Qiu-Hong Wang, and Johannes B Ullrich. A comparative study of cyberattacks. *Communications of the ACM*, 55(3) :66–73, 2012.

[73] G Klocker. Cyber risks a threats : a demanding challenge for the maritime industry. *Look-Out-2016 Maritime Domain Cyber : Risks, Threats & Future Perspectives*, 2015.

[74] Sotiris B Kotsiantis, Ioannis Zaharakis, P Pintelas, et al. Supervised machine learning : A review of classification techniques. *Emerging artificial intelligence applications in computer engineering*, 160(1) :3–24, 2007.

[75] Kristen Kuhn, Salih Bicakci, and Siraj Ahmed Shaikh. Covid-19 digitization in maritime : understanding cyber risks. *WMU Journal of Maritime Affairs*, 20(2) :193–214, 2021.

[76] Rajesh Kumar, Rohan Kela, Siddhant Singh, and Rolando Trujillo-Rasua. Apt attacks on industrial control systems : A tale of three incidents. *International Journal of Critical Infrastructure Protection*, 37 :100521, 2022.

[77] B. Lamrini, A. Gjini, S. Daudin, F. Armando, P. Pratmarty, and L. Trave-Massuyes. Anomaly detection using similarity-based one-class svm for network traffic characterization. In *Proc. 29th International Workshop on Principles of Diagnosis*, pages 1–8, 2018.

[78] Terran Lane, Carla E Brodley, et al. Sequence matching and learning in anomaly detection for computer security. In *AAAI Workshop : AI Approaches to Fraud Detection and Risk Management*, pages 43–49. Providence, Rhode Island, 1997.

[79] R. Langner. Stuxnet : Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9 :49–51, 05 2011.

[80] Paul B Larsen. International regulation of global navigation satellite systems. *J. Air L. & Com.*, 80 :365, 2015.

[81] Xue Li and Kum Fai Yuen. Autonomous ships : A study of critical success factors. *Maritime Economics & Logistics*, pages 1–27, 2022.

[82] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system : A comprehensive review. *Journal of Network and Computer Applications*, 36(1) :16–24, 2013.

[83] W. Lin, Ch. Hamilton, and P. Chitrapu. A generalization to the Teager-Kaiser energy function application to resolving two closely-spaced tones. In *Proc. ICASSP*, pages 1637–1640, 1995.

[84] Fei Tony Liu, Kai Ming Ting, and Zhi-Hua Zhou. Isolation forest. In *2008 Eighth IEEE International Conference on Data Mining*, pages 413–422, 2008.

[85] Eric Luiijf. *Threats in Industrial Control Systems*, pages 69–93. 08 2016.

[86] Mass Soldal Lund, Odd Sveinung Hareide, and Øyvind Jøsok. An attack on an integrated navigation system. 2018.

[87] Batta Mahesh. Machine learning algorithms-a review. *International Journal of Science and Research (IJSR).[Internet]*, 9 :381–386, 2020.

[88] Scott Manson and Dwight Anderson. Cybersecurity for protection and control systems : An overview of proven design solutions. *IEEE Industry Applications Magazine*, 25(4) :14–23,

2019.

[89] Goncalo Martins, Sajal Bhatia, Xenofon Koutsoukos, Keith Stouffer, CheeYee Tang, and Richard Candell. Towards a systematic threat modeling approach for cyber-physical systems. In *2015 Resilience Week (RWS)*, pages 1–6. IEEE, 2015.

[90] C Masala and K Tsetsos. A demanding challenge for the maritime industry. *Look-Out-2016 Maritime Domain Cyber : Risks, Threats & Future Perspectives*, 2015.

[91] Duncan McCrory. Russian electronic warfare, cyber and information operations in ukraine : Implications for nato and security in the baltic states. *The RUSI Journal*, 165(7) :34–44, 2020.

[92] Michael McFail, Jordan Hanna, and Daniel Rebori-Carretero. Detection engineering in industrial control systems. ukraine 2016 attack : Sandworm team and industroyer case study. Technical report, MITRE CORP MCLEAN VA, 2022.

[93] B. McGuinness and L. Foy. A subjective measure of SA : the crew awareness rating scale (CARS). In *First human performance, situation awareness, and automation conference*, volume 16, pages 286–291, 2000.

