Modèle d'analyse et d'évaluation de la propagation d'anomalies dans les systèmes cyber-physiques maritimes

Nicolas Pelissero

DOCTORAT BRETAGNE LOIRE / MATHSTIC

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

THESE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM 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

Nicolas Pelissero

Modèle d'analyse et d'évaluation de la propagation d'anomalies dans les systèmes cyber-physiques maritimes

Thèse présentée et soutenue à Brest, le 25 janvier 2022
Unité de recherche : Lab-STICC – UMR CNRS 6285
Thèse N° : 2022IMTA0286

Rapporteurs avant soutenance :

Martine COLLARD	Professeure émérite, Université des Antilles
Joaquín GARCIA-ALFARO	Professeur, Télécom Sud Paris

Composition du Jury :

Président :	Laurent NANA	Professeur, Université de Bretagne Occidentale
Examinateurs :	Solange GHERNAOUTI	Professeure, Université de Lausanne
	Martine COLLARD	Professeure émérite, Université des Antilles
	Joaquín GARCIA-ALFARO	Professeur, Télécom Sud Paris
Dir. de thèse :	John PUENTES	Professeur, Institut Mines-Télécom Atlantique Bretagne Pays de la Loire
Encadrant de thèse :	Pedro MERINO LASO	Chargé de recherche, Ecole Nationale Supérieure Maritime

Invité(s)

Julien FRANCQ	Responsable recherche & innovation cybersécurité, Naval Group
Marc PENNAMEN	Responsable développement des offres et projets cybersécurité, Thales SIX

Table des matières

Table des figures

Liste des tableaux

Introduction

Sommaire

Cette introduction a pour objectif d'appréhender le sujet de la thèse en le positionnant vis-à-vis des domaines de recherche scientifique connexes. Ainsi, le contexte, la problématique, et les questions de recherches associés sont explicités. Un résumé des contributions scientifiques, théoriques et expérimentales, est de même présenté en dernière partie.

Contexte de la thèse

Ces dernières années, plusieurs destroyers T-45 de la *Royal Navy*[1] opéraient dans les eaux du golfe Arabo-Persique lorsque que leurs missions ont été subitement compromises. Pendant plusieurs heures, les navires sont à l'arrêt, comme paralysés. Cette avarie s'avère être une conséquence d'une défaillance électrique. L'équipage est alors plongé dans l'obscurité la plus totale. Évidemment, tous les systèmes maritimes embarqués cessent eux aussi de fonctionner. Des éléments directement impliqués dans la survie du navire, tels que les systèmes de propulsion ou le système d'armes, sont inopérants. Dans une zone où les conflits géopolitiques sont exacerbés [Kam18], les conséquences de cet incident auraient pu être critiques pour le navire, comme pour l'équipage.

1. Composante maritime de l'armée britannique

L'origine de cette défaillance a été explicitée en 2016 [2]. Le système de propulsion et de production d'électricité des destroyers T-45 est composé de deux turbines, et deux générateurs additionnels. Lorsque la température extérieure était trop importante, les systèmes de refroidissements associés aux 2 turbines n'étaient pas assez performants. Ce qui induisait leur surchauffe et leur arrêt. Les générateurs additionnels n'étant pas dimensionnés pour fournir la totalité de la puissance électrique nécessaire à bord, cela a engendré une panne électrique globale. Comment expliquer qu'un tel navire moderne [3], caractérisé par une technologie avancée, puisse subir une telle défaillance ? Pourquoi aucune solution n'a-t-elle permis à l'équipage d'anticiper cet incident et d'atténuer son impact ?

Une défaillance du système de production d'énergie s'est ainsi répercutée sur l'ensemble des systèmes à bord, on parle de *défaillance en cascade*. Bien que la source initiale ne soit pas d'origine *cyber*, nous pourrions facilement envisager qu'une cyberattaque génère une anomalie initiatrice similaire. La propagation d'anomalies engendrée est ainsi une conséquence du fort niveau de dépendances entre les systèmes maritimes embarqués. Cet incident souligne l'importance et la criticité de cette caractéristique.

La cybersécurité des systèmes maritimes est assurée par diverses solutions de *cyber-protection* mises en place dans l'architecture réseau associée. On y distingue une multitude d'outils (matériels ou logiciels), tels que des sondes de détection d'intrusion, de détection d'anomalies, des systèmes de gestion et de corrélation d'évènements, etc. L'ensemble des données et informations collectées est ensuite mis en perspective pour obtenir une vue tactique de la cybersécurité du système concerné. Cette vue tactique est alors supervisée par un opérateur dédié. Il est cependant difficile de collecter, de corréler, et d'analyser les sources d'informations disponibles afin de détecter les anomalies, et d'évaluer l'impact de leur propagation à l'échelle globale du navire. Cela est pourtant un besoin majeur pour réagir efficacement et proportionnellement, de manière logicielle ou humaine.

Il est donc primordial d'analyser la propagation d'anomalies dans les systèmes maritimes, et ce durant la totalité du cycle de vie du navire, à partir d'une solution adaptée aux besoins et contraintes du secteur maritime. Cette analyse doit à la fois se caractériser par une identification, une caractérisation, et une évaluation quantitative des chemins de propagation potentiels. Cela est d'autant plus critique au regard des conséquences majeures qui résultent de ces propagations.

2. Britain's Royal Navy warships are breaking down because sea is too hot. CNN. Consulté le 09 septembre 2021. `https://edition.cnn.com/2016/06/09/europe/britain-royal-navy-warships/index.html`

3. Les 6 navires de la classe T-45 ont été mis en service entre 2009 et 2013

Contexte de la problématique

De tout temps, le secteur maritime a été marqué par les différentes révolutions industrielles. De l'utilisation de la vapeur, jusqu'à l'automatisation d'opérations grâce à l'électronique et l'informatique, de nombreuses technologies de rupture ont transformé les navires. Cette transformation s'accompagne de gains capacitaires, mais induit également de nouveaux risques dont l'identification, l'analyse et la remédiation sont indispensables.

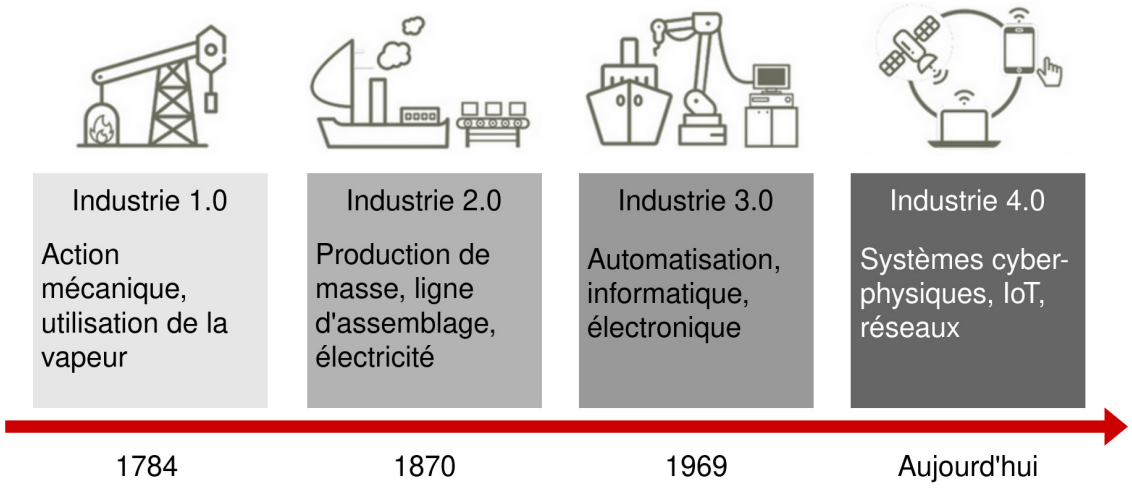


FIGURE 1: Révolutions industrielles associées au secteur maritime

Depuis une dizaine d'années, la forte numérisation du secteur maritime engendre une évolution majeure des navires. Cela est observable dans leurs modes de fonctionnement, mais surtout au niveau des équipements employés à bord. Que ce soit dans le secteur maritime civil, ou militaire, l'emploi d'équipements numériques permet de bénéficier de navires toujours plus performants en combinant une réduction significative des équipages.

L'émergence actuelle du maritime 4.0 [4] a introduit dans les navires l'utilisation de CPS (*Cyber Physical System*) (Figure 1). La dualité intrinsèque caractérisant ce type de système, permet de contrôler et de gérer numériquement diverses opérations physiques. Ces actions sont réalisées en temps réel à partir de divers éléments interdépendants tels que des automates, des capteurs, ou encore des actionneurs. À bord, ils sont associés à des fonctions extrêmement hétérogènes, de la plus basique à la plus critique, pour couvrir une grande partie du spectre fonctionnel d'un navire. À cause de leur fort niveau de dépendance, l'ensemble des CPS qui composent un navire ne peut être défini comme une agrégation de systèmes. La no-

4. Composante maritime de la 4ème révolution industrielle

tion de réseau multicouche [BBC+14] est davantage appropriée pour décrire leurs propriétés et contraintes inhérentes.

De par les vulnérabilités induites par leur dualité cyber-physique, les CPS présentent une surface d'attaque démultipliée. Des cyberattaques ou des attaques physiques sont des sources potentielles de perturbations du contrôle des opérations associées à ce type de système. Outre les vulnérabilités inhérentes de leurs caractéristiques, les CPS maritimes sont exposés à des vulnérabilités associées aux spécificités du secteur maritime : durée de conception et d'exploitation particulièrement longues, difficulté de mises à jour pour corriger les failles existantes, etc. Ces faiblesses caractérisent tout système informatique embarqué et sont exacerbées par des contraintes environnementales, physiques et technologiques. En raison de leur fort niveau de dépendance et leur emploi dans des fonctions critiques, les dysfonctionnements générés par l'exploitation (volontaire ou non) de ces vulnérabilités peuvent se propager et engendrer des conséquences critiques pour le navire. Le spectre des conséquences potentielles est vaste, de l'impact environnemental ou humain, à la destruction d'équipement, voire à la compromission de la mission du navire.

Il apparaît alors évident que la considération de la problématique d'évaluation de la propagation d'anomalies dans les CPS maritimes est un besoin majeur pour anticiper et restreindre les potentiels impacts induits par celles-ci. Cette problématique doit être étudiée grâce à une solution caractérisant les perspectives internes et externes des systèmes, tout en englobant les différentes étapes du cycle de vie du navire.

Objectifs des travaux et questions de recherche

L'objectif de cette thèse est de fournir des éléments de réponses à la problématique de recherche associée à l'évaluation de la propagation d'anomalies dans un CPS maritime, et ce comme conséquence induite de leur fort niveau de dépendance. Pour y répondre, trois questions de recherche, et une question de développement ont été identifiées pour appuyer les travaux de cette thèse :

1. **QR1 : Comment se caractérise la notion de dépendance dans un navire ?** Le premier objectif de cette thèse sera de définir les spécificités génériques des dépendances dans un navire, ainsi que ses éléments impliqués dans celles-ci. Cela permettra ensuite de définir, à l'échelle globale du navire, la criticité des dépendances associées aux CPS.

2. **QR2 : Quelle est la solution de modélisation la plus adaptée pour fournir une analyse structurelle des composants d'un CPS et des dépendances associées ?** Parmi l'ensemble des solutions existantes, nos travaux devront identifier la plus pertinente, et la plus adaptée, pour la visualisation et l'identification des dépendances. De surcroît, cette solution devra fournir une formulation mathématique suffisante à leurs analyses. Il sera aussi nécessaire de définir en amont les caractéristiques majeures et inhérentes aux CPS, afin de les considérer dans cette solution de modélisation. Cela permettra d'obtenir une modélisation générique applicable à d'autres domaines d'application que le maritime.
3. **QR3 : Comment évaluer la propagation d'anomalies dans un CPS ?** À partir de la solution de modélisation choisie dans la QR2, il sera nécessaire d'analyser et évaluer quantitativement les chemins potentiels de propagation d'anomalies. Pour répondre à cette question de recherche, il s'agira de proposer une méthode d'évaluation de la propagation basée sur la formulation mathématique du problème des dépendances dans un CPS.
4. **QD1 : En adéquation avec les QR2 et QR3, quel outil informatique peut être développé pour faciliter la modélisation et les analyses qui en découlent ?** Cela permettra d'automatiser la génération de la solution de modélisation (QR2), ainsi que de faciliter l'utilisation de différentes métriques pour évaluer la propagation d'anomalies (QR3).

Démarche et contributions de la thèse

Les contributions issues des travaux de recherche de cette thèse sont le résultat de l'union de trois domaines de recherche spécifiques appliqués aux spécificités du secteur maritime : les CPS, la propagation d'anomalies, et la théorie des graphes. Les zones d'intersections, illustrées dans la Figure 2, définissent les axes de recherche majeurs.

Dans le cadre de la **première question de recherche**, nous nous sommes focalisés sur les différents aspects de la notion de dépendance relative aux systèmes maritimes. Pour cela, nous avons dans un premier temps explicité les différentes propriétés et contraintes associées à ces systèmes. Par la suite, nous avons caractérisé de manière générique les principales dépendances constitutives d'un navire. Cela a été réalisé en considérant les perspectives interne et externe, inhérentes à tout système. Nous avons ainsi pu identifier la criticité

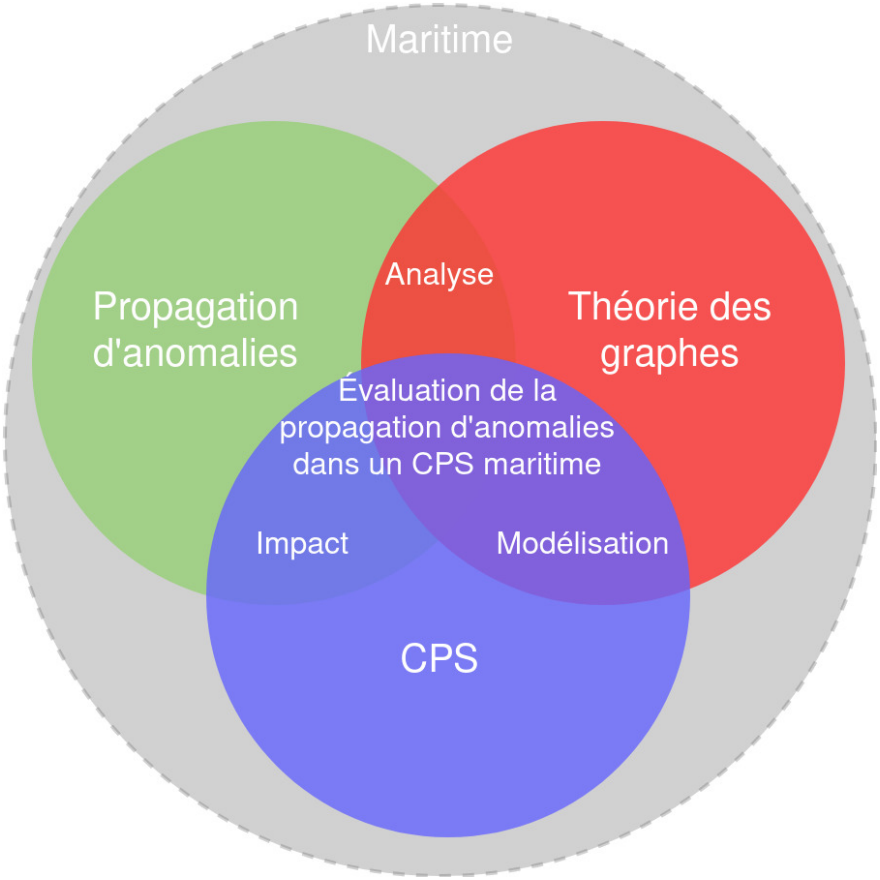


FIGURE 2: Domaines de recherche étudiés dans cette thèse

des dépendances associées aux CPS maritimes. Cela permet de mieux appréhender cette problématique à l'échelle globale du navire, tout en fournissant un regard éclairé sur leurs caractéristiques et propriétés, ainsi que les potentielles conséquences qui en résultent.

Pour répondre à la **deuxième question de recherche** sur l'analyse structurelle d'un CPS, nous avons formulé une modélisation spécifique basée sur la théorie des graphes. Le modèle de graphe orienté multicouche proposé permet de représenter les éléments du CPS, ainsi que les dépendances qui le caractérisent. Différentes métriques et propriétés du graphe sont directement exploitables dans divers cas d'étude, selon la problématique concernée. Une méthodologie spécifique à la génération du modèle a aussi été élaborée, et minutieusement détaillée. Cela facilite son implémentation dans d'autres domaines d'application relatifs aux CPS.

La **troisième question de recherche**, concernant l'évaluation de la propagation d'anomalies, a été traitée à partir d'une méthode d'évaluation quantitative des chemins de propagation. Celle-ci repose essentiellement sur un algorithme de parcours de graphe qui

bénéficie des propriétés d'orientation et pondération du modèle développé pour répondre à la QR2. Afin de fournir une évaluation représentative, une méthode de pondération spécifique a été développée en adéquation avec les caractéristiques des CPS maritimes. Les travaux de thèse proposés permettent de générer une cartographie, une identification, et une analyse des différents chemins de propagation d'anomalies induites par une attaque ou un dysfonctionnement. Le fait de considérer la propagation des anomalies, en plus de leur détection, représente un apport majeur pour répondre plus efficacement à la problématique de *cyberprotection* de ces systèmes. Dans un contexte maritime, l'importance de cet aspect est d'autant plus exacerbée au regard des potentielles conséquences qui résultent de ces anomalies.

Enfin, la **question de développement**, relative à l'outil de génération de la solution de modélisation et d'évaluation de la propagation, a été abordée en proposant une solution informatique qui facilite le processus d'interaction avec le graphe généré, associé au modèle proposé. Cela simplifie son utilisation dans diverses applications relatives au domaine de recherche des CPS. Celui-ci est basé sur un logiciel *open-source* de gestion de graphe. Il se caractérise par deux procédures principales d'interaction, en adéquation avec les besoins d'automatisation relatifs aux questions de recherche 1 et 2. La première procédure facilite la génération du graphe, en adéquation avec le modèle énoncé. Tandis que la deuxième procédure permet l'extraction de différentes métriques et propriétés du graphe. L'utilisateur peut ainsi directement les analyser, ou les intégrer dans diverses analyses connexes.

Pour illustrer l'approche proposée de modélisation d'une représentation structurelle des CPS, et d'évaluation de la propagation d'anomalies, nous avons défini **deux protocoles expérimentaux**. Les deux cas d'études concernent des CPS représentatifs du domaine d'application maritime. Chacun d'entre eux est associé à des risques majeurs, potentiellement critiques pour le navire ou l'équipage. Le premier cas d'étude est composé d'un prototype de CPS de la boucle « mobilité » du *Naval Cyber Range* de l'École Navale. Le deuxième cas d'étude est quant à lui associé à la simulation d'un CPS de distribution d'eau. Cette ressource étant particulièrement importante à bord d'un navire, l'étude de ce type de CPS est extrêmement pertinente. Différents scénarios expérimentaux ont été formulés pour l'injection d'anomalies dans chaque cas d'étude. Ces anomalies sont générées par une cyberattaque ou un dysfonctionnement. Pour fournir des scénarios représentatifs de la réalité opérationnelle, nous avons particulièrement étudié les caractéristiques et vulnérabilités inhérentes des CPS. L'étude de ces deux CPS, aux fonctions profondément éloignées, illustre la polyvalence et la généricité de l'approche énoncée dans ces travaux de thèse.

Plan du manuscrit

Le **premier chapitre** détaille l'état de l'art des différents domaines de recherche associés à notre problématique. Nous y présentons dans un premier temps l'importance du secteur maritime, ainsi que les spécificités et contraintes des systèmes maritimes embarqués dans les navires. Par la suite, nous détaillons les principales caractéristiques et propriétés des CPS. Ensuite, nous explicitons les solutions majeures d'analyse de la propagation d'anomalies dans les systèmes. Enfin sont présentés les différents aspects de la théorie des graphes quant à son apport pour répondre à cette même problématique.

Dans le **deuxième chapitre**, une identification générique des principales dépendances constituant un navire est proposée. Une fois le cadre de la problématique défini, une méthodologie de modélisation d'une représentation structurelle d'un CPS, et de ses dépendances, est formulée. Ce modèle de graphe multicouche est ensuite utilisé au sein d'une méthode spécifique d'évaluation de la propagation d'anomalies.

Dans le **troisième chapitre**, deux cas d'étude basés sur des CPS sont présentés : un prototype expérimental de la boucle « mobilité » du *Naval Cyber Range*, et la simulation d'un réseau de distribution d'eau intelligent. Grâce aux données générées à partir de l'exécution des différents scénarios, la méthodologie proposée est appliquée à partir de la modélisation du système concerné, puis à l'évaluation de la propagation d'anomalies. L'outil informatique développé permet d'automatiser l'implémentation de la méthodologie.

Le quatrième chapitre conclut le manuscrit en discutant des résultats obtenus et en présentant de nombreuses perspectives relatives aux travaux de thèse formulés dans ce manuscrit.

Le manuscrit de la présente thèse est composé de quatre chapitres. Les différentes relations entre ceux-ci sont illustrées dans la Figure 3.

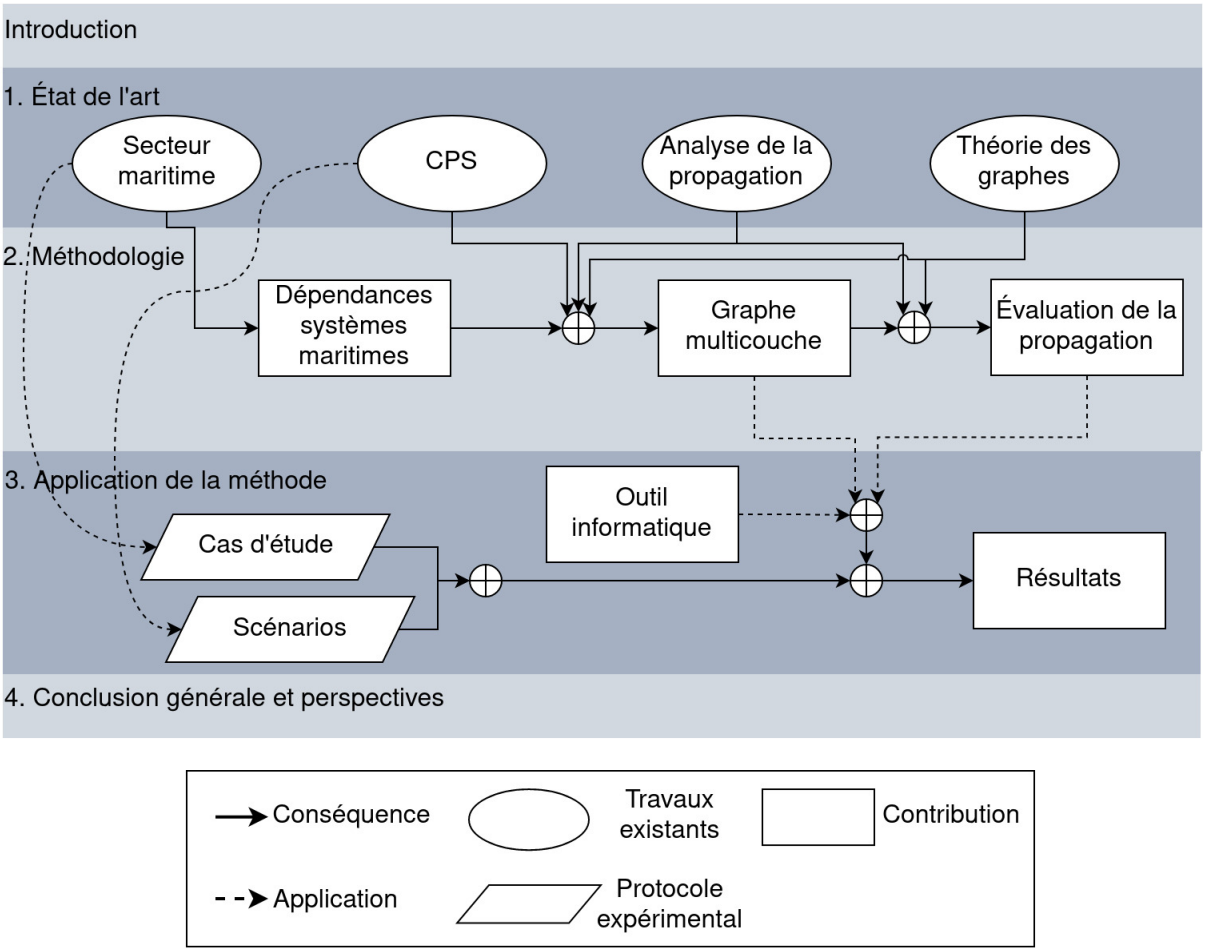


FIGURE 3: Description des relations entre les chapitres du manuscrit de thèse

Chapitre I

État de l'art

Sommaire

Ce chapitre dépeint dans un premier temps l'importance du secteur maritime, ainsi que les spécificités des systèmes qui y sont employés. Sont ensuite décrites les principales caractéristiques d'un type particulier de système maritime : les CPS. Enfin, les principaux apports et limitations des solutions d'analyse de la propagation d'anomalies dans un système sont explicités. Cela est présenté à partir des différents travaux scientifiques traitant de cette problématique. Pour finir, les différents aspects de la théorie des graphes sont détaillés pour souligner son apport quant à la résolution de cette même problématique.

I.1 Secteur maritime

Après avoir explicité la criticité du secteur maritime, nous présenterons dans la suite de cette section les spécificités des navires employés pour répondre aux besoins associés. Qu'ils soient économiques, géopolitiques, ou encore militaires.

I.1.1 Importance du secteur maritime

La planète Terre se distingue de toutes les autres planètes connues à ce jour par la présence des océans qui recouvrent plus de deux tiers de sa surface. De par les nombreuses activités économiques qui y sont associées, les océans sont définis comme des contributeurs majeurs de l'économie mondiale. Évidemment, il est difficile d'obtenir leur valeur réelle tant elle est définie par de nombreux éléments immensurables. Cependant, il est toujours possible d'estimer une valeur minimale. Selon une étude du *Boston Consulting Group*, la valeur associée aux océans est ainsi estimée dans son ensemble à 24 000 milliards de dollars américains [HG15]. Selon cette même étude, les océans créeraient annuellement 2 500 milliards de dollars américains de richesse. En comparant cette valeur estimée aux PIB [1] des différents pays, cela placerait les océans comme 7$^{\text{ème}}$ plus grande économie mondiale.

Depuis des millénaires, l'Homme exploite les océans de manière directe en prélevant ses ressources vivantes, pétrolières, gazières, ou en tirant profit de ses phénomènes physiques associés. Mais aussi de manière indirecte, via le transport de marchandises, de passagers, ou en y implantant des câbles sous-marins de télécommunications. La recherche en science marine

1. Produit Intérieur Brut

est aussi un aspect indissociable de l'exploitation des océans. Elle regroupe différentes disciplines scientifiques qui fournissent des expertises et créent des innovations pour protéger les océans et exploiter ses ressources de manière durable. Ces différents secteurs d'activités cohabitent ainsi dans les mêmes espaces maritimes. De par leurs forts potentiels économiques, ces zones maritimes sont régulièrement la source de conflits géopolitiques entre différents états [2]. Leur surveillance et leur contrôle deviennent alors un enjeu majeur pour l'état souverain, ou non. Pour cela, le développement et l'emploi d'une marine militaire sont indispensables. Parmi les différentes missions qu'elle assure, la protection du territoire et de ses zones maritimes est l'une des principales [Jac21b].

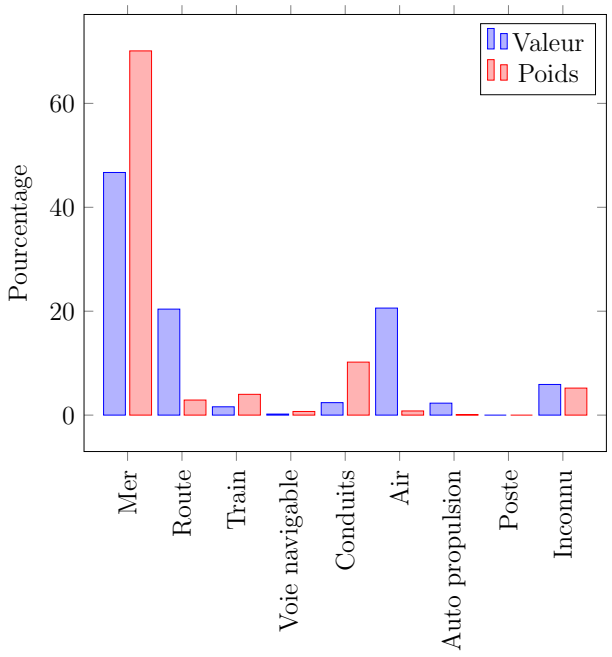


FIGURE I.1: Commerce des 27 pays de l'UE par moyen de transport en 2018 [Com20]

De l'ensemble des secteurs d'activités liés à l'exploitation des capacités maritimes, le transport de marchandises est l'un des secteurs principaux. De ce fait, nous nous y intéressons plus particulièrement dans la suite de cette section. De par son importance économique et stratégique, le transport maritime est vecteur indispensable de la mondialisation. Pour une forte région économique telle que l'Union Européenne (UE), ce mode de transport représentait en 2018 près de 46,7% en valeur, et 70,1% en poids, de la totalité de ses échanges commerciaux (Fig. I.1). Les routes maritimes qui relient les principaux pôles

2. Pourquoi la Grèce et la Turquie s'affrontent en Méditerranée orientale. Le Monde. Consulté le 28 juillet 2021. https://www.lemonde.fr/international/article/2020/09/14/pourquoi-la-grece-et-la-turquie-s-affrontent-en-mediterranee-orientale_6052162_3210.html

économiques sont ainsi devenues des maillons essentiels de l'économie mondiale. Néanmoins, comme cela est illustré dans la Figure I.2 [3], ces routes concentrent un certain nombre de passages stratégiques (détroits, et canaux), ainsi que de zones à risques (surfréquentation, piraterie, terrorisme, etc.). La présence de forces navales dans ces espaces est alors essentielle pour y garantir la libre circulation .

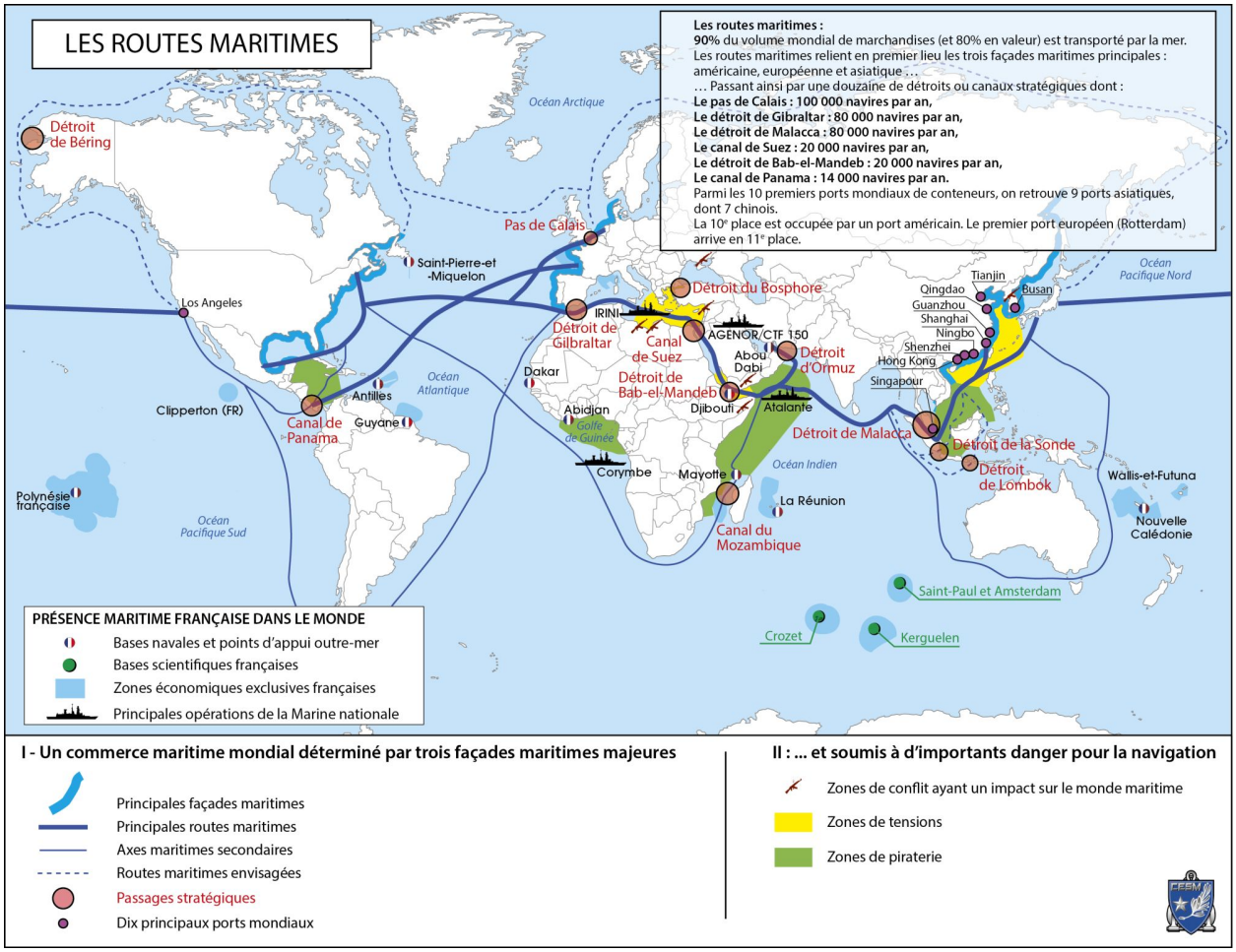


FIGURE I.2: Routes maritimes mondiales (source : Centre d'Études Stratégiques de la Marine)

La Conférence des Nations Unies sur le Commerce et le Développement publie chaque année depuis 1968 une étude sur les transports maritimes pour analyser l'état actuel et les évolutions du secteur en fonction de différents indicateurs. La version fournie pour l'année 2020 est majoritairement orientée sur l'étude de l'impact de la crise sanitaire de la COVID-19

3. Infographie du mois : les routes maritimes. Centre d'Études Stratégiques de la Marine. Consulté le 2 novembre 2021. `https://cesm.marine.defense.gouv.fr/index.php/publications/infographies-du-mois/588-octobre-2021-les-routes-maritimes`

sur le secteur du transport maritime [oTD20]. Le commerce maritime mondial a ainsi accusé en 2020 une baisse de 4,1% en raison des perturbations liées à la pandémie. Malgré cette crise sans précédent, le transport maritime a néanmoins démontré toute sa résilience et son importance stratégique à l'échelle mondiale [MBZ+20, YŞYT20].

Comme illustré dans la Figure I.3, le développement du commerce maritime international ne cesse de s'accroître. Cette augmentation engendre avec elle des besoins de transport de tonnages toujours plus élevé. Pour cela, le secteur maritime conçoit et exploite des navires toujours plus imposants. Le taux d'augmentation de la taille des porte-conteneurs s'est ainsi fortement accéléré au cours des dernières décennies. L'Organisation de Coopération et de Développement Économiques évalue dans un rapport publié en 2015 qu'il n'aura fallu qu'une seule décennie pour doubler la capacité moyenne des porte-conteneurs (de 1500 à 3000 TEU [4]). Alors que 30 années ont été nécessaires pour atteindre 1500 TEU [dT15]. Le *Ever Ace*, porte-conteneur de l'armateur taiwanais *Evergreen*, détient actuellement le record de capacité de transport de marchandises en culminant à 24000 TEU [5]. Outre le transport de marchandises, le secteur d'activité du transport de passagers est tout autant concerné par le gigantisme des navires. Les compagnies de croisière ne cessent de rivaliser avec des paquebots toujours plus imposants, pouvant accueillir toujours plus de passagers. Ces *méga paquebots* sont ainsi capables de transporter jusqu'à 6 680 passagers et 2200 membres d'équipage [6].

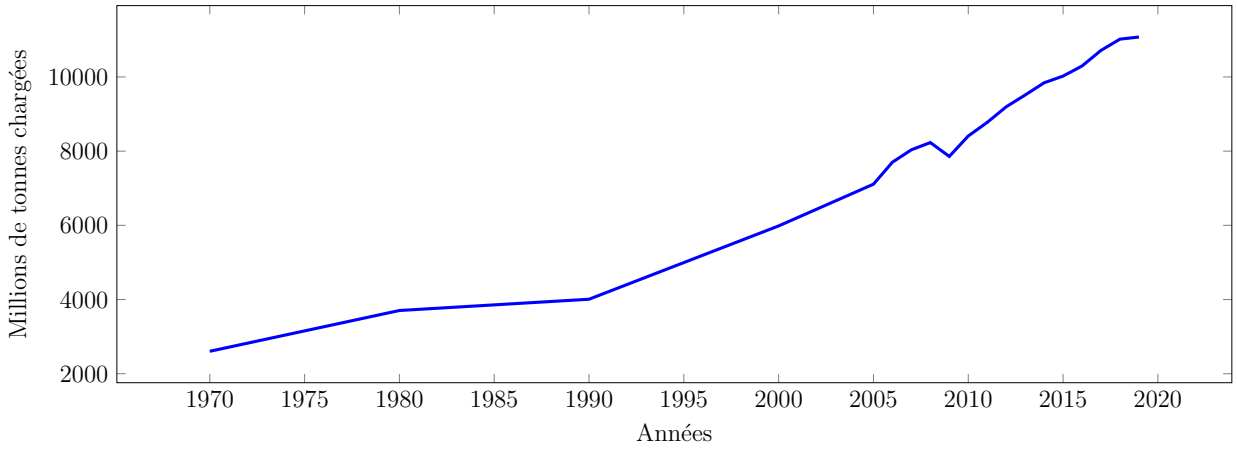


FIGURE I.3: Développement du commerce maritime international par année [oTD20]

4. *Twenty-foot Equivalent Units*

5. L'« Ever Ace », plus grand porte-conteneur du monde, est arrivé en Europe. Consulté le 28 juillet 2021. https://lemarin.ouest-france.fr/secteurs-activites/shipping/40761-l-ever-ace-plus-grand-porte-conteneurs-du-monde-en-europe

6. Symphony of the Seas Cruise Ship. Ship Technology. Consulté le 28 juillet 2021. https://www.ship-technology.com/projects/symphony-seas-cruise-ship/

L'importance du secteur maritime à l'échelle mondiale ne cesse de s'accroître et engendre des nouveaux besoins dans tous les secteurs d'activité sous-jacents. D'après les indicateurs actuels, il semblerait que cette tendance n'est pas près de s'inverser, et ce malgré la crise sanitaire traversée. Que ce soit pour le transport de marchandises ou de passagers, les navires employés repoussent les limites technologiques pour répondre à une demande toujours plus importante. La criticité des enjeux économiques associés au secteur maritime est d'autant plus majeure de par les tensions géopolitiques qui y sont associées.