[94] Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5) :1039–1057, 2016.

[95] Stephen McLaughlin, Charalambos Konstantinou, Xueyang Wang, Lucas Davi, Ahmad-Reza Sadeghi, Michail Maniatakos, and Ramesh Karri. The cybersecurity landscape in industrial control systems. *Proceedings of the IEEE*, 104(5) :1039–1057, 2016.

[96] PH Meland, K Bernsmed, E Wille, ØJ Rødseth, and DA Nesheim. A retrospective analysis of maritime cyber security incidents. *TransNav : International Journal on Marine Navigation and Safety of Sea Transportation*, 15, 2021.

[97] Pedro Merino Laso. *Détection de dysfonctionements et d'actes malveillants basée sur des modèles de qualité de données multi-capteurs*. Theses, Ecole nationale supérieure Mines-Télécom Atlantique, December 2017.

[98] Joan Mileski, Christopher Clott, and Cassia Bomer Galvao. Cyberattacks on ships : a wicked problem approach. *Maritime Business Review*, 2018.

[99] M Murrison. Maritime industry slowly embracing potential of iot. *Internet of Business*, 2016.

[100] Anna Nagurney and Shivani Shukla. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, 260(2) :588–600, 2017.

[101] Lee Neitzel and Bob Huba. Top ten differences between ics and it cybersecurity. *InTech*, 61(3) :12–18, 2014.

[102] Marshall E Newberry. Maritime critical infrastructure cyber risk. *Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council*, 71(4), 2014.

[103] Carlton Northern, Kathleen Mayfield, Robert Benito, and Michelle Casagni. Handbook for implementing agile in department of defense information technology acquisition. Technical

report, MITRE CORP MCLEAN VA, 2010.

[104] Harun Oz, Ahmet Aris, Albert Levi, and A Selcuk Uluagac. A survey on ransomware : Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 2021.

[105] Cédric Pernet. *Sécurité et espionnage informatique : Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage.* Editions Eyrolles, 2015.

[106] François Peyret, Pierre-Yves Gilliéron, Laura Ruotsalainen, Jesper Engdahl, David Bétaille, Philippe Bonnifait, Nuria Delgado, Vassilis Gikas, Michal Hodon, and Shaojun Feng. Better use of global satellite systems for safer and greener transport. 09 2015.

[107] J Pietrzykowski, Z Pietrzykowski, and J Hajduk. Operations of maritime autonomous surface ships. *TransNav : International Journal on Marine Navigation and Safety of Sea Transportation*, 13, 2019.

[108] Derek A Pisner and David M Schnyer. Support vector machine. In *Machine learning*, pages 101–121. Elsevier, 2020.

[109] Nineta Polemi and Spyros Papastergiou. Current efforts in ports and supply chains risk assessment. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 349–354. IEEE, 2015.

[110] Jeff Radgowski and Katherine Tiongson. Cyberspace—the imminent operational domain. *Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council*, 71(4), 2014.

[111] C. Ray, R. Gallen, C. Iphar, A. Napoli, and A. Bouju. Deais project : detection of ais spoofing and resulting risks. In *OCEANS 2015 - MTS/IEEE*, pages 1–6, 2015.

[112] Xuanle Ren, Ronald D Blanton, and Vítor Grade Tavares. A learning-based approach to secure jtag against unseen scan-based attacks. In *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 541–546. IEEE, 2016.

[113] Maria Riveiro, Giuliana Pallotta, and Michele Vespe. Maritime anomaly detection : A review. *Wiley Interdisciplinary Reviews : Data Mining and Knowledge Discovery*, 8 :e1266, 05 2018.

[114] Jean-Paul Rodrigue. The vulnerability and resilience of the global container shipping industry. *Current History*, 121(831) :17–23, 2022.

[115] Dinesh Sathyamoorthy. Global navigation satellite system(gnss) spoofing : A review of growing risks and mitigation steps. *Defence S&T Technical Bulletin*, 6(1) :42–61, 2013.

[116] Andreas Schmidt. The estonian cyberattacks. *A fierce domain : Conflict in cyberspace*, 2012 :174–193, 1986.

[117] Carl Schuett, Jonathan Butts, and Stephen Dunlap. An evaluation of modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, 7(1) :61–68, 2014.