I.1.2 Diversité des navires

Comme nous venons de le présenter, une forte diversité des domaines d'activité résulte du secteur maritime global. Chaque domaine d'activité maritime se caractérise par des besoins distinctifs. Des navires sont ainsi employés pour y répondre à partir de caractéristiques et propriétés spécifiques. Ils se distinguent par une forte diversité à différentes échelles.

En fonction de la mission qui leur est attribuée, il est possible de distinguer plusieurs types de navires [7]. Du navire-citerne destiné au transport de liquide, au câblier utilisé pour la pose et l'entretien des câbles sous-marins, en passant par le navire de guerre, ou bien d'autres encore, chaque bâtiment est mis à flot pour exercer une mission spécifique. Au-delà de la diversité entre ces différents types de navire, il existe une diversité tout aussi importante au sein d'un même type. Prenons comme exemple les navires militaires français de la Marine Nationale.

Afin d'assurer la sécurité du territoire et des concitoyens français, la Marine Nationale dispose d'un large spectre de moyens et de compétences. Du secours aux populations à l'action à la défense maritime du territoire, différents systèmes navals sont nécessaires à la Marine Nationale pour réaliser l'ensemble des missions qui lui sont attribuées [Nat21]. Rien que pour sa flotte de surface, elle dispose d'une centaine de bâtiments regroupés au sein d'une même Force d'Action Navale [8]. Ces navires sont extrêmement différents de par leurs caractéristiques et les missions attribuées. Par exemple, on y retrouve à la fois des bâtiments de commandement et de projection de forces comme les porte-hélicoptères amphibies et des chasseurs de mines. Cette diversité est utilisée au sein de différents « groupes » pour assurer une forte complémentarité opérationnelle. Le groupe aéronaval, concentré

7. A Guide To Types of Ships. Marine Insight. Consulté le 28 juillet 2021. https://www.marineinsight.com/guidelines/a-guide-to-types-of-ships/

8. Forces de surface. Ministère des armées. Consulté le 28 juillet 2021. https://www.defense.gouv.fr/marine/operations/forces/force-d-action-navale/forces-de-surface/forces-de-surface

autour du porte-avions nucléaire Charle de Gaulle, est l'un des plus représentatifs de la force navale française [9]. Il permet à la fois la projection d'unités opérationnelles sur des théâtres d'opérations lointains, ainsi qu'une maîtrise de l'espace maritime, sous-marin, et aérien.

La diversité des navires se répercute aussi à une échelle plus spécifique, notamment pour les navires militaires, en fonction de la mission attribuée. Afin de faciliter leur construction, ainsi que les maintenances pour leur Maintien en Conditions Opérationnelles, certains bâtiments sont construits en série selon des mêmes plans. On parle alors de « classe de navire ». Chaque bâtiment de la série se distinguera, ou non, par les équipements qui lui sont intégrés dans la cadre de la mission attribuée. Prenons le cas de la classe *Aquitaine* de la Marine Nationale, composée de frégates multi missions. De par leurs équipements intégrés, la *Normandie* (sixième frégate de la classe) est spécialisée dans la lutte anti-sous-marine, tandis que l'*Alsace* (septième frégate de la classe) est plus fortement orientée vers la lutte antiaérienne.

I.1.3 Spécificités des navires

De par la particularité de l'environnement dans lequel il est employé, un navire présente de nombreuses spécificités et contraintes à différents niveaux d'étude. Ces aspects doivent obligatoirement être pris en compte lorsque l'on traite de cette problématique. Olivier Jacq *et al.* ont proposé une liste non exhaustive de ces spécificités et contraintes [JBB+18], nous allons ainsi la détailler et l'agrémenter davantage.

Un produit de consommation est défini par différentes phases de cycle de vie [Sta16]. Les navires sont alors caractérisés par un cycle de vie particulièrement long, constitué par 4 étapes majeures : conception, construction, exploitation et démantèlement [10]. Cela est d'autant plus vrai pour les navires militaires qui, en raison de leur complexité, peuvent subir une phase de conception de 15 ans et avoir une durée de vie supérieure à 30 ans. Ce qui signifie que les équipements choisis lors de la phase de conception auront déjà une obsolescence technologique de plusieurs années lors de leur mise en service. Ils seront aussi exploités pendant plusieurs dizaines d'années avec des failles, plus ou moins importantes, et plus ou moins connues par le grand public. Pour pallier ce problème, les navires militaires sont généralement soumis à une refonte à mi-vie imposée par l'obsolescence de leur système

9. Le groupe aéronaval français. Ministère des armées. Consulté le 28 juillet 2021. https://www.defense.gouv.fr/english/marine/magazines/infographies/moyens/le-groupe-aeronaval-francais

10. Le cycle de vie d'un navire. Ministère des armées. Consulté le 28 juillet 2021. https://www.defense.gouv.fr/marine/magazine/le-cycle-de-vie-d-un-navire/le-cycle-de-vie-d-un-navire

d'armement. Ce qui n'est donc pas le cas pour tous les autres types de navires (cargo, bateau de croisière, etc.). Dans ce cas, la modernisation des équipements est effectuée lorsque ceux-ci sont beaucoup trop vieillissants, ou que plusieurs équipements sont à remplacer.

À cette durée de vie étendue s'ajoutent différentes contraintes inhérentes au domaine d'application. Les navires sont ainsi soumis à plusieurs contraintes environnementales, physiques, et technologiques. Premièrement, le milieu marin dans lequel évoluent les navires est un milieu hostile. L'état de la mer, caractérisé par la force du vent et de la houle, est un facteur majeur qui soumet le navire et ses occupants à des contraintes importantes. Le déploiement des navires à des milliers de kilomètres au milieu des océans implique aussi des contraintes supplémentaires. Tout navire est assujetti aux connexions satellitaires qui assurent des moyens de communication et d'accès au réseau Internet. Ces connexions sont caractérisées par une bande passante limitée, associées à un coût élevé et une forte instabilité. Ce qui est une contrainte majeure pour la maintenance, le contrôle et la surveillance à distance. Cela est d'autant plus exacerbé avec la recrudescence de l'intérêt porté aux navires autonomes. La durée de la mission associée au navire est aussi une contrainte majeure. Celle-ci pouvant s'étendre de quelques jours à plusieurs semaines, le navire doit se montrer extrêmement résilient durant toute sa durée. Cela est notamment le cas lors d'apparition d'avarie environnementale (feu, voie d'eau, etc.), mais surtout en cas d'avarie informatique. En effet la majorité des navires, d'autant plus les navires civils, n'embarquent pas d'expert ou de technicien informatique à bord. Ces avaries peuvent engendrer des conséquences critiques pour le navire, son équipage, sa mission, ou encore pour l'environnement.

Outre ces contraintes et caractéristiques globales associées aux navires, les systèmes qui les composent sont autant caractérisés par différentes spécificités critiques qu'il est nécessaire de définir, d'analyser et de remédier. Les travaux de thèse présentés s'orientant principalement autour de la problématique des CPS constituant un navire, nous nous focaliserons davantage sur les spécificités associées à ceux-ci dans les sections suivantes.

I.2 Systèmes d'information maritimes

Dans cette section, nous traiterons des principaux systèmes constituant un navire. Nous utiliserons le terme « Systèmes d'Information Maritimes (SIM) » tel que proposé par Olivier Jacq dans ses travaux de thèses [Jac21b]. Ce terme est utilisé pour évoquer la composante informatique de la *marétique* (Définition I.1), défini dans le Livre Bleu du cluster Marétique

publié en 2013 [mf12].

Definition I.1. *La marétique regroupe l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'utilisation des opérations relatives aux activités maritimes, fluviales et portuaires.*

Nous présenterons les principales caractéristiques et propriétés de ces systèmes, ainsi que leurs différentes contraintes inhérentes au domaine d'application maritime. Nous détaillerons ensuite les aspects de cybersécurité immuables à leur emploi.

I.2.1 Spécificité des systèmes d'information maritimes

Comme nous l'avons défini dans la Section I.1.2, les navires se caractérisent par la diversité des missions qui leur sont attribuées. Un navire moderne, pouvant accueillir plusieurs milliers de passagers, cumule différents systèmes pour assurer les missions qui lui sont attribuées tout en garantissant un niveau de qualité de vie optimal à bord. Cela s'est accentué avec la modernisation des navires qui permettent aux équipages et aux passagers d'apprécier un confort en mer relativement semblable à celui à terre. De par la diversité des missions associées, les SIM embarqués se distinguent par leur hétérogénéité. De plus, l'emploi de chaque système est caractérisé par des contraintes spécifiques qui sont plus ou moins critiques.

Prenons comme exemple le porte-avion *Charles de Gaulle*. Qualifié de « ville flottante »[11] il cumule des systèmes nécessaires au fonctionnement de ses capacités de centrale nucléaire, d'aéroport, et pour l'emploi d'armes d'autodéfense. À cela s'ajoutent les différents systèmes utilisés pour garantir un confort de vie optimal auprès de 2000 marins. Hôpital, restauration, gestion de l'eau et de l'électricité, et autres, sont autant de capacités diverses et variées du navire auxquelles sont associées différents systèmes. Les navires modernes cumulent ainsi des systèmes hétérogènes nécessaires à l'exercice de leur fonction propre de navigation, et des systèmes supplémentaires relatifs à leur mission et à la vie à bord. Hétérogénéité qui se distingue à la fois par leurs caractéristiques et leurs fonctions.

L'ensemble des SIM est divisible en deux catégories principales selon des caractéristiques inhérentes à leurs emplois. À bord, on distingue ainsi principalement des systèmes associés à l'*Information Technology (IT)* et à l'*Operational Technology (OT)* du navire [BIM20]. Les

11. Dans les entrailles de notre porte-avions « Charles-De-Gaulle ». Capital. Consulté le 28 juillet 2021. https://www.capital.fr/economie-politique/dans-les-entrailles-de-notre-porte-avions-charles-de-gaulle-1134660

systèmes *IT* sont des systèmes génériques, généralement associés à la gestion des données. Tandis que les systèmes *OT*, aussi qualifiés de systèmes « métier », regroupent les différents équipements nécessaires à la surveillance et au contrôle des processus physiques. Ces systèmes s'opposent par leurs caractéristiques et contraintes inhérentes à leur utilisation [ZR19]. Un récapitulatif des différences de caractéristiques les plus significatives est présenté dans la Table A.1 de l'Annexe A. Le National Institute of Standards and Technology (NIST) propose une définition pour chacun de ces termes *IT* (Définition I.2) et d'*OT* (Définition I.3).

Definition I.2. *IT : Désigne tous les services, équipements, systèmes ou sous-systèmes d'équipements interconnectés, qui sont utilisés pour l'acquisition, le stockage, l'analyse, l'évaluation, la manipulation, la gestion, le déplacement, le contrôle, l'affichage, la commutation, l'échange, la transmission ou la réception automatiques de données ou d'informations par l'entité concernée [NDP17]*[12].

Definition I.3. *OT : Systèmes ou dispositifs programmables qui interagissent avec l'environnement physique (ou gèrent les dispositifs qui interagissent avec l'environnement physique). Ces systèmes/dispositifs détectent ou provoquent un changement direct par la surveillance ou le contrôle de dispositifs, de processus et d'évènements [R+18]*[13].

Système IT

Parmi les systèmes IT à bord [Jac21b] [BIM20], on distingue notamment l'ensemble des moyens de communication vers l'extérieur du navire avec différents services et réseaux vers la terre (téléphonie, Internet, etc.) utilisant une connexion satellitaire (SATCOM) en zone hauturière, ou encore des réseaux *Global System for Mobile communications (GSM)* (3G/4G/5G) en navigation côtière. D'un point de vue interne au navire on dénote aussi différents réseaux de communication. Cela comprend à la fois les systèmes d'alarmes, de téléphonie et d'interphonie, mais aussi les réseaux informatiques *Internet Protocol (IP)*, et *Wireless Fidelity (WiFi)* qui relient les systèmes entre eux. Ces réseaux informatiques sont constitués de différents équipements et solutions de gestion et de protection. On y retrouve des routeurs, commutateurs, *Virtual Private Network (VPN)*, et *Virtual Local Area Network*. Ainsi que divers moyens de sécurité tels que des passerelles, sondes, pare-feu, et

12. Means any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

13. Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.

autres outils de journalisation. Les systèmes de communication interne regroupent aussi la totalité des équipements et services utilisés pour gérer les personnes à bord et les moyens mis à leur disposition. Cela comprend à la fois la connexion Internet fournie à l'équipage et aux passagers pour leur distraction, et différents systèmes de gestion de ressources humaines et matérielles. Pour finir, l'IT centralise également les ressources et services informatiques « classiques » tels que les postes bureautiques et les applications associées comme l'intranet ou la messagerie interne.

Système OT

De même, l'OT exploitée à bord se caractérise par un ensemble de systèmes [BIM20] [14]. On différencie ainsi 3 fonctions majeures parmi les systèmes d'OT employés à bord : la **conduite du navire**, la **conduite de la plateforme**, et enfin, la réalisation de **fonctions spécifiques à la mission** du navire.

Concernant les systèmes nécessaires à la bonne conduite du navire. On distingue les systèmes de navigation électronique tels que cartographie numérique (*Electronic Chart Display Information System (ECDIS)*), radar et sondeurs, les systèmes de positionnement géographique par satellite comme le *Global Positioning System (GPS)*. Divers systèmes sont aussi utilisés pour établir la situation nautique du navire à différents instants, et ainsi adapter sa conduite en quasi-temps réel ou en projection temporelle. Cela regroupe par exemple les équipements nécessaires à l'échange de messages d'identification entre navires (*Automatic Identification System (AIS)*) ainsi que les *Global Maritime Distress and Safety System (GMDSS)* [15], tel que les *navigational text messages*. Divers instruments comme l'anémomètre, ou encore le baromètre sont aussi largement employés pour connaître et prévoir les conditions météorologiques.

La conduite de la plateforme est quant à elle assurée par différents **systèmes de contrôle industriel**, aussi appelés *Industrial Control Systems (ICS)* [16]. Parmi l'ensemble des systèmes de plateforme on distingue notamment : la propulsion, la production d'électricité, le contrôle des apparaux, la gestion du carburant, les alarmes et les éléments de sécurité contre les incendies ou les voies d'eau, etc. D'autres systèmes de plateforme comme

14. Les systèmes de la marétique. Cybermarétique.fr. Consulté le 01 août 2021. `https://cybermaretique.fr/les-systemes-de-la-maretique/`

15. Systèmes mondiaux de détresse et de sécurité en mer

16. Ce terme générique est utilisé pour décrire différents types de systèmes de contrôle et de surveillance, composé de réseaux et de divers équipements pour opérer ou automatiser un processus physique industriel.

le traitement des eaux, le frigidaire, ou encore le contrôle du chauffage, de la ventilation et de la climatisation, impactent plus directement le confort de vie de l'équipage. Dans la suite de ces travaux de thèse, nous nous attarderons plus particulièrement sur deux types de systèmes de plateforme employés dans des fonctions critiques d'un navire : la propulsion et la gestion de l'eau.

Les navires civils, comme les navires militaires, disposent de systèmes OT spécifiques à la réalisation de la mission qui leur est attribuée. Par exemple, les cargos [17] possèdent un ensemble de systèmes de contrôle et de surveillance spécifiques aux équipements nécessaires à la gestion de la cargaison (*Cargo Control Room*), que ce soit lors de son chargement, de son transport, ou de son déchargement. Ces systèmes sont regroupés au sein d'un espace spécifique dans le navire, ou au sein de la passerelle. Concernant les navires militaires les systèmes OT particuliers à leur mission, et les plus représentatifs, sont les systèmes d'armes. Ils sont composés par exemple de différents senseurs tels qu'un sonar (de coque ou remorqué), un radar, ou encore un équipement de surveillance panoramique électrooptique pour détecter les signatures infrarouges. Suite à une détection de ces senseurs, différents actionneurs comme des brouilleurs, des lance-leurres, ou encore un système d'artillerie peuvent être potentiellement mis en œuvre.

En résumé, les systèmes OT employés à bord sont généralement composés de dispositifs physiques, en lien avec un processus physique associé, et des équipements numériques en charge du contrôle et de la surveillance du processus. En raison de cette dualité entre le monde physique et numérique, ils sont souvent associés au concept de ***système cyber-physique*** que nous détaillerons dans une section suivante.

L'OT utilisée à bord comprend également l'ensemble des systèmes logiciels embarqués, nécessaires au contrôle et à la surveillance des systèmes matériels présentés précédemment. Différents systèmes extrêmement complexes sont ainsi utilisés selon les besoins inhérents au navire. Un navire armé moderne est constitué d'un système de combat permettant de gérer et d'exploiter les informations transmises par les différents senseurs. À titre d'exemple, le système de combat SETIS®, développé par Naval Group, est approximativement codé sur 20 millions de lignes. À cela s'ajoute un système de gestion de la plateforme du navire, codé sur 2 millions de lignes (source : Naval Group).

Comme nous venons de le présenter, l'ensemble des systèmes employés au sein d'un navire se caractérise par leur hétérogénéité, tant au niveau de leurs fonctions que de leurs

17. Navire destiné au transport de marchandises diverses.

caractéristiques. Le niveau de complexité de ces systèmes ne cesse de s'accroître depuis la forte numérisation des navires. De plus, ces systèmes sont souvent choisis « sur étagère » et directement intégrés au navire sans tenir compte des potentielles vulnérabilités que cela peut impliquer [18].

Un navire ne peut être caractérisé comme une agrégation de systèmes. L'ensemble des systèmes qui le composent est associé à un grand nombre de dépendances, à la fois intrinsèques et extrinsèques, qu'il est nécessaire d'analyser durant tout le cycle de vie du navire. Dans les sections suivantes, nous traiterons davantage de la problématique des dépendances associée aux systèmes navals.

I.2.2 Évolution des systèmes d'information maritimes

La transformation du secteur maritime s'est accompagnée, s'accompagne, et s'accompagnera encore, d'une évolution des systèmes d'information employés à bord.

Dans le secteur maritime **civile**, cette évolution est fortement liée au développement actuel des navires semi-autonomes et autonomes [Lev17]. En 2018, le concepteur de navire *Rolls-Royce* a notamment effectué le premier test en condition réelle de ferry autonome [19]. Lors de cette traversée expérimentale, le navire était entièrement autonome à l'aller, puis téléopéré au retour par un opérateur situé à une cinquantaine de kilomètres. En réponse à ce rapide développement, l'Organisation Maritime Internationale a défini en 2021 un cadre réglementaire spécifique pour les navires de surface autonomes *(Maritime Autonomous Surface Ship (MASS))* [MSC21]. Cette réglementation caractérise 4 degrés d'autonomie, du premier degré associé à l'utilisation de processus automatisés impliqués dans le contrôle ponctuel du navire, jusqu'au quatrième degré caractérisant la totale autonomie du navire. Cette évolution majeure est associée à de nombreux bénéfices directs et indirects pour le secteur maritime et son environnement. Depuis quelques années, des études scientifiques se focalisent sur les potentiels bénéfices économiques engendrés par l'emploi de navires autonomes. D'après leurs résultats, cela permettrait de réduire les coûts opérationnels de fonctionnement (équipage, consommables, maintenance, etc.), ainsi que les coûts de consommation de carburant (meilleure utilisation de l'espace, réduction du poids, etc.) [KBJ17]. Ce qui

18. La problématique de la marétique. Cybermarétique.fr. Consulté le 01 août 2021. `https://cybermaretique.fr/la-problematique/`

19. Rolls-Royce And Finferries Demonstrate World's First Fully Autonomous Ferry. Marine Insight. Consulté le 02 août 2021. `https://www.marineinsight.com/shipping-news/rolls-royce-and-finferries-demonstrate-worlds-first-fully-autonomous-ferry/`

permettrait indirectement de réduire l'impact environnemental du secteur maritime. Ces résultats sont discutables de par la non-considération des coûts associés à l'assurance, ainsi que ceux émanent de la mise en œuvre de l'ensemble des moyens (humains et technologiques) nécessaires à la cybersécurité de ces navires [ZPM21]. En effet, de par leurs caractéristiques inhérentes, les *MASS* se distinguent par une surface d'attaque numérique accrue [BTBV19].

L'emploi de **véhicule sans pilote** (*Unmanned Vehicle (UV)*) s'est aussi largement démocratisé dans le secteur civil, mais surtout pour des applications militaires [RCM+17]. Mis en œuvre dans les 3 espaces (surface, sous-marin, et aérien), ils sont généralement associés à des missions de renseignement, de surveillance, ou de chasse aux mines. Dans un futur proche, leurs capacités pourraient être enrichies par l'ajout de systèmes d'armes [20]. Ces systèmes autonomes présentent de nombreux avantages pour les forces navales. Ils démultiplient leurs capacités opérationnelles, avec une furtivité accrue, tout en limitant le risque humain. Ces véhicules tendent aujourd'hui à gagner en autonomie et en fonctionnalités. Naval Group a récemment présenté un prototype de « grand » drone sous-marin océanique, destiné à être employé au sein d'une force navale [21]. Contrairement aux drones déjà existants, il sera dans la capacité de réaliser en toute autonomie des missions de plusieurs milliers de kilomètres, et ce pendant plusieurs semaines.

Ces évolutions des systèmes maritimes génèrent de nouvelles problématiques majeures, nécessaires à considérer. Cela concerne notamment le traitement et l'analyse de l'important flux de données maritimes généré par ces systèmes. Diverses technologies numériques, basées sur l'**Intelligence Artificielle (IA)**, apparaissent comme des solutions adaptées pour tirer profit de ce flux de données dans différentes applications bénéfiques à diverses phases de cycle de vie du navire. Ce flux de données pourrait par exemple enrichir un **jumeau numérique** du navire [AG20], ou être utilisé par un modèle d'**apprentissage automatique** pour la détection d'anomalies dans un système de propulsion [EHC+20]. Aussi, ces systèmes autonomes se distinguent par une complexité et un niveau de **dépendances** accrus. Ces caractéristiques, associées à une réduction de l'équipage, tendent à accroître les impacts de la propagation d'anomalies, et donc le besoin d'études associées. Pour cela, nous étudierons dans la section suivante la littérature existante traitant de la problématique de propagation d'anomalies relatives aux systèmes, et plus précisément aux systèmes maritimes.

20. U.S. Navy To Weaponize Unmanned Craft For Surface Warfare. Marine Insight. Consulté le 02 août 2021. https://www.marineinsight.com/shipping-news/u-s-navy-weaponize-unmanned-craft-surface-warfare/

21. Naval Group lance son premier drone océanique sous-marin. Mer et Marine. Consulté le 08 octobre 2021. https://www.meretmarine.com/fr/content/naval-group-experimente-son-premier-drone-oceanique-sous-marin

I.2.3 Cybersécurité des systèmes d'information maritimes

Dans le futur, le secteur maritime continuera de s'appuyer toujours plus sur l'utilisation de solutions numériques pour accomplir différentes fonctions en lien avec des activités diverses et variées. L'évolution rapide, la forte disponibilité des données et informations, ainsi que la vitesse de transfert et de traitement, sont autant de caractéristiques de ces solutions dont bénéficient les acteurs du secteur pour optimiser les opérations, réduire les coûts associés, mais aussi améliorer la sécurité et l'impact sur l'environnement. Toutefois, ce gain en fonctionnalité s'accompagne de contraintes et risques inhérents. Les solutions numériques employées se caractérisent par une connectivité accrue entre des serveurs, des systèmes informatiques et opérationnels, le tout majoritairement réalisé par une connexion Internet. De ce fait, l'ensemble des SIM évoqués dans la section I.2.1 est directement, ou indirectement, en lien avec le *cyberespace*, concept défini dans la Définition I.4.

Definition I.4. *Cyberespace : un domaine global dans l'environnement de l'information consistant en un réseau interdépendant d'infrastructures de systèmes d'information comprenant Internet, les réseaux de télécommunications, les systèmes informatiques et les processeurs et contrôleurs intégrés [For17]*[22].

À cause de son processus de numérisation, le secteur maritime est devenu la cible de nombreux incidents affectant la *cybersécurité* (Définition I.5) de ses acteurs, au travers des SIM employés. Ces dernières années l'entrée dans le maritime 4.0 a fortement accéléré ce processus, et donc augmenté la surface d'attaque. Comme illustré dans la Figure I.4, en résulte une augmentation exponentielle des incidents cyber impactant ce secteur. Ces incidents sont majoritairement liés à des virus et ransomware (38.3%) et des intrusions dans les systèmes d'informations (28 %) (Figure I.5).

Definition I.5. *La cybersécurité est un état recherché pour un système d'information, lui permettant de résister à des évènements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles [Gar15].*

22. A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

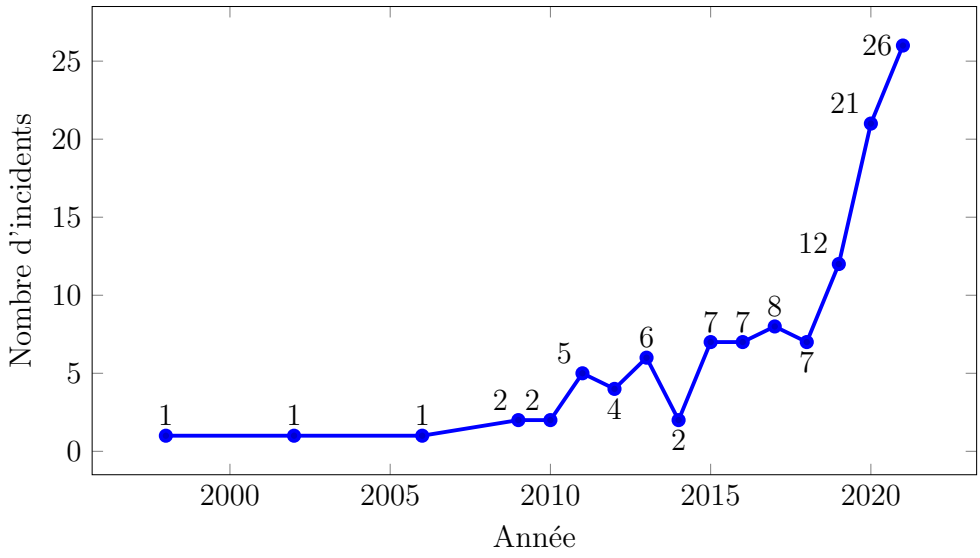


FIGURE I.4: Nombre d'incidents de cybersécurité répertoriés ayant visé le secteur maritime depuis 1998 (source des données : [Jac21a])

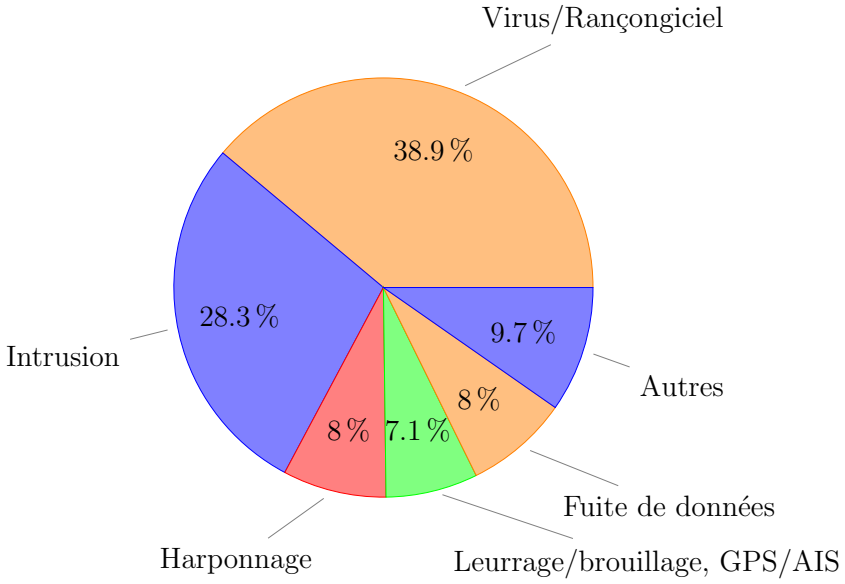


FIGURE I.5: Répartition des types d'incidents de cybersécurité répertoriés ayant visés le secteur maritime depuis 1998 (source des données : [Jac21a])

Ces incidents sont majoritairement la cause d'une exploitation de vulnérabilités spécifiques aux SIM. Un évènement, volontaire ou non, est susceptible de compromettre l'un des 3 critères de la sécurité (disponibilité, intégrité, et confidentialité). Ces évènements sont susceptibles d'induire l'apparition d'anomalies dans un ou plusieurs SIM. Dans la suite de ces travaux, nous utiliserons le mot « anomalie » sans différencier l'origine volontaire ou non. Parmi l'ensemble de ces vulnérabilités, trois types de vecteurs principaux peuvent être identifiés [Jac21b] : le cycle de vie long d'un navire, le manque de maturité cyber du secteur maritime, et une absence quasi générale d'équipement de cybersécurité à bord des navires. Les vulnérabilités induites doivent cependant être nuancées par les immenses apports du numérique dont bénéficie le secteur maritime. Cependant, un ensemble de mesures et de réglementations doivent être considérées pour limiter les potentiels impacts résultant de l'exploitation de ces vulnérabilités. La cybersécurité des SIM est fortement liée à leur *cyberprotection* (Définition B.1), leurs capacités de *cyberdéfense* (Définition B.2) et *cyber résilience* (Définition B.3).

I.2.4 Gestion des risques cyber associés aux SIM

Les navires, les plateformes pétrolières, ou encore les installations portuaires, l'ensemble du secteur maritime est confronté aux risques cyber. Quelle que soit l'entité visée, les menaces se caractérisent par leur diversité et leur impact opérationnel conséquent. Elles représentent des enjeux primordiaux pour la sécurité et la sûreté des biens, des personnes, et de l'environnement. En 2017, l'OMI (Organisation Maritime Internationale) a élevé la gestion des cyber-risques maritimes comme priorité majeure pour l'ensemble des acteurs du secteur d'activité. Un ensemble de directives a ainsi été publié pour fournir des recommandations pour protéger le transport maritime contre les menaces cyber [Int17]. En complément, une résolution relative à la gestion des cyber-risques maritimes a été adoptée. Ces résolutions visent à encourager les organisations concernées à traiter la problématique du risque cyber au sein du code ISM (*International Safety Management*) [23], lors de la première vérification annuelle de l'attestation de conformité [24] de la compagnie, depuis le 1er janvier 2021. Les mesures de l'OMI ont été complétées par différentes organisations maritimes internationales telles que l'*International Chamber of Shipping*, le *Baltic and International Maritime Council*, l'*International Union of Marine Insurance*, et bien d'autres, qui se sont unies pour développer

23. Un code de sécurité applicable aux compagnies maritimes et entré en vigueur au 1er juillet 2002 pour tous les navires d'un tonnage supérieur à 500.

24. *Document of compliance* : un certificat de sécurité délivré aux compagnies maritimes conformément au code ISM de 1998 en vertu du chapitre 9 de la convention SOLAS.

un document proposant les lignes directrices principales pour assurer la cybersécurité à bord d'un navire. Actuellement il existe 4 versions de ce document, dont la dernière date de 2020 [BIM20].

Au niveau européen, la directive NIS (*Network and Information System Security*) [25] prévoit la mise en œuvre de mesures et de moyens nécessaires pour assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d'information au sein de l'UE. En France, cette directive a été transposée dès 2018 avec l'identification des **Opérateurs de Services Essentiels (OSE)** [26]. Cela concerne évidemment l'ensemble des acteurs du transport maritime (compagnie maritime, gestionnaire de ports, etc.), qui doivent adopter des mesures techniques et organisationnelles afin de les protéger au mieux des risques cyber.

Au niveau national, divers dispositifs visant à protéger les **Opérateurs d'Importance Vitale (OIV)** [27] ont déjà été adoptées entre 2013 et 2016. Cela concerne notamment le sous-secteur des « Transports maritime et fluvial », dont les obligations en matière de sécurité informatique ont été écrites par les services de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), et sont entrées en vigueur en 2016 [28]. Depuis 2015, la France est ainsi particulièrement engagée dans la sensibilisation aux cyber-risques maritimes des acteurs concernés. L'administration des affaires maritimes française a publié trois guides à destination des compagnies françaises pour les sensibiliser à la protection de leurs navires [dam16] [dam17] [Age18a]. Le 17 novembre 2020, la réponse française aux enjeux de cybersécurité du monde maritime s'est d'autant plus renforcée avec la création de **France Cyber Maritime** [29]. Les missions accordées à cette association sont multiples : -fédérer les différents acteurs du maritime et de la cybersécurité, -renforcer l'offre de services de cybersécurité adaptée au secteur, -fournir des services opérationnels.

Une démarche de gestion des cyber-risques maritimes a été proposée dans la version n°4 du document développé par les différentes organisations maritimes internationales [BIM20].

25. Directive (UE) 2016/1148. Journal officiel de l'Union européenne. Consulté le 12 octobre 2021. `https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033122937`

26. Une entité publique ou privée qui fournit un service dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

27. LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. Journal Officiel. Consulté le 12 octobre 2021. `https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000028338907?r=fTBzVqx2C3`.

28. Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relative au sous-secteur d'activités d'importance vitale « Transports maritime et fluvial ». JORF n°0197 du 25 août 2016. Consulté le 12 octobre 2021. `https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033063081`

29. `https://www.france-cyber-maritime.eu/`.

FIGURE I.6: Démarche de gestion du risque cyber (source : [BIM20])

La Figure I.6 illustre le processus cyclique, composé de différentes étapes, qui définit cette démarche. Ses auteurs insistent sur le fait que celle-ci doit être supervisée par un expert tout au long de sa réalisation pour s'assurer que les mesures mises en place face aux cyber-risques maritimes soient appropriées aux différentes menaces et vulnérabilités. Parmi les étapes les plus critiques, l'**évaluation des risques** fournit des éléments de quantification des éléments qui composent le navire en fonction de leurs caractéristiques, ainsi que les potentiels impacts qui en découlent. Cela permet dans l'étape suivante du processus de définir et d'opérer des mesures de protection et de détection adaptées. En lien avec la démarche formulée dans ce document, une méthode spécifique d'évaluation des impacts associés aux risques. Cette méthode est basée sur le modèle *Confidentiality, Integrity and Availability* [Pub04]. Cependant ce modèle est assez ancien, il a été développé en 2002 pour répondre aux problématiques d'évaluation associées aux systèmes d'information dits « classiques ». De plus l'évaluation de l'impact potentiel n'est pas quantitative, elle repose uniquement sur 3 critères : *low*, *moderate*, *high*.

Dans la littérature scientifique, un certain nombre d'études basées sur l'évaluation des cyber-risques maritimes ont déjà été formulées. Kevin Jones *et al.* ont par exemple formulé le modèle *Maritime Cyber-Risk Assessment* basé sur la considération des vulnérabilités des systèmes, leur facilité d'exploitation, ainsi que le gain potentiel résultant [JT19]. Dans une

autre étude, le modèle *Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges* développé par Microsoft pour l'identification des menaces de sécurité informatique, a été employé pour évaluer les risques cyber associés à un navire autonome [KKG18]. Victor Bolbot *et al.* ont quant à eux formulé une méthode dénommée *Cyber Preliminary Hazard Analysis* pour l'identification et l'évaluation des impacts de cyberattaques visant un navire [BTBV19]. Là aussi cette méthode a été illustrée sur un cas d'étude de navire autonome, plus précisément sur les systèmes associés à ses fonctions de navigation et de propulsion. L'ensemble de ces travaux se focalisent sur une évaluation non quantifiée de l'impact des risques potentiels, uniquement basés sur des critères de sévérité tels que : mineur, significatif, grave, catastrophique. De surcroît, la cartographie du système, composée des multiples interdépendances entre ses éléments, n'est que trop peu considérée pour évaluer les risques critiques potentiels qui en découlent.

I.3 Systèmes cyber-physiques

Les CPS sont associés au contrôle et monitoring de processus physiques grâce à différents systèmes informatiques. Ils sont caractérisés par diverses interdépendances entre des composants du cyberespace et du monde physique. Un CPS est ainsi composé d'un ensemble d'éléments de calcul, de communication, et de contrôle. Nous étudierons dans les sections suivantes les caractéristiques de ces systèmes, comment celles-ci sont employées dans divers domaines, et quelles vulnérabilités associées un potentiel attaquant pourrait exploiter.

I.3.1 Définition, emploi et défis associés

De part leur fort impact potentiel sur la société, l'environnement, et le domaine de la santé, les CPS suscitent l'intérêt du monde scientifique, de l'industrie, et des gouvernements depuis l'année 2006. Date à laquelle le terme « système cyber-physique » est créé par la Fondation Nationale pour la Science (*National Science Foundation*) [LS17]. Depuis cette année-là, d'innombrables définitions de ce terme ont été proposées. Nous utiliserons la définition suivante dans nos travaux :

Definition I.6. *Un CPS peut être considéré comme une confluence de système intégré, système en temps réels, système de contrôle et monitoring, et se caractérise par des interdépendances complexes entre le cyberespace et le monde physique. Ils sont composés*

d'éléments de calculs, de communication, de contrôle, et d'éléments physiques, fortement intégrés [Che17][30].

Les CPS se caractérisent par leur emplois dans des domaines d'application hautement sensibles tels que l'énergie [VEM+15], la santé [STB17], ou encore le transport [MV16]. Comme tout système critique, un dysfonctionnement volontaire (cyberattaque, attaque physique, etc.) ou non (panne, erreur humaine ou matérielle, etc.) peut engendrer des conséquences inconcevables [Kni02]. Dégâts humains, dégâts matériels, ou encore dégâts environnementaux, ces conséquences varient selon le domaine d'application du système. Différents niveaux de criticité sont ainsi établis suivant l'impact possible des dysfonctionnements et selon le domaine d'application.

Les CPS sont associés à de nombreux défis pour répondre aux besoins du domaine d'application dans lequel ils sont employés. Il existe alors des défis spécifiques au domaine d'application, ainsi que des défis communs et généraux à tous les CPS. Volkan Gune *et al.* ont ainsi proposé 6 défis principaux associés à un système cyber-physique [GPGV14] : la fiabilité, la sécurité, l'exactitude, la durabilité, la prévisibilité, et l'interopérabilité. Parmi ces défis, la sécurité de ces systèmes est l'un des plus critiques. De par ces caractéristiques propres, les CPS sont exposés à un grand nombre de menaces et d'attaques. Rasim Alguliyev *et al.* ont regroupé les principales formes d'attaque et de menace sous forme de schéma [AIS18]. Yuriy Zacchia Lun *et al.* ont quant à eux particulièrement étudié les tendances de publications scientifiques traitant de la sécurité des CPS pour mieux comprendre comment cette problématique est abordée [ZLDS+18].

Parmi les 2828 publications, seulement 138 remplissaient tous leurs critères de filtration et ont donc été retenues. La distribution par année de ces publications est présentée dans la Figure I.7. On dénote notamment qu'aucune publication ne traite de la sécurité des CPS avant 2009. On remarque aussi une forte augmentation du nombre de publications à partir de 2012. Cela peut s'expliquer par un intérêt croissant pour les méthodes et techniques associées à la sécurité de ces systèmes, suscité par l'impact sans précédent de la célèbre cyberattaque **Stuxnet** en 2010 [Kar11]. Enfin, 112 publications (81.2%) sur les 138 étudiées ont été publiées au cours de ces trois dernières années. Cela dénote bien que la sécurité des CPS est une problématique de recherche récente.