[118] H.J. Shin, D.H. Eom, and S.S. Kim. One-class support vector machines—an application in machine fault detection and classification. *Computers & Industrial Engineering*, 48(2) :395–408, 2005.

[119] Jinsoo Shin, Hanseong Son, Gyunyoung Heo, et al. Development of a cyber security risk model using bayesian networks. *Reliability Engineering & System Safety*, 134 :208–217, 2015.

[120] Franck Sicard. *Prise en compte des risques de cyber-attaques dans le domaine de la sécurité des systèmes cyber-physiques : proposition de mécanismes de détection à base de modèles comportementaux*. PhD thesis, 10 2018.

[121] Franck Sicard, Estelle Hotellier, and Julien Francq. An industrial control system physical testbed for naval defense cybersecurity research. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 413–422. IEEE, 2022.

[122] Franck SICARD, Éric ZAMAI, and Jean-Marie FLAUS. An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. *Reliability Engineering System Safety*, 188 :584–603, 2019.

[123] A. Siraj and R.B. Vaughn. Multi-level alert clustering for intrusion detection sensor data. pages 748 – 753, 07 2005.

[124] Shamika N Sirimanne, J Hoffman, W Juan, R Asariotis, M Assaf, G Ayala, H Benamara, D Chantrel, J Hoffmann, A Premti, et al. Review of maritime transport 2019. In *United Nations Conference on Trade and Development, Geneva, Switzerland*, 2019.

[125] Roman Smierzchalski. Evolutionary trajectory planning of ships in navigation traffic areas. *Journal of marine science and technology*, 4(1) :1–6, 1999.

[126] Dongping Song. A literature review, container shipping supply chain : Planning problems and research opportunities. *Logistics*, 5(2) :41, 2021.

[127] K. Stouffer, J. Falco, and K. Kent. Guide to supervisory control and data acquisition (scada) and industrial control systems security. 01 2006.

[128] Keith Stouffer, Joe Falco, Karen Scarfone, et al. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82) :16–16, 2011.

[129] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. Mitre att&ck : Design and philosophy. In *Technical report*. The MITRE Corporation, 2018.

[130] Xiaoling Tao, Yang Peng, Feng Zhao, Peichao Zhao, and Yong Wang. A parallel algorithm for network traffic anomaly detection based on isolation forest. *International Journal of Distributed Sensor Networks*, 14(11) :1550147718814471, 2018.

[131] Nida Tariq. Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, 23(2) :1–11, 2018.

[132] Q.A. Tran, H. Duan, and X. Li. One-class support vector machine for anomaly network traffic detection. *China Education and Research Network (CERNET)*, 310 :1–6, 2004.

[133] Brett van Niekerk. Analysis of cyber-attacks against the transportation sector. In *Cyber Security and Threats : Concepts, Methodologies, Tools, and Applications*, pages 1384–1402. IGI Global, 2018.

[134] Eric York Wallischeck et al. Ics security in maritime transportation : a white paper examining

the security and resiliency of critical transportation infrastructure. Technical report, John A. Volpe National Transportation Systems Center (US), 2013.

[135] Y. Wang, J. Liu, C. Yang, L. Zhou, Sh. Li, and Zh. Xu. Access control attacks on plc vulnerabilities. *J. Comput. Comm.*, 06 :311–325, 01 2018.

[136] Gregory C Wilshusen. Maritime critical infrastructure protection : Dhs needs to enhance efforts to address port cybersecurity. Technical report, 2015.

[137] Feng Xia, Laurence T Yang, Lizhe Wang, and Alexey Vinel. Internet of things. *International journal of communication systems*, 25(9) :1101, 2012.

[138] Luo Xu, Qinglai Guo, Yujie Sheng, SM Muyeen, and Hongbin Sun. On the resilience of modern power systems : A comprehensive review from the cyber-physical perspective. *Renewable and Sustainable Energy Reviews*, 152 :111642, 2021.

[139] Ran Yan, Shuaian Wang, Lu Zhen, and Gilbert Laporte. Emerging approaches applied to maritime transport research : Past and future. *Communications in Transportation Research*, 1 :100011, 2021.

[140] Tianlei Zang, Shibin Gao, Baoxu Liu, Tao Huang, Tao Wang, and Xiaoguang Wei. Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks. *Reliability Engineering & System Safety*, 189 :232–241, 2019.