30. CPS can be considered as a confluence of embedded systems, realtime systems, distributed sensor systems and controls, which focus on complex interdependencies and integration between cyberspace and physical world, and are composed of tightly-integrated computation, communication, control, and physical elements

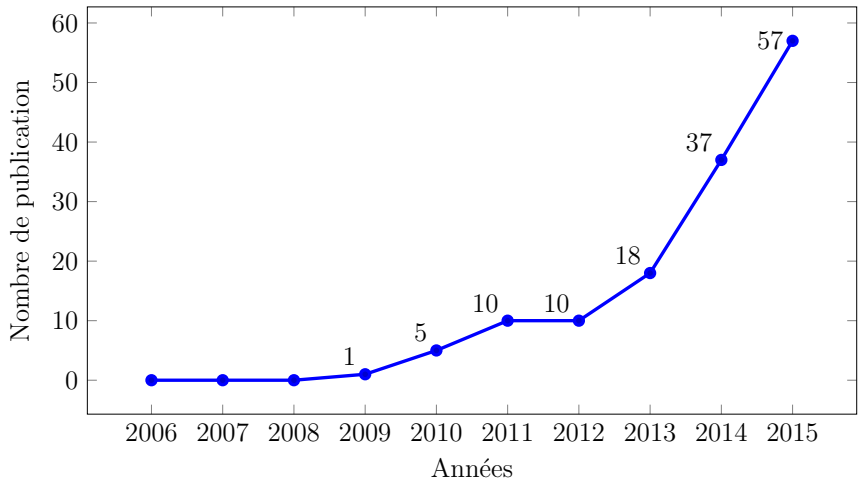


FIGURE I.7: Distribution du nombre de publications entre 2006 et 2015 (source des données : [ZLDS+18])

I.3.2 Architecture d'un CPS

Un système cyber-physique est composé par divers éléments définis par des caractéristiques spécifiques, et associés à des fonctions précises, selon le domaine d'application du CPS. Il est donc difficile de décrire tous ces systèmes à partir d'une architecture commune et générique. Le standard ANSI/ISA-95 [ISA], proposé par la Société Internationale d'Automatisation (*International Society of Automation*), permet néanmoins de décomposer les CPS à partir d'une architecte hiérarchique composée de cinq niveaux (Table I.1) [ISA]. Dans le cadre des travaux réalisés au cours de cette thèse, nous étudions plus particulièrement les niveaux 0, 1 et 2.

Les éléments des niveaux 0, 1 et 2 qui composent un CPS peuvent être dissociés en deux catégories principales : -les éléments physiques qui interagissent avec un processus physique, -les éléments numériques qui intègrent des capacités de calcul et/ou de réseau. Chacun de ces éléments participe à la réalisation du contrôle d'un processus physique donné [GPGV14]. Pour cela des **capteurs** mesurent différentes données à partir du processus physique pour les transmettre à un ***PLC (Programmable Logic Controller)***, ou API (Automate Programmable Industriel) en français,. Cet élément se caractérise par un programme de contrôle intégré qui permet de générer des commandes de contrôle proportionnelles aux données mesurées reçues. Ces commandes sont ensuite transmises aux différents **actionneurs** du CPS pour interagir avec le processus physique concerné. Il existe ainsi différents types de mécanismes de contrôle [Hop00], qui dans le cas des CPS, doivent impérativement s'opérer

TABLE I.1: Architecture hiérarchique d'un CPS selon le standard ANSI/ISA-95 [Las17].

Niveau	**Nom**	**Description**
0	Physique	Processus physiques
1	Capteurs, actionneurs et automates	Interaction de perception et d'action sur les processus physiques
2	Surveillance et contrôle	Interaction de surveillance et de contrôle sur les processus physiques
3	Opérations de fabrication	Définition des activités du flux de travail (*workflow*) pour la réalisation d'une tâche ou d'un produit désiré
4	Haute gestion	Management et réalisation des plans d'activité pour gérer la production

en **temps réel**.

L'ensemble de ce processus est surveillé et contrôlé à distance à partir de deux systèmes différents, selon l'application souhaitée. On distingue alors les systèmes de contrôle et d'acquisition de données (*Supervisory Control And Data Acquisition (SCADA)*), et les systèmes de contrôle distribués (*Distributed Control System (DCS)*). Un **SCADA** se définit comme un système qui combine des propriétés de collecte de données et d'informations, ainsi que de contrôle et monitoring [BW03]. L'affichage des données sur une station centrale fournit une aide décisionnelle à l'opérateur en charge du contrôle et monitoring des systèmes reliés au SCADA. Un SCADA s'étend généralement sur une zone géographique vaste, ce qui crée une forte dépendance avec les moyens de communication employés. Un **DCS** se caractérise comme un système d'acquisition et de contrôle composé de différents contrôleurs reliés aux équipements [AS14]. Ce type de système intègre aussi des fonctionnalités plus avancées telles que des interfaces homme-machine pour faciliter le contrôle et le monitoring effectués par les opérateurs. Un DCS se distingue principalement d'un SCADA par sa proximité géographique avec les équipements contrôlés. Il est généralement employé dans des espaces restreints tel que dans un navire.

La catégorisation en élément physique ou numérique des équipements employés dans un CPS n'est pas toujours évidente. En effet, certains équipements cumulent les propriétés des deux catégories. C'est par exemple le cas des ***smart components***, ou composants intelligents, qui interagissent avec des processus physiques et intègrent des capacités de communication pour optimiser la surveillance et le contrôle de processus physiques. Ils peuvent

ainsi être connectés à d'autres systèmes par le biais d'une connexion filaire, même si la tendance actuelle est à l'emploi de connexions sans-fils. L'utilisation de ces composants favorise l'apparition du concept d'*IoT*[31] dans les CPS [WW18]. Les récentes applications émergentes de ces problématiques, notamment celles basées sur l'intelligence artificielle, nécessitent de grandes capacités de calculs. Cependant, les composants *IoT* ne disposent pas des ressources informatiques suffisantes pour gérer ce type d'applications. De plus, il est parfois impossible de sous-traiter ces tâches de calcul à des ressources basées dans le *cloud*. Les latences élevées induites par l'utilisation de communication Internet ne correspondent pas aux exigences de réponse en temps réel pour des applications sensibles telles qu'associées à un CPS. En conséquence, selon le domaine d'application il est nécessaire de privilégier l'emploi d'équipements d'*edge computing*[32] dans un réseau local [LWXP19] pour satisfaire les exigences de latence et de sécurité.

I.3.3 Cyber-attaques visant les CPS

Comme nous l'avons noté dans la section I.3.1, la sécurité des systèmes cyber-physiques est l'un des enjeux majeurs associés à leur utilisation. En raison des vulnérabilités inhérentes à leur présence dans le cyberespace, et leur emploi dans domaines d'application critiques, les CPS sont des cibles de choix pour les cyberattaquants. Les fortes interactions entre les systèmes de contrôle et le monde physique caractérisant les CPS sont des sources majeures de perturbation, neutralisation, ou encore destruction des équipements, des infrastructures ou des installations critiques dans lesquelles ils sont employés. Nous détaillerons dans la suite de cette section les différentes vulnérabilités associées aux CPS, ainsi que les types d'attaques principaux qui les exploitent.

Vulnérabilités des CPS

Le NIST définit une vulnérabilité comme une faiblesse dans le système d'information (SI), dans ses procédures de sécurité, dans les contrôles internes, ou lors de son implémentation, qui pourrait être exploitée par une source de menace [SSCO08]. Dans le cadre des CPS un grand nombre de vulnérabilités est notamment découvert dans les éléments qui le composent, que ce soit les équipements, les logiciels ou les moyens de communication utilisés. D'autres vulnérabilités apparaissent dans la conception du système, ou lors de son

31. *Internet of Things*
32. informatique de périphérie

utilisation à partir de procédures et configuration inadaptées [SJ18]. Du fait qu'un système cyber-physique se caractérise comme un ensemble d'éléments hétérogènes, par leurs fonctions et propriétés, cela accentue la diversité des vulnérabilités auxquelles il est exposé. Ces vulnérabilités sont plus ou moins connues du grand public, et donc plus ou moins facilement exploitables. L'organisme MITRE, soutenu par le département de la Sécurité intérieure des États-Unis, fournit plusieurs bases de données de vulnérabilités sous forme de *Common Vulnerabilities and Exposures)*[33]. Chaque vulnérabilité connue est ainsi rendue publique sous forme d'un identifiant commun. Cela facilite le partage des informations entre les bases de données et les outils de sécurité informatique pour la correction des vulnérabilités identifiées dans le système employé. Yusuke Mishina *et al.* ont par exemple utilisé cette source d'information pour fournir une méthode d'analyse des menaces auxquelles est exposé un CPS [MTU18].

Types principaux de cyberattaques visant les CPS

Les vulnérabilités des CPS peuvent être exploitées par des attaques injectées, de façon discrète et imprédictible, à partir des éléments numériques du système [DSDB16]. De par les nombreuses vulnérabilités associées à ce type d'élément, il ne fait aucun doute que les cyberattaques représentent les menaces principales des CPS. Comme tout SI, les CPS possèdent un ordre d'importance des critères de sécurité : disponibilité, intégrité et confidentialité. Comme cela est détaillé dans la première ligne de la Table A.1 de l'Annexe A, l'ordre d'importance des critères est différent pour les systèmes OT (comprenant les CPS), et les systèmes d'information « classiques », aussi appelés systèmes IT. En conséquence, un cyberattaquant visera principalement à perturber le bon fonctionnement du système en le rendant indisponible ou en altérant l'intégration des flux de données et d'informations qui transitent en son sein. Parmi les types de cyberattaques particulièrement étudiées dans littérature, on dénote principalement [DHX+18], et par ordre d'importance [ZLDS+18] : les *deception attack*[34], les attaques par déni de service (*Denial Of Service (DoS)*), et les attaques par rejeu.

Une ***deception attack*** est un type de cyberattaque qui se caractérise par une altération des données et informations transmises entre les éléments numériques du système [DWHW16]. Le terme « attaque par injection de fausses données » est aussi employé pour désigner ce type d'attaque. L'objectif de cette attaque est d'impacter les mécanismes de contrôle du système [MS10] pour contraindre une commande de contrôle inadaptée à l'état

33. `https://cve.mitre.org/`
34. Attaque par tromperie

du processus physique à un instant t.

L'objectif principal d'une **attaque DoS** est de rendre le système, ou la ressource associée, indisponible. Pour cela, l'attaquant va généralement submerger de requêtes réseau le système cible. Et ce, jusqu'à ce que les requêtes associées au trafic normal ne puissent plus être traitées. On distingue alors différents sous-types d'attaques DoS selon les caractéristiques de celles-ci.

Les **attaques par rejeu** se définissent par la répétition ou le retard volontaire d'une transmission de données entre des éléments du système. Pour la perpétrer, un cyberattaquant enregistre les données transmises dans le réseau puis les réinjecte dans celui-ci. Ce type d'attaque est utilisé pour dégrader directement les performances d'un système, ou pour dissimuler une seconde attaque réalisée en parallèle. C'est notamment ce deuxième aspect qui a été utilisé pour réaliser l'attaque **Stuxnet**. La détection des attaques par rejeu est particulièrement difficile à mettre en œuvre, mais elle est d'une importance majeure pour la sécurité des CPS [YZG19].

Parmi les exemples les plus connus, la cyberattaque Stuxnet [Kar11] a permis aux attaquants de compromettre le système de contrôle des centrifugeuses iraniennes d'enrichissement d'uranium en exploitant plusieurs vulnérabilités du système. Ils ont ainsi pu agir sur des paramètres critiques du système physique tel que la vitesse des rotors des centrifugeuses. Cela n'a pu être détecté car une attaque par rejeu dissimule les données issues de ce comportement anormal des rotors. Ce qui a induit la destruction d'environ un millier de centrifugeuses, et ralentit le programme nucléaire de l'Iran. Cela a été réalisé à partir d'une altération du programme embarqué dans les PLC en charge du contrôle des centrifugeuses. En raison de la nouveauté de l'attaque, sa sophistication, et les systèmes visés, cette cyberattaque est considérée comme l'une des plus marquantes, si ce n'est la plus marquante, dans le domaine de la sécurité des CPS [Den12].

I.3.4 Détection d'anomalies dans les CPS

La détection d'anomalies est une problématique majeure ayant fait l'objet de nombreuses études scientifiques dans divers domaines de recherche et d'application. Une anomalie est généralement définie comme un schéma de données non conforme par rapport au schéma attendu. Une anomalie peut être induite de façon malveillante (fraude bancaire, cyberintrusion, cyberattaque, etc.), ou non (panne d'un système, maladie, environnement, etc.)

Selon les domaines d'application, la détection d'anomalie sera donc associée à une fonction et une notion différente. Par exemple, une légère variation du comportement normal dans le domaine médical (e.g. une variation du taux de la protéine C-réactive [35] dans le sang) sera considérée comme une anomalie. Tandis que cette même variation dans un autre domaine d'application (e.g. la température d'un élément d'un système) sera considérée comme normale.

Il existe donc d'innombrables définitions associées à cette notion, en fonction du domaine d'application. Une définition générique qui est applicable à tous les domaines, dont les CPS, est la suivante :

La **détection d'anomalie** consiste à identifier des schémas de données non conformes par rapport au comportement attendu. [CBK09] [36]

Dans le cas des CPS, leur diversité d'emploi dans des domaines d'application différents engendre des propositions de méthodes de détection d'anomalie spécifiques à ces mêmes domaines. Les réseaux électriques *intelligents* [SLX16], les véhicules autonomes [KLYM19], les dispositifs médicaux [MC14], ou encore les processus industriels [YZY+17] sont autant de domaines particulièrement traités dans la littérature. Parmi les techniques proposées, nous allons détailler dans les paragraphes suivants celles qui sont le plus utilisées. Dans le cadre de nos travaux traitant de l'analyse de la propagation d'anomalies, nous avons principalement utilisé la méthode de détection par analyse de la qualité des données. Nous détaillerons alors davantage cette méthode.

Apprentissage automatique

L'apprentissage automatique (« *Machine Learning* » *(ML)* en anglais) constitue un ensemble de techniques d'IA octroyant à une machine la possibilité de résoudre au mieux un certain nombre de tâches à partir d'un algorithme. Ces techniques se caractérisent par une phase d'apprentissage qui permet la dissociation de différents types d'algorithmes. On distingue ainsi l'apprentissage supervisé, non supervisé, et par renforcement. Les techniques de ML sont particulièrement employées pour répondre à diverses problématiques des CPS, dont la détection d'anomalie [RKR+20]. L'avantage principal de ce type de méthode est

35. Une protéine sécrétée par le foie dont le taux de concentration dans le sang augmente rapidement suite à une inflammation, ou à une infection dans l'organisme.

36. Anomaly detection refers to the problem of finding patterns in data that do not conform to expected behavior.

de pouvoir automatiser des tâches de détection d'anomalies complexes, incapables à traiter avec des méthodes classiques. Ce type de méthode présente néanmoins un certain nombre de limitations, notamment sur la grande quantité de données nécessaire pour entraîner correctement l'algorithme utilisé. De plus, selon la complexité des données analysées, les résultats de détection peuvent être longs à obtenir. Nous détaillerons dans les paragraphes suivants diverses méthodes de détection d'anomalies basées sur le ML.

Classification

Les techniques de détection d'anomalie par **classification** sont basées sur un modèle permettant de distinguer une donnée « normale », d'une donnée « anormale ». Pour cela, un apprentissage du modèle, à partir de jeux de données étiquetées, est nécessaire. Cette technique se caractérise ainsi par deux phases principales : -la phase d'apprentissage du modèle, -et la phase de classification des données. De nombreuses méthodes de détection découlent de cette technique.

Les **machines à vecteur de support** (*Support Vector Machine (SVM)*) sont des techniques, nécessitant un apprentissage supervisé, utilisées par le ML pour la classification de données. Le principe général de cette méthode est de définir une « frontière linéaire », appelée hyperplan, optimale pour séparer un ensemble de données en deux catégories. Ainsi les SVM sont qualifiés de *classifieurs linéaires*. La difficulté de cette technique réside donc dans la définition de l'hyperplan. S'il n'existe aucune solution linéaire, une fonction de transformation *kernel* peut être appliquée. Clet Boudehenn *et al.* ont par exemple utilisé cette méthode pour détecter des anomalies dans des jeux données issues de systèmes maritimes de navigation [BJL+21]. Parmi l'ensemble des limitations associées à cette technique, la définition de la fonction de transformation est l'une des principales tant celle-ci est critique pour les résultats en sortie. De plus, comme toute méthode de ML, le temps de traitement des données peut être particulièrement long selon leurs complexités.

Un **réseau de neurones** est un algorithme de classification dont le fonctionnement est directement inspiré de celui des neurones biologiques. Les méthodes de détection d'anomalie basées sur ce type d'algorithme sont caractérisées par deux étapes majeures. Premièrement, le réseau neuronal subit une phase d'apprentissage des classes normales à partir d'un jeu de données d'entraînement. Une fois l'apprentissage effectué, le réseau peut fonctionner normalement en lui fournissant en entrée les données à classifier. Chaque instance est alors classifiée comme normale ou anormale. Parmi l'ensemble des types de réseaux de neurones

existants, ceux associés aux méthodes de *deep learning* sont particulièrement employés depuis plusieurs années pour la détection d'anomalies dans les CPS [LXC+21]. Les réseaux de neurones fournissent ainsi une technique de classification autonome dont l'architecture se caractérise par son adaptabilité. Une de ses limitations principales réside dans la capacité de calcul nécessaire pour la mettre en œuvre. De plus, la quantité de données d'entraînement doit être particulièrement importante.

Parmi les méthodes de classification employées pour les CPS, on distingue notamment celle des **réseaux bayésiens**. Cette méthode repose sur une représentation graphique probabiliste qui modélise une structure, et permet de calculer la probabilité de situations particulières. Cette structure est alors plus ou moins complexe, elle peut à la fois représenter un sous-système, un système, ou même un système de systèmes sociotechniques maritimes [PSHB20]. L'ensemble des probabilités associées aux variables de la structure sont stockées sous forme de table de probabilité (les paramètres). Les réseaux bayésiens ont par exemple été utilisés dans les CPS pour détecter les menaces auxquelles est exposé un véhicule autonome [BLGA17]. Une des limitations de cette méthode se caractérise par la difficulté à obtenir des probabilités représentatives selon le cas applicatif.

D'autres techniques de classification, telles que la définition de **règles** pour définir le comportement normal du CPS, sont aussi utilisées pour la détection d'intrusion [SLX16].

Modèles statistiques

Les **modèles statistiques** de détection d'anomalies caractérisent le système étudié producteur de données à partir d'un modèle stochastique. Ainsi, une méthode de détection basée sur ces techniques définit une anomalie comme une donnée qui n'a pas été produite par un modèle stochastique particulier. Ces techniques de détection sont alors basées sur la supposition suivante : *les données normales se concentrent dans les régions de haute probabilité, tandis que les anomalies se produisent dans les régions de faible probabilité* [CBK09]. Différentes techniques de détection d'anomalies basées sur des modèles statistiques ont particulièrement été étudiées dans la littérature [ZLDS+18]. On distingue principalement les techniques basées sur un modèle gaussien, la méthode des moindres carrés, ou encore les filtres de Kalman. Le principal inconvénient des modèles statistiques est qu'elles reposent sur l'hypothèse que les données sont générées à partir d'une distribution particulière, or cette hypothèse ne se vérifie pas toujours.

Détection par évaluation de la qualité des données et des informations

L'étude de la qualité des données et de l'information est un concept pluridisciplinaire particulièrement associé aux systèmes, et source de nombreux défis. Ce lien s'est particulièrement renforcé avec l'apparition du concept de *Big Data*. L'augmentation exponentielle de données générées, traitées, et analysées au sein d'un même système a engendré de nouveaux challenges liés à l'étude de la qualité des données et de l'information. De par leurs caractéristiques inhérentes, les CPS sont particulièrement concernés par les problématiques associées à la qualité des données. Souvent qualifié de système « basé sur la donnée » (*data-driven system*) de nombreux défis et opportunités sont associés à l'évaluation de la qualité des données dans les CPS [SZ15]. La majorité des recherches scientifiques ayant traité ce sujet ont proposé des méthodologies appliquées, et applicables, à des domaines précis. Les domaines principalement étudiés sont les systèmes de santé connectés [SYM+16], les réseaux de capteurs [Alw21], ou encore les réseaux *intelligents* de distribution d'électricité [GCRP19].

Contrairement à ces études, Pedro Merino Laso *et al.* ont défini et fourni une méthodologie générique d'évaluation de la qualité pour la détection d'anomalies dans les CPS [LBP16]. Cette méthodologie basée sur la pyramide DIKW (*Data-Information-Knowledge-Wisdom*) fournit une quarantaine de métriques d'évaluation de la qualité pour chaque dimension de celle-ci [Las17]. Ils définissent plus précisément les flux de données et informations circulant au sein d'un système cyber-physique comme tel :

$$Information = \text{Donnée} + Contexte_{sous\text{-système}} + Contexte_{\text{système}} \tag{I.1}$$

Cette méthode multicritère se caractérise notamment par sa généricité et sa polyvalence d'application. De plus, elle est particulièrement adaptée à la contrainte de réponse en temps réel inhérente aux CPS. Sa principale limitation réside dans l'identification et la mise en place des critères et d'évaluation qui sont répétées pour chaque élément du système étudié.

I.3.5 Choix de la méthode de détection

Chacune des méthodes présentées se caractérise par différents avantages et limitations d'application. En accord avec le cadre applicatif de ces travaux de thèse, il est nécessaire de considérer l'ensemble des contraintes et caractéristiques associées aux SIM, et plus précisément aux CPS maritimes. Comme nous l'avons détaillé précédemment dans la section

I.2.1, les SIM se caractérisent par une forte hétérogénéité, tant au niveau de leurs fonctions que de leurs propriétés. Il est alors obligatoire de choisir une méthode de détection particulièrement polyvalente et générique. En complément, comme identifié dans la section I.3.2, la prise en compte de la contrainte de réponse en temps réel est essentielle à toute solution proposée pour répondre à toute problématique émanant des CPS. De plus parmi l'ensemble des méthodes présentées, une grande partie d'entre elles nécessite des jeux de données d'entraînement conséquent. Or dans le cadre applicatif des CPS, et plus particulièrement des CPS maritimes, l'obtention de jeux de données représentatifs est particulièrement difficile en raison de la confidentialité inhérente des domaines d'application critiques. La grande majorité des méthodes présentées nécessitent également de grandes capacités de calcul, ce qui n'est pas en accord avec les caractéristiques d'une majorité de secteurs d'application de ces systèmes.

Pour l'ensemble de ces raisons, nous avons fait le choix de considérer exclusivement la méthode de détection d'anomalies par évaluation de la qualité telle que proposée dans les travaux de recherche de Pedro Merino Laso [Las17]. L'objectif de nos travaux étant centré sur l'évaluation de la propagation d'anomalies dans les CPS maritimes, il est primordial d'utiliser une méthode de détection adaptée aux contraintes de ces systèmes. En accord avec les limitations de nos cas d'étude, nous avons restreint l'emploi de cette méthode à l'évaluation de la qualité des données et des informations. Nous considérerons alors exclusivement les deux premiers niveaux de la pyramide DIKW, et les métriques qui en découlent. Ces métriques sont regroupées au sein du vecteur d'évaluation de la qualité par dimension concernée. Sont ainsi définis le vecteur d'évaluation de la qualité des données ($\overrightarrow{DQV}$), et celui de l'évaluation de la qualité des informations ($\overrightarrow{IQV}$). Dans le Chapitre III, nous détaillerons plus précisément les métriques employées pour chaque cas d'application de nos travaux.

I.4 Analyse de la propagation d'anomalies

Il est développé dans les sections suivantes les différents aspects liés à l'analyse de la propagation d'anomalies dans un système. Premièrement, nous définirons la notion de « dépendance », qui est intrinsèquement associée à la problématique de recherche. Puis nous présenterons les solutions principales, proposées dans la littérature scientifique, pour répondre à cette problématique. Parmi l'ensemble des conséquences potentielles résultantes de la propagation d'anomalies dans des systèmes interdépendants, la défaillance en cascade est une des plus critiques. Nous détaillerons tous les aspects de ce concept à la fin de ces

sections.

I.4.1 Définition de la notion de « dépendance »

Avant de traiter de la problématique des dépendances entre les systèmes, il est nécessaire définir de manière générique et inclusive la notion de « système ». L'INCOSE (*International Council On Systems Engineering)* définit cette notion telle que présentée dans la Définition I.7.

Definition I.7. *Un système est un arrangement de parties ou d'éléments qui ensemble possèdent un comportement ou un sens, qu'ils ne posséderaient pas de manière individuelle*[37] *[SMM+19].*

En considérant cette définition, un système peut être à la fois étudié comme un **ensemble unifié**, et comme une agrégation **de parties, d'éléments, ou de composants, interconnectés ou interdépendants**. Cette dualité est caractérisée dans la littérature par deux perspectives différentes [VPQVS16] : une perspective interne, pour décrire les composants en interaction qui composent un système (Figure I.8 (a)), et une perspective externe, qui définit le système comme un ensemble (Figure I.8 (b)).

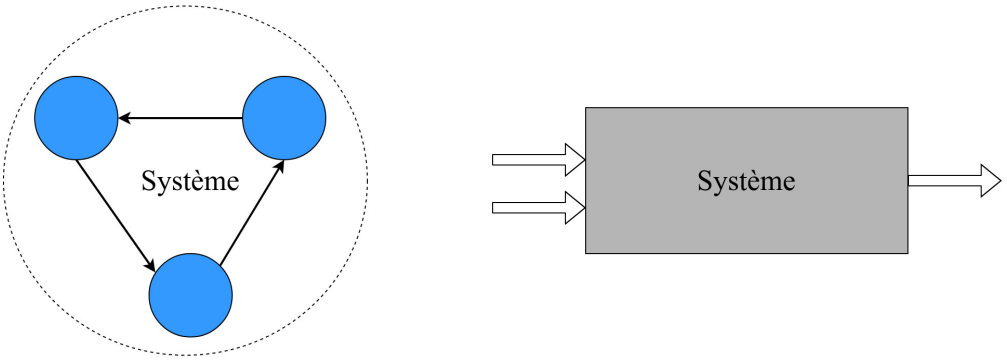


FIGURE I.8: Différentes perspectives de représentation et d'analyse de système

Bien souvent les termes « dépendance », « connectivité », « interaction », et « connexion » sont utilisés dans la littérature pour caractériser l'impact d'un élément sur un autre, ou

37. A system is an arrangement of parts or elements that together exhibit behavior or meaning that the individual constituents do not.

un échange entre eux. Dans la majorité des cas ces notions sont employées sans même les définir, alors que leur sens diffère selon le domaine d'application.

Concernant la notion d'interaction, celle-ci est majoritairement utilisée en science de l'ingénierie des systèmes et donc directement associée à la notion de « système ». William D. Schindel définit un système comme « *un ensemble de composants en interaction* », à cela se greffe la notion d'interaction entre deux éléments qu'il caractérise à partir de plusieurs aspects [Sch13] :

- Une « interaction » entre deux composants d'un même système signifie que l'un des composants modifie l'état de l'autre par le biais de l'échange d'énergie, de force, de masse ou d'informations.
- L'« état » d'un composant désigne une de ses propriétés, évolutive au cours du temps, qui influence son comportement dans d'autres interactions à différentes temporalités.
- Le comportement d'un composant, défini par plusieurs interactions, est associé à son état. Réciproquement, l'évolution de son état est associée à ses interactions.

La différenciation entre la dépendance et la connectivité reste néanmoins plus marquée. Dans le domaine de recherche de l'étude des réseaux, Roni Parshani *et al.* [PBH11] définissent la connectivité comme un lien entre deux éléments du réseau leur permettant de fonctionner et de coopérer. Ils caractérisent aussi la dépendance comme un lien entre deux éléments unifiant leur défaillance. Grâce à ces éléments de réponse, on peut distinguer une différence fondamentale entre la connectivité et la dépendance [Yan20] : pour un lien de dépendance entre deux éléments d'un réseau, si l'un est défaillant l'autre le sera forcément aussi (avec une certaine probabilité), ce qui n'est pas le cas pour le lien de connectivité. En science de l'ingénierie, et plus précisément en ingénierie des exigences, un lien de dépendance entre deux entités caractérise le fait qu'une entité bénéficiaire dépende d'une entité émettrice pour atteindre un objectif, exécuter une tâche ou fournir une ressource [Yu96]. Le type de dépendance décrit alors la nature de l'engagement entre les deux entités. Par conséquent, si l'entité bénéficiaire ne reçoit pas l'engagement de l'entité émettrice, elle sera impactée dans la réalisation de ses objectifs.

Georgios Kavallieratos *et al.* [KKG20], exploitent à la fois la notion de connexion et de dépendance entre différents systèmes cyber-physiques maritimes. Ils définissent ainsi une « connexion » entre deux CPS lorsqu'il existe un échange d'informations entre eux. De surcroît, ils caractérisent le lien de dépendance entre deux CPS lorsque l'état de l'un influence l'état de l'autre. Bien que ces définitions soient assez vagues, il est intéressant de

souligner l'ajout d'une caractéristique de direction à ces notions. Une connexion bilatérale entre les CPS, i.e. un lien d'échange d'informations bidirectionnel, est définie comme une « interconnexion ». De même pour une dépendance bilatérale qui est définie comme une « interdépendance ». Dans le cas d'étude proposé, ils font cependant un amalgame de ces définitions et finissent par seulement employer les termes de « dépendance » et « interdépendance ».

Frederic Petit *et al.* [PVB+15] apportent quant à eux des éléments de réponse bien plus précis concernant la définition de la notion de dépendance. Ils définissent une dépendance comme «*une relation unidirectionnelle entre deux éléments (e.g., une infrastructure critique, une entreprise, une organisation, ou une installation) où les opérations de l'élément A affectent les opérations de l'élément B* »[38] (Figure I.9 (a)). Cette définition peut être illustrée par le cas d'exemple suivant : il existe une relation de dépendance entre un système de refroidissement de l'air et un PLC qui contrôle ses opérations. De la même façon ils caractérisent une interdépendance comme «*une relation bidirectionnelle entre deux éléments où les opérations de l'élément A affectent les opérations de l'élément B, et les opérations de l'élément B affectent ensuite les opérations de l'élément A* »[39] (Figure I.9 (b)). Pour reprendre le cas d'exemple précédent : il existe une interdépendance entre le système de refroidissement de l'air, contrôlé par le PLC, lui-même refroidit par ce même système de refroidissement. Ils observent aussi qu'une interdépendance peut être considérée comme une combinaison de deux dépendances, chacune associée à une compréhension, une évaluation et une caractérisation spécifique (Figure I.9 (c)).

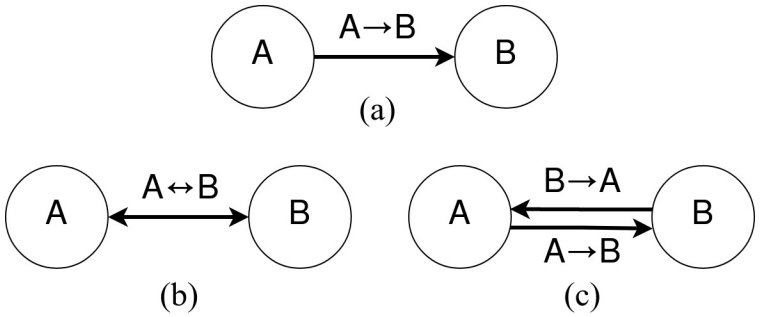


FIGURE I.9: Différences entre la notion de dépendance et interdépendance

Outre les diverses approches utilisées pour définir la notion de dépendance, S.M. Rinaldi *et al.* associent 6 dimensions distinctes à cette notion pour la qualifier dans un contexte

38. A dependency is a unidirectional relationship between two assets (e.g., critical infrastructure, firm, organization, or facility) where the operations of Asset A affect the operations of Asset B.

39. An interdependency is a bidirectional relationship between two assets where the operations of Asset A affect the operations of Asset B, and the operations of Asset B then affect the operations of Asset A.

d'étude d'infrastructures critiques [RPK01]. Nous définirons par la suite ce qu'est une infrastructure critique. Ces dimensions sont à la fois associées à la relation de dépendances, et aux infrastructures critiques impliquées. Une dimension, parmi les 6 proposées, est particulièrement intéressante pour nos travaux de recherche. Il s'agit de la dimension qui catégorise les dépendances entre 4 types distincts, mais qui ne s'excluent pas mutuellement. Les 4 types de dépendances proposées sont :

- Physique, un élément est physiquement dépendant d'un autre si son état de fonctionnement dépend de la production matérielle d'un autre élément. Le tout réalisé par le biais d'un lien fonctionnel et structurel.
- *Cyber*, un élément possède une relation de cyber-dépendance si son état de fonctionnement dépend de la transmission de données, ou d'information, par un autre élément. Le tout réalisé par différents moyens de communication.
- Géographique, un élément est géographiquement dépendant si un évènement environnemental peut modifier son état de fonctionnement.
- Logique, un élément est associé à une dépendance logique si son état de fonctionnement dépend de l'état d'un autre élément par un mécanisme qui n'est pas physique, cyber, ou géographique. Une dépendance logique est imputable à des décisions et actions humaines qui ne seraient pas le résultat de processus physiques ou cyber.

Comme nous venons de le présenter, ces notions sont complexes et les nombreuses définitions, parfois imprécises, proposées dans la littérature ne font que renforcer cet aspect-là. Il existe néanmoins des similitudes entre la définition de la notion d'interaction proposée par William D. Schindel [Sch13], et celle de la notion de dépendance énoncée par Frederic Petit *et al.* [PVB+15]. Nous étudierons dans la suite de cette section les principaux domaines de recherche traitant de la problématique des dépendances. De ce fait, nous considérerons la notion de dépendance à partir de la définition qui suit.

Definition I.8. *Un lien de dépendance entre deux éléments caractérise une relation unidirectionnelle d'un élément A vers un élément B, par un échange physique, cyber, géographique, ou logique. Cet échange affecte ainsi, positivement ou négativement, les opérations de l'élément de B.*

I.4.2 Analyse structurelle des systèmes

Comme il a été défini précédemment (Définition I.7), un système est considéré comme une association structurée d'éléments, sous-systèmes ou composants, qui interagissent d'une

manière organisée pour accomplir une finalité commune. L'analyse structurelle d'un système, composante primordiale de l'ingénierie système, consiste alors à décrire ses composants et les dépendances qui existent entre eux. Lorsque cette analyse est réalisée à partir d'un modèle de représentation mathématique, tel qu'un *graphe*[40], différentes propriétés structurelles en découlent. Ces propriétés peuvent alors être traduites à partir de diverses métriques pertinentes pour l'évaluation de l'impact d'une potentielle propagation d'anomalies dans le système étudié [XBM21]. L'analyse structurelle permet alors de répondre aux questions suivantes : de quoi est composé le système ? comment est organisé le système ? En cas de propagation d'anomalies, quels sont les impacts potentiels ? Dans cette section, nous étudierons principalement l'état de l'art de l'analyse structurelle des CPS et des SIM.

Analyse structurelle des CPS

L'analyse structurelle d'un CPS nécessite un modèle de représentation et d'étude le plus générique possible pour s'adapter à leur hétérogénéité inhérente. De nombreux travaux scientifiques tirent profit de la modélisation abstraite des graphes pour faciliter cette analyse. Nous détaillerons dans une section suivante ce type de modèle au travers de leurs fonctions, caractéristiques, et avantages. Dans la littérature, la modélisation d'un CPS sous forme de graphe se caractérise principalement par une représentation des sous-systèmes sous forme de nœuds. Les dépendances entre ceux-ci sont quant à elles représentées à partir d'arêtes entre ces mêmes nœuds. Cela est notamment le cas du modèle proposé par Aida Akbarzadeh *et al.*, qui se base sur la théorie des graphes pour à la fois modéliser les dépendances internes et externes d'un CPS [AK21]. En complément, quatre paramètres quantitatifs d'évaluation des dépendantes sont fournis : l'*Impact of Dependency*, la *Susceptibility of Dependency*, le *Weight of Dependency* , et la *Criticality of Dependency*. Elles sont majoritairement basées sur l'évaluation topologique des éléments du graphe. Agostino Sturaro *et al.* ont quant à eux modélisé un CPS de production d'électricité sous forme de graphe pour représenter ses composants, et ses diverses dépendances associées, pour analyser la propagation de défaillance [SSCD18].

D'autres études utilisent une représentation sous forme de graphe multicouche pour analyser les dépendances entre CPS, et intra-CPS. Yingrui Zhang *et al.* ont notamment tiré profit de cette représention pour modéliser et analyser les potentielles défaillances en cascade résultantes de dépendances entre réseaux de CPS [ZY18]. Le graphe généré est

40. Une structure mathématique dont nous détaillerons les caractéristiques dans les sections suivantes.

alors composé d'un nombre fini de couches associées à chaque réseau étudié. D'autres études modélisent les CPS, et les dépendances qui les composent, comme un graphe multicouche défini à partir de deux couches principales. Ces deux couches sont définies à partir des éléments qui les composent. On distingue alors une couche associée aux éléments numériques (aussi appelés « *cyber* »), et une deuxième couche composée des éléments physiques. Une étude a précisément caractérisé ces deux couches distinctes, mais communicantes, au sein d'une méthode d'évaluation quantitative de propagation des risques dans un réseau de CPS utilisés pour la distribution d'électricité [QZQ+18]. Le modèle de représentation associé à cette méthode est ainsi spécifique au domaine de recherche concerné. Les couches physique et *cyber* du modèle proposé sont uniformément définies à partir d'un graphe *non pondéré* et *non orienté*.

Koosha Marashi *et al.* ont quant à eux utilisé cette représentation de graphe multicouche, *cyber* et physique, pour définir et évaluer quantitativement les interdépendances composant un CPS [MSH16]. Comme cela est illustré dans la Figure I.10, chaque couche est associée à un graphe de dépendance *pondéré* et *orienté*, composé de nœuds représentant des éléments *cyber* (C_i), ou physiques (P_i). Quatre types de dépendances sont définis pour caractériser les différents échanges au sein d'un CPS. La pondération définie à chacune d'entre elles représente le *degré d'influence* d'un élément du graphe sur un autre. Cette valeur comprise dans l'intervalle $[0, 1]$ est définie de manière arbitraire selon différents cas de figure. Elle peut ainsi être calculée à partir des connaissances d'un expert, de retour d'expériences ou de simulations, ou encore grâce à diverses informations. Différentes métriques d'évaluation des dépendances sont calculées à partir des paramètres de ces dépendances (nombre, direction, poids, etc.). Cette méthodologie a exclusivement été testée sur un cas d'étude de CPS employé pour la distribution d'électricité [MSH17].

Analyse structurelle des SIM

L'analyse structurelle est un besoin critique pour un système complexe tel qu'un navire. Celle-ci doit être réalisée à partir de différents modèles de représentation spécifiques pendant l'ensemble du cycle de vie du navire, du développement au déploiement opérationnel, en passant par de multiples opérations de maintenance. Plusieurs modèles de représentation des dépendances et interdépendances au sein d'un navire ont ainsi été proposés pour divers besoins de modélisation associés à différentes phases de cycle de vie du navire.