[141] Kexiong Curtis Zeng, Yuanchao Shu, Shinan Liu, Yanzhi Dou, and Yaling Yang. A practical gps location spoofing attack in road navigation scenario. In *Proceedings of the 18th international workshop on mobile computing systems and applications*, pages 85–90, 2017.

[142] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. Taxonomy of cyber attacks on scada systems. 10 2011.

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Titre : **Génération de données pour l'analyse et la détection d'anomalies dans les systèmes cybernétiques navals**

Mots clés : Détection d'anomalie ; Génération de données ; Systèmes de Contrôles Industriels, Systèmes de Positionnement par Satellites, Système de Détection d'Intrusion, Cybersécurité Maritime

Résumé : De nos jours plus de 90% du transport de marchandises passent par les voies maritimes. Les systèmes navals représentent une part indéniablement stratégique pour le commerce international et les activités militaires. Les systèmes présents à bord sont de plus en plus informatisés de sorte à optimiser les capacités opérationnelles, la navigation, la gestion des opérations et les performances. Pour atteindre ces objectifs, les systèmes cybernétiques navals ont connu, au cours de la dernière décennie, une transformation numérique globale. De nos jours, les systèmes de l'information et les systèmes opérationnels ont fortement convergé en termes de fonctionnement. Cependant, ces changements majeurs ont rendu ces systèmes vulnérables et ont considérablement augmenté la surface d'attaques et les risques d'incidents. Ces systèmes sont d'ailleurs devenus une cible de choix pour les pirates informatiques au regard des préjudices potentiels. En conséquence, la prise en compte de ces vulnérabilités dans ce secteur mondialisé doit devenir une problématique de premier plan à en croire les enjeux stratégiques, économiques et géopolitiques.

Dans cette thèse nous proposons une méthodologie pour la génération de données réalistes dédiées à l'amélioration de la cybersécurité des systèmes cybernétiques navals. Dans ce sens, nous avons pu élaborer un certain nombre de scénarios de cyberattaques propres aux Systèmes de Contrôles Industriels ainsi que des cas de falsification GNSS à travers plusieurs cas d'études pour combler le manque de données dans le secteur. La génération de données réalistes nous a permis de proposer une méthodologie d'extraction de caractéristiques originale adaptée aux méthodes de détection d'anomalie dans le but d'améliorer les systèmes de détection d'intrusion. Au cours de ces recherches, nous nous sommes appuyés sur une plate-forme de simulation numérique représentant toute la partie fonctionnelle et opérationnelle que l'on peut retrouver à bord d'un navire. Par ailleurs, toutes les expériences réalisées et outils développer au cours de cette thèse viennent corroborer cette plate-forme qui propose un degré de réalisme dédié à la formation et à la communauté scientifique.

Title : Data generation for anomaly detection in naval cybernetics systems

Keywords : Anomaly detection; Data generation; Industrial Control Systems, GNSS, Intrusion Detection System, Maritime Cybersecurity

Absract : Nowadays, more than 90% of the goods transportation is made by sea. Naval systems are strategic part of international trade and military activities. Onboard systems are increasingly computerised to optimize operational capabilities, navigation, operations management and performance. To achieve these objectives, naval cyber systems have known a global digital transformation over the past decade. Today, information systems and operational systems have strongly converged in terms of operation. However, these major changes have made these systems vulnerable and have significantly increased the attack surface and risk of incidents. These systems have become a prime target for hackers in terms of potential harm. As a consequence, taking into account these vulnerabilities in this globalized sector must become a major issue considering the strategic, economic and geopolitical stakes.

In this thesis, we propose a methodology for the generation of realistic data to improve the cybersecurity of naval cybernetic systems. We have been able to develop a number of cyberattack scenarios specific to Industrial Control Systems as well as GNSS tampering cases through several case studies in response to the critical lack of data in the sector. The generation of realistic data allowed us to propose an original feature extraction methodology adapted to anomaly detection methods in order to improve intrusion detection systems capacities. We relied on a numerical simulation platform representing all the functional and operational capacities similar to a real ship. In addition, all the experiments and tools developed during this thesis support this platform which proposes a degree of realism dedicated to training and research community.