En raison de la longue durée d'un navire, l'étape de conception est une phase fon-

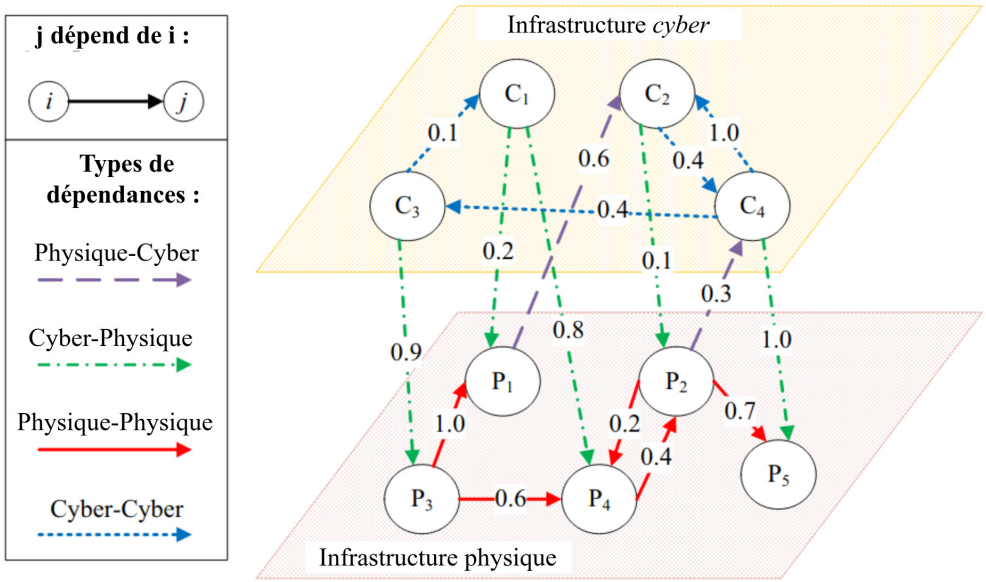


FIGURE I.10: Graphe de dépendances du CPS [MSH16] (adapté)

damentale de son cycle de vie. Durant celle-ci, différentes études et analyses sont menées pour traduire les exigences associées à la mission du navire, ou spécifiées par l'armateur, en caractéristiques architecturales et d'ingénierie navale [NZ19]. De par les potentielles conséquences critiques impliquées par les nombreuses dépendances des systèmes maritimes, il est nécessaire de les décrire et évaluer dès le stade de la conception à partir d'une analyse structurelle. Dorian Brefort *et al.* [BSH+18] ont ainsi défini un *framework*[41] de modélisation pour décomposer un système en un bloc architectural composé de trois représentations : physique, logique et opérationnelle. Ces représentations ont ensuite été utilisées pour décrire les dépendances entre les composants d'un système distribué donné. Pendant l'étape de conception les informations concernant les systèmes impliquées dans l'architecture, et les dépendances associées, sont néanmoins limitées. Or ces informations sont primordiales pour analyser la vulnérabilité du navire à partir de l'identification des défaillances des systèmes qui le composent et qui sont des potentielles sources de défaillance en cascade [GSS18]. Divers modèles ont ainsi été proposés pour évaluer la vulnérabilité d'un navire à partir de l'étude des dépendances entre les systèmes distribués le composant, et ce, en phase de conception. Différentes études caractérisent et remédient à la vulnérabilité causée par les fortes dépendances entre les systèmes maritimes en proposant diverses métriques d'évaluation

41. Structure

basées sur les caractéristiques d'architectures de système distribué. Giota Paparistodimou *et al.* ont ainsi fourni une nouvelle métrique de *robustesse*, basée sur la théorie des graphes, pour mesurer la capacité de l'architecture d'un système à maintenir un niveau d'exigence fonctionnelle après une perturbation [PDK+18]. Dans cette même idée, une autre étude a proposé différentes métriques d'évaluation de la vulnérabilité à partir d'informations issues d'un réseau multicouche. Ce réseau est modélisé sous forme d'un graphe où chaque nœud représentant un élément du réseau est associé à une couche spécifique parmi 4 proposées. Les couches sont reliées entre elles à partir d'arêtes entre les nœuds, symbolisant les différentes dépendances qui existent entre chaque élément du système [BGS+21].

À des phases plus avancées du cycle de vie du navire, l'analyse structurelle des SIM et des dépendances qui les composent reste un besoin majeur. En dépit de la conception, la représentation de l'architecture d'un système est un élément crucial pour implémenter, déployer et maintenir un système conformément aux spécifications données. Pour les systèmes simples, ces processus peuvent être réalisés de manière semi-formelle, par communication directe entre les différentes équipes impliquées. Cependant, cette approche n'est pas aussi facilement réalisable pour un système de systèmes (*System of Systems (Sos)*) complexes tel qu'un navire. De multiples équipementiers fournissent de nombreux systèmes hétérogènes et interdépendants, avec des exigences et spécifications profondément différentes. Une des solutions à cette problématique est le développement d'un modèle d'architecture de référence [URN+19]. Une architecture de référence décrit la structure d'un système à partir de ses composants, des interactions entre eux et avec leur environnement. La description de ces éléments permet de définir les restrictions et spécifications à considérer pour instancier l'architecture de référence et obtenir une architecture concrète. Une architecture de référence est ainsi générique pour un domaine d'application spécifique. Un modèle d'architecture de référence a spécifiquement été proposé pour représenter au mieux les divers systèmes maritimes, et les dépendances associées, qui composent un navire [RCL11]. Ce modèle se base sur une représentation multicouche des différents réseaux composant le navire. De la couche **instrumentation** à la couche représentant les **liens extérieurs**, ce modèle de référence permet de représenter les composants interdépendants du navire, impliqués dans l'échange de données et d'informations. Une architecture de référence pour représenter des réseaux maritimes est d'autant plus importante lorsque différents types de systèmes autonomes doivent communiquer et coopérer entre eux [RT14]. Le *Maritime Architectural Framework (MAF)*, une architecture de référence spécifique au domaine maritime, a également été explicitée pour faciliter le développement et l'intégration de nouveaux systèmes et de nouvelles technologies dans le domaine concerné [WHN16]. En s'appuyant sur les caractéristiques du *MAF*, Geor-

gios Kavallieratos *et al.* ont proposé un autre modèle d'architecture spécifiquement adapté aux *Cyber-Enabled Ship (C-ES)* [KKG20] (Figure I.11). Un *C-ES* est décrit comme un navire intégrant des CPS dans son architecture, et dont les opérations peuvent être entièrement ou partiellement autonomes. Il peut alors définir un navire conventionnel, téléopéré, ou autonome [KDK20]. L'architecture ainsi proposée est modélisée sous la forme d'un cube multidimensionnel, composé de différentes perspectives. Cela permet de fournir une représentation graphique du système et du domaine maritime associé. Au travers de cette représentation, les dépendances et interdépendances entre les systèmes du navire sont clairement explicitées afin de les analyser.

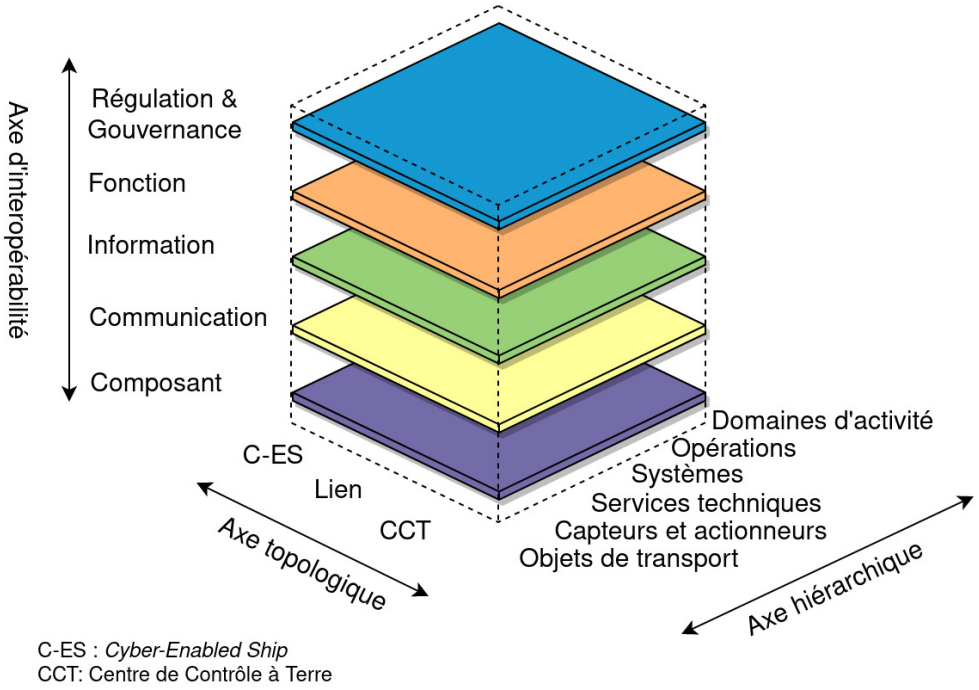


FIGURE I.11: Architecture MAF étendue (source : [KKG20])

La modélisation structurelle des dépendances et interdépendances fournit également des informations d'importance majeure lors des phases de déploiement opérationnel d'un navire. L'évaluation de l'impact de la propagation d'anomalie, en quasi-temps réel, est un besoin majeur. Afin d'atténuer et de remédier au risque associé, les opérateurs doivent à la fois être informés des dépendances existantes entre les éléments du système, ainsi que les magnitudes associées pour les comparer et évaluer au mieux le risque. L'analyse quantitative des dépendances est alors un besoin d'autant plus critique [LHS15]. Cette approche n'a encore été que trop peu considérée dans la littérature scientifique existante.

Comme nous venons de le voir la considération des dépendances, à partir d'une analyse

structurelle, est un besoin majeur pour les CPS, et d'autant plus pour les SIM. Lorsque cette analyse s'inscrit dans une démarche de modélisation adaptée, notamment à partir de graphe, elle constitue une solution pertinente pour fournir une représentation visuelle du système, ainsi qu'une formulation mathématique pour l'évaluation des impacts potentiels d'une propagation d'anomalies. L'ensemble de ces aspects est alors potentiellement exploitable pour fournir une aide décisionnelle à l'opérateur en charge de la surveillance et du contrôle du système. Cette approche présente cependant une limitation majeure. L'évaluation de l'impact de la propagation est exclusivement statique puisqu'elle s'appuie uniquement sur diverses métriques en lien avec les propriétés structurelles de la représentation du système.

I.4.3 Modélisation mathématique de la propagation

Les modèles mathématiques de propagation d'anomalies résultent principalement des études en épidémiologie [42]. De tout temps les populations ont dû faire face à de nombreux virus se définissant par des caractéristiques différentes, et des impacts sur celles-ci parfois majeurs. Depuis près d'un siècle [KM27], la communauté scientifique est capable de prévoir l'évolution temporelle de ces virus, avec plus ou moins de précision, grâce à divers modèles de propagation. La modélisation mathématique des maladies infectieuses permet de fournir des métriques scientifiques qui peuvent être exploitées pour l'épidémiosurveillance [43] de la maladie, mais surtout pour fournir des éléments de réponses quant à la prise de décision relative aux politiques de santé publique. L'épidémie de la COVID-19 est un exemple récent et pertinent qui souligne l'importance de l'apport de ces modélisations contre la lutte de la propagation d'un virus.

Parmi l'ensemble des solutions de modélisation dynamique de propagation de virus biologique, le modèle *Susceptible, Infected, Recovered (SIR)* est l'un des plus étudiés. Il illustre parfaitement le fonctionnement de la globalité des modèles mathématiques de propagation existants. Un nombre important de ces modèles s'appuie en effet sur les principes de base du SIR. Ce modèle est composé de la représentation de trois types d'individus, au sein d'une même population P étudiée : les individus sains (S), ceux qui sont infectés (I), ceux qui sont rétablis et qui ne peuvent plus être infectés (R). L'effectif de chacune de ces populations d'individus est évidemment variable dans le temps. De ce fait, l'évolution de la population P

42. Un domaine de recherche scientifique dont l'objectif est de déterminer les causes des maladies, ainsi que les facteurs ou marqueurs de risque influençant leurs survenues au sein d'une population.

43. Suivi de l'évolution des maladies et des agents pathogènes, et détection de l'émergence sur le territoire national d'un nouvel agent infectieux.

dans le temps est définie tel que : $P = S(t)+I(t)+R(t)$. Un système d'équations différentielles est ensuite dérivé de ces fonctions, en y intégrant des paramètres β [44] et γ [45], ainsi que R_0 [46]. Récemment, le modèle SIR a été employé pour l'étude de la dynamique de propagation de la COVID-19 [SJB21]. Outre son application en épidémiologie, ce modèle a aussi été largement employé dans divers domaines d'application en implémentant le modèle de base, ou en y apportant différentes spécifications liées aux cas d'études. Le SIR est notamment employé pour l'étude de propagation de virus informatiques dans différents types de réseaux. Miguel López *et al.* ont par exemple étudié la propagation d'une cyberattaque par *jamming* [47] dans un réseau de communication sans-fil d'équipements IoT [LPO19]. Il est aussi utilisé dans le domaine des réseaux sociaux pour analyser la propagation de *fake news* [48] [SKO+20, XCW+19].

Divers travaux scientifiques ont eux aussi spécifiquement traité de la modélisation mathématique de propagation d'anomalies dans les CPS, notamment le domaine d'application des réseaux électriques intelligents. À partir du modèle SIR, Tao Wang *et al.* ont par exemple modélisé mathématiquement la propagation d'un virus informatique dans la couche numérique de communication d'un CPS pour analyser les répercussions sur les éléments physiques du réseau de distribution d'électricité [WWH+19]. Cette étude a permis de démontrer qu'une anomalie dans le réseau de communication peut se propager et engendrer des impacts conséquents sur le réseau électrique. Boyu Zhu *et al.* ont quant à eux développé leur propre modèle mathématique de propagation en se basant sur le modèle SIR [ZDX+19]. Le modèle *Susceptible, Exposed, Infected, Recovered* résultant se caractérise par l'ajout d'un type d'éléments dans l'ensemble étudié : les éléments exposés (E) aux virus. Ce modèle est ensuite mis à profit pour analyser la propagation des risques liés à la sécurité de l'information dans un CPS en charge de la distribution de l'électricité. Les évaluations fournies par ce modèle sont des ressources intéressantes pour proposer un certain nombre d'indicateurs sur les risques encourus par le système selon sa structure. Martine Collard *et al.* se sont aussi en partie basés sur le SIR pour proposer un modèle de propagation multidimensionnelle de rumeurs [CBCS15]. Le modèle *ODS (Open-minded, Disseminator, Stifler)* résultant a notamment permis de mettre en avant les différentes caractéristiques de propagation associées à la notion de *rareté* de la rumeur considérée.

44. Taux d'infection.
45. Taux de guérison.
46. Nombre de reproduction effectif.
47. Un type d'attaque DoS qui empêche la communication dans le canal visé.
48. Fausses nouvelles.

En conclusion, l'ensemble de ces études traitant de la propagation d'anomalies (virus biologique, informatique, *fake news*, etc.) depuis la perspective d'un modèle mathématique, fournissent des éléments d'analyse pertinents quant à l'évolution dynamique de la propagation et de ses impacts. Elle permet aussi de tester et d'évaluer quantitativement des stratégies d'action en lien avec l'objet de l'étude. Néanmoins, la considération de ce type de modélisation présente un certain nombre de limitations d'usages. Tout d'abord l'ensemble de ces approches sont probabilistes, la pertinence des résultats obtenus dépend donc fortement de la bonne caractérisation des paramètres associés aux équations résultantes de la formulation mathématique. Deuxièmement, les modèles proposés se basent sur des approximations comportementales de l'objet étudié. Ce qui peut poser problème lorsque le comportement réel de l'objet étudié est particulièrement complexe. Ce qui est notamment le cas des CPS. Comme nous l'avons détaillé dans la section I.3.2, l'architecture d'un CPS se définit par un nombre élevé de dépendances entre divers sous-systèmes hétérogènes, de par leurs natures, leurs fonctions, ainsi que les protocoles de communication associés. Ces sous-systèmes se caractérisent par une dualité cyber-physique qui complexifie la modélisation de leurs comportements dans diverses analyses. En effet, les éléments physiques du CPS fonctionnent principalement en temps continu, tandis que les éléments numériques opèrent en temps discret [KK12]. Enfin, ces modèles permettent de formuler mathématiquement le problème de l'analyse de la propagation d'anomalies, mais ne fournissent pas de représentation adaptée à la visualisation de celui-ci. En conséquence, ce type de modélisation n'est pas forcément adapté pour fournir une aide décisionnelle en temps réel aux opérateurs assurant leurs contrôles et surveillances du système concerné. Selon le cas d'application, cette limitation est d'autant plus exacerbée par les ressources de calcul nécessaires à la mise en oeuvre de ces modèles. Pour conclure, ce type d'approche est plus adapté à des phases de validation ou vérification du système, qu'à des phases opérationnelles.

I.4.4 Graphes d'attaque

Comme nous l'avons évoqué précédemment dans la section I.2.3, les SIM, et plus généralement la globalité des SI, sont vulnérables aux cyberattaques. Leurs caractéristiques inhérentes, telles que les protocoles de communication, les logiciels, ou encore les équipements employés, induisent une multitude de vulnérabilités dont la considération et la remédiation sont des besoins critiques. La complexité, ainsi que les changements fréquents d'architecture et de configuration des SI ne font qu'accentuer la criticité de ces besoins. Cependant, la masse de données et d'informations à traiter peut facilement submerger les opérateurs en charge de

la sécurité informatique de ces systèmes [MBGJ]. Cela peut générer des réponses retardées, inadaptées, ou même inexistantes, face à ces incidents. Il est alors primordial de fournir une approche préventive, afin d'anticiper ces menaces, et d'y répondre, le plus rapidement possible. Ce qui limiterait l'impact de la propagation des anomalies générées par ces attaques dans l'ensemble du SI. L'utilisation de **graphes d'attaque** apparaît alors comme une solution pertinente pour identifier et évaluer les différents scénarios d'attaques auxquelles le SI est susceptible d'être soumis.

Le graphe d'attaque d'un système est une représentation succincte, basée sur la théorie des graphes, composée de tous les chemins d'attaques possibles. L'identification de ces **chemins d'attaque** est le principal avantage de cette représentation [AMMN+16]. Les prémices des graphes d'attaque ont été présentées dans les travaux de thèse de Marc Dacier en 1994, où il introduit le concept de *graphe de privilèges* [Dac94]. Le concept de graphe d'attaque a par la suite été davantage explicité en 1998 dans les recherches scientifiques de Cynthia Phillips, pour l'analyse de vulnérabilités associées à un système [PS98]. D'après Harjinder Singh Lallie *et al.*, les graphes d'attaques sont dissociables en 5 catégories distinctes : *générique* ; *corrélation d'alerte* ; *vulnérabilités* ; *divers* ; et *dépendances*[49] [LDB20]. L'identification des potentiels chemins d'attaque, en tant qu'objectif principal des graphes d'attaque, peut être facilitée par différents outils logiciels d'analyse de graphes d'attaque, présentés dans la littérature scientifique suivante : MulVAL [OGA+05], TVA [JNO05], ou encore NuSMV [AWK02]. Une étude complète sur les différentes méthodes d'analyse de graphes a été proposée par Jianping Zeng *et al.* [ZWC+19]. D'autres études, comme celle de Gustavo Gonzalez-Granadillo *et al.*, ont tiré profit du formalisme des graphes d'attaque pour fournir différentes contre-mesures qui identifient et atténuent l'attaque [GGDKGA17]. Concernant l'identification des chemins d'attaques, un certain nombre d'études ont tiré profit de l'algorithme de *Deep First Search (DFS)* pour réaliser cette tâche [PPM18, MD18, KK20].

Divers travaux de recherche ont appliqué les graphes d'attaque au domaine d'application des **CPS**. Khaled Karray *et al.* ont par exemple proposé une méthode de modélisation des composants de l'architecture cyber-physique d'un véhicule connecté, en se basant sur les graphes d'attaque [KDGE18]. Le modèle formulé se base sur la politique de sécurité mise en place, les informations détenues sur les différentes vulnérabilités des composants, ainsi que les divers droits d'accès associés. Concernant le secteur maritime, Georgios Kavallieratos *et al.* ont défini une méthode d'identification et d'analyse des chemins d'attaques dans les CPS maritimes interdépendants [KK20], à partir d'un graphe de dépendance. Elle fournit

49. Generic ; alert correlation ; vulnerability ; miscellaneous ; and dependency.

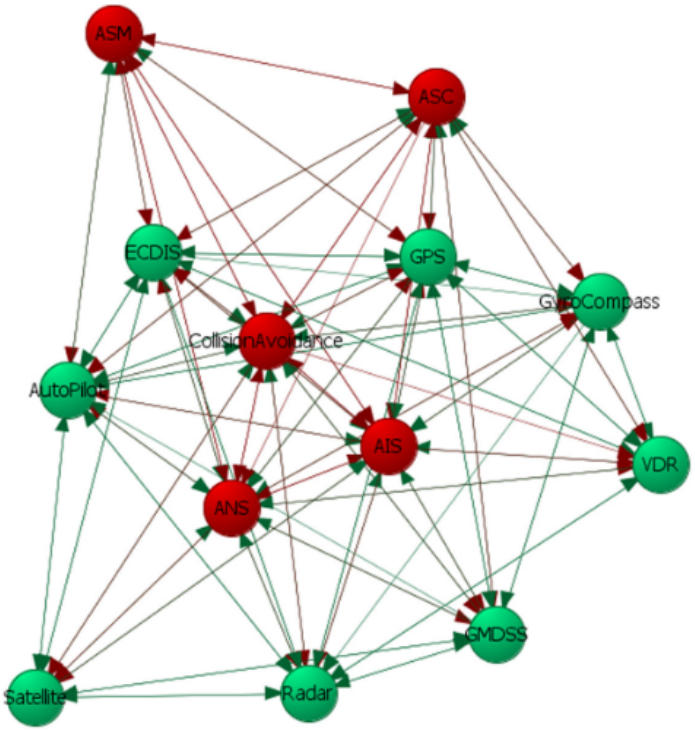


FIGURE I.12: Graphe de dépendance des CPS impliqués dans la navigation du C-ES [KK20]

à la fois les différents chemins potentiels de propagation de l'attaque, ainsi que les scores associés pour comparer la criticité de chaque chemin. Comme illustré dans la Figure I.12, cette approche a été testée sur les CPS impliqués dans la navigation du navire (C-ES). La valeur d'une métrique Z, formulée dans les travaux d'Aida Akbarzadeh *et al.* [AK20], est calculée pour chaque système (représenté sous forme de nœud) du graphe afin de caractériser leur criticité. Plus la valeur Z d'un système est faible, plus celui-ci est critique. Les nœuds de couleur rouge caractérisent ainsi les 5 systèmes dont la valeur de Z est la plus faible. Bien que le graphe résultant soit limité dans sa taille (seulement composé d'une dizaine de nœuds), il s'agit d'une première approche intéressante pour modéliser, analyser, et quantifier les chemins d'attaque, et donc de propagation, entre les SIM.

Dans certains cas d'étude, les graphes d'attaques présentent néanmoins diverses limitations. Lih-Hsing Hsu *et al.* ont par exemple mis avant l'explosion combinatoire associée à cette représentation lorsque le taille du graphe concerné est trop importante [HL08]. Ainsi, le concept de graphes d'attaques ne peut être appliqué qu'à des réseaux de systèmes de taille limitée [JNO05]. Pour des systèmes à plus grande échelle, il est nécessaire de réduire la complexité du graphe pour obtenir des analyses pertinentes, et dans des temps de calcul convenables, en accord avec les besoins du système étudié.

I.4.5 Comparatif des solutions d'analyse de la propagation d'anomalies

Comme nous venons de le présenter dans les sections précédentes, la résolution de la problématique de l'analyse de la propagation d'anomalies dans un système est associée à trois solutions majeures : l'**analyse structurelle**, la **modélisation mathématique**, et les **graphes d'attaque**. Chacune d'entre elles se définit par différents paramètres et propriétés. Au regard de leurs caractéristiques, il est difficile de qualifier ces solutions d'antagonistes. Il est plus approprié de les définir comme complémentaires, avec des attributs plus ou moins bénéfiques selon l'analyse souhaitée. Les apports et les limitations de chacune de ces trois solutions sont présentés dans la Table I.2.

TABLE I.2: Comparaison des solutions pour l'analyse de la propagation d'anomalies

	Apports	**Limitations**
Analyse structurelle	►Bonne représentation visuelle du système ►Métriques basées sur les propriétés structurelles	►Analyse statique
Modélisation mathématique	►Analyse dynamique ►Indicateurs d'évolution de la propagation ►Pluridisciplinaire	►Approche probabiliste ►Mauvaise représentation visuelle ►Ressources de calcul nécessaires
Graphes d'attaque	►Chemins de propagation	►Explosion combinatoire

Dans la section suivante, nous présentons un domaine de recherche majeur lié à la problématique de la propagation d'anomalie dans les systèmes qui exploitent les solutions présentées.

I.4.6 Défaillances en cascade dans les infrastructures critiques

Lorsqu'une anomalie se propage à l'échelle globale d'un système, les défaillances induites peuvent générer une **défaillance en cascade**[50] et impacter celui-ci de manière irréversible. Ce concept est fortement associé au domaine des **Infrastructures Critiques**

50. La défaillance d'un élément entraîne la défaillance d'un ou plusieurs autres.

(IC). Une infrastructure est définie comme un ensemble d'éléments, de systèmes, ou de réseaux, nécessaires au bon fonctionnement d'une entité. Lorsque cet actif est vital pour le fonctionnement d'une société ou de l'économie, on parle alors d'IC. Même si cette notion ne bénéficie pas d'une définition précise, et que chaque État possède une liste d'IC qui lui est propre, certains actifs restent communs à chacun. On dénote par exemple les systèmes de production d'électricité, les systèmes de gestion de l'eau, les hôpitaux, ou encore les réseaux de communications, etc. Bien que différentes dans leurs fonctions et caractéristiques, ces infrastructures se caractérisent par leur complexité [EPKP15]. Au niveau national, ces infrastructures sont identifiées à partir de 12 secteurs d'activités d'importance vitale. Des OIV sont alors caractérisés pour chaque secteur par arrêté ministériel. Comme nous l'avons défini dans la section I.2.4, cela est notamment le cas pour le sous-secteur des « Transports maritime et fluvial ». Production d'électricité, gestion de l'eau, service de soins, utilisation de l'énergie nucléaire, etc. : de par ses caractéristiques, un navire moderne peut être considéré comme une agrégation d'infrastructures critiques. Celles-ci sont interdépendantes, regroupées dans un espace physique limité, et assujetti à différentes contraintes environnementales et technologiques spécifiques qui complexifient leurs emplois.

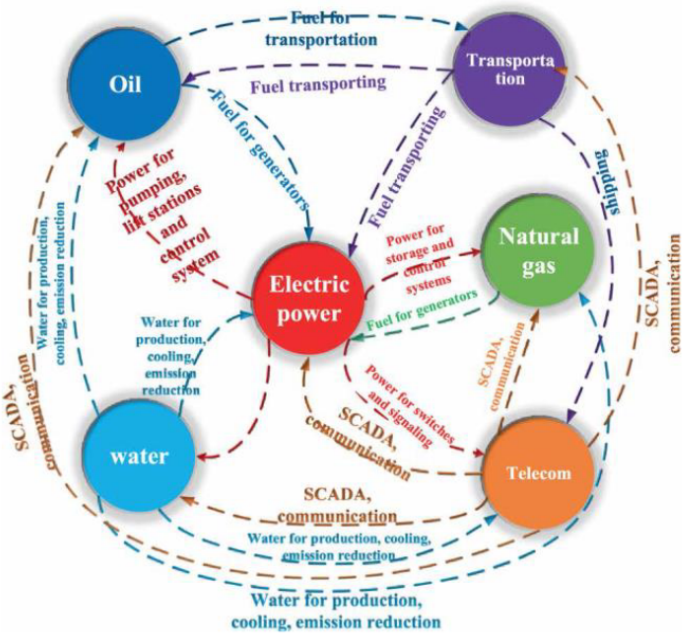


FIGURE I.13: Interdépendances entre différentes infrastructures critiques [BLLL17]

Ces infrastructures se caractérisent principalement par l'influence qu'elles exercent les unes sur les autres. Notamment les infrastructures de production d'électricité, dont

la ressource est vitale pour le fonctionnement des autres infrastructures. Zhaohong Bie, en s'appuyant sur les travaux de Richard G. Little [Lit03], a notamment illustré diverses interdépendances existantes entre différents types d'infrastructures critiques (Figure I.13) [BLLL17]. En raison de leurs potentiels impacts critiques, les défaillances en cascade, associées aux dépendances, sont particulièrement étudiées dans la littérature au travers de deux types de solutions majeures que nous avons présentés dans les sections précédentes : l'analyse structurelle et la modélisation mathématique.

L'analyse structurelle est principalement utilisée pour évaluer les performances globales d'un réseau constitué de plusieurs IC en cas de défaillance en cascade. Les principales propriétés structurelles étudiées sont la robustesse [QYL20], la fiabilité [DC15], et la résilience [YCM20]. Dans le cas spécifique du secteur maritime, Niamat Ullah Ibne Hossain *et al.* [HAJ+20] ont par exemple analysé l'impact d'une perturbation dans une chaîne logistique maritime (*maritime supply chain*) [VS20]. Pour cela ils ont proposé une modélisation des interdépendances entre les infrastructures portuaires et les différentes chaînes d'approvisionnement qui les entourent pour évaluer comment la défaillance de l'une d'entre elles peut déclencher une défaillance en cascade dans l'ensemble de la chaîne logistique. Le modèle proposé est ainsi constitué de trois types de dépendances : géographique, provision de services et accès pour réparation.

Le second aspect se focalise sur les différents mécanismes et modèles dynamiques probabilistes de propagation de défaillances. Différentes approches, associées à des modèles mathématiques probabilistes, ont par exemple été proposées. Ren Wendi *et al.* ont par exemple utilisé un modèle stochastique basé sur la théorie de l'état de transition pour étudier la dynamique des défaillances dans des réseaux de communication [RWZ+18]. Un modèle basé sur les réseaux bayésiens a aussi été proposé pour estimer l'impact de défaillances induites par un tremblement de terre sur des systèmes critiques [LCLP20]. Une autre étude combine diverses méthodes statistiques pour développer un modèle de propagation des défaillances basé sur des systèmes dynamiques discrets[WCZ+21].

Parmi l'ensemble des IC étudiées dans la littérature, nous pouvons aisément identifier deux types d'infrastructure majoritairement étudiés en raison de leur importance vitale. Il s'agit des infrastructures de gestion de l'électricité [KUG12] [JHZ13], et plus particulièrement celles associées à la gestion de l'eau [Bir17] [QMSC20] [RAMH18]. Cela s'explique par l'importance vitale de ces systèmes, ainsi que par les nombreux incidents récents subis. Concernant les infrastructures de gestion d'électricité, des *black-outs* électriques ont été récemment répertoriés en Amérique, en Europe, ou encore en Inde [Sun19]. En complément, d'autres

études se focalisent sur l'analyse, et les potentielles conséquences des interdépendances entre ces deux types d'infrastructures critiques [PTT+20] [TFN+19].

Comme nous venons de le présenter, l'étude de défaillances en cascade est particulièrement associée à la notion d'infrastructures critiques. Différentes méthodes d'évaluation de la propagation présentées dans les sections précédentes sont particulièrement employées. Parmi l'ensemble de ces méthodes, l'analyse structurelle du système semble particulièrement adaptée. Elle fournit à la fois une représentation visuelle, mais aussi un modèle mathématique, d'où différentes métriques structurelles peuvent résulter. Elle permet également la représentation des différents chemins de propagation à travers de la modélisation des dépendances entre les éléments du système étudié.

I.5 Théorie des graphes

La théorie des graphes est une discipline en Mathématique basée sur l'étude d'une structure abstraite de modélisation. Cette structure, un graphe, est définie comme un ensemble fini de « points » (ses « sommets ») reliés par des « traits » ou des « flèches » (ses « arêtes ») [CAB00]. La théorie des graphes est une discipline relativement récente en Mathématique. Son étude débute en 1736 avec la solution proposée par Leonhard Euler pour résoudre le problème de la traversée des ponts de la ville de Königsberg [Eul53] (Figure I.14). La modélisation du problème sous forme de graphe a permis de décrire les plans de la ville en ne gardant que les informations essentielles à l'objet de l'étude, ainsi que de traduire le problème sous forme mathématique.

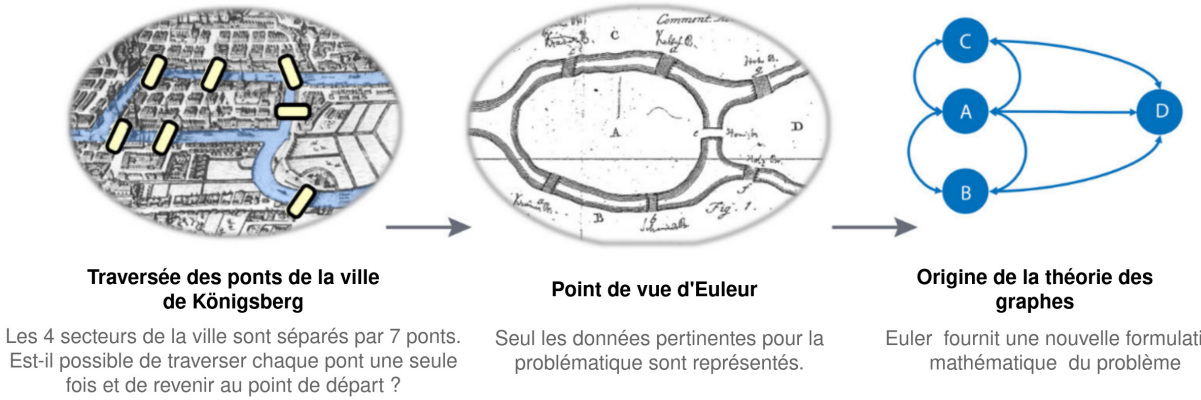


FIGURE I.14: Origines de la théorie des graphes [HN19] (adapté)

Cela fait alors apparaître les principales propriétés d'un graphe, qui sont respective-

ment l'**abstraction** et la **formalisation** mathématique. Depuis, la théorie des graphes se caractérise par sa pluridisciplinarité. Que ce soit en informatique, économie, biologie, gestion des réseaux, ou même en psychologie, de nombreux domaines d'application bénéficient des propriétés des graphes.

I.5.1 Définition et propriétés d'un graphe

Un **graphe** G est défini comme un couple formé de deux ensembles qui définissent respectivement ses *sommets* et ses *arêtes* (Équation I.2). L'ensemble S de ses sommets est défini tel que : $S = \{s_1, s_2, ..., s_n\}$, et l'ensemble A de ses arêtes se caractérise par : $A = \{a_1, a_2, ..., a_m\}$. Lorsque $a = \{x_i, x_{i+1}\} \in A$, on dit a est l'arête de G d'extrémité x_i et x_{i+1}. Les sommets x_i et x_{i+1} sont alors définis comme *adjacents*, x_i est l'extrémité initiale de a, et x_{i+1} son extrémité finale.

$$G = (S, A) \tag{I.2}$$

En complément, un graphe $H = (T, B)$ est considéré comme un **sous-graphe** de G, si et seulement si, $T \subseteq S$ et $B \subseteq A$.

Bien que les sommets et les arêtes d'un graphe peuvent être associés à un grand nombre de caractéristiques, certaines sont plus courantes et plus représentatives que d'autres. Cela est notamment le cas pour les caractéristiques de **direction** et de **pondération** associées aux arêtes. Ainsi, parmi les principaux types de graphes, nous nous intéresserons plus particulièrement aux graphes orientés et aux graphes pondérés.

Graphe orienté

Un graphe *orienté* G est constitué de deux ensembles : un ensemble de sommets $S = \{s_1, s_2, ..., s_n\}$, et un ensemble $A = \{a_1, a_2, ..., a_m\}$ issu d'une partie du produit cartésien $S \times S$, dont les éléments sont appelés *arcs*. La différence entre un graphe non orienté et orienté est présentée dans la Figure I.15.

Le concept de *chemin* est aussi directement associé à celle de graphe orienté. Dans un graphe orienté, on appelle un *chemin* toute suite finie de sommets $(s_1, s_2, ..., s_k)$ tels que, pour tout i, il existe une arête de s_i vers s_{i+1}. La longueur du chemin est définie par le nombre

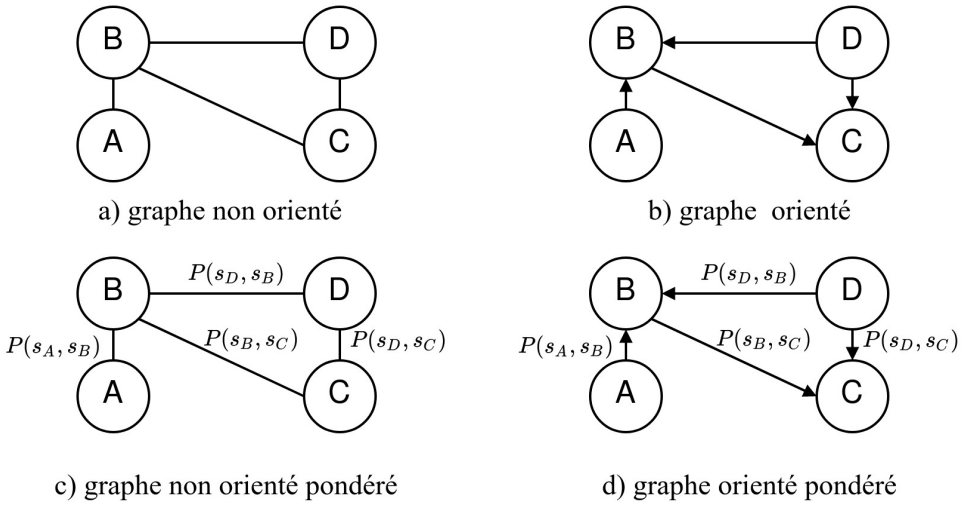


FIGURE I.15: Différences entre les différents types de graphes selon leurs caractéristiques d'orientation et de pondération

d'arêtes traversées, soit 1 de moins que le nombre de sommets visités. Le chemin concerné dépend évidemment de l'orientation des arcs.

Graphe pondéré

Un graphe $G = (S, A)$ est dit *pondéré* s'il existe une application P dans $\mathbb{R}$ qui à chaque arc a possible, associe un nombre réel : $P : A \rightarrow \mathbb{R}$. Bien que dans le cadre applicatif il s'agit plus généralement de nombres réels strictement positifs ($P : A \rightarrow \mathbb{R}_+^*$). Le poids de l'arête a est défini comme tel : $P(a)$. Le graphe pondéré est alors un triplet (S, A, P). Un exemple de graphe orienté et pondéré est illustré dans la Figure I.15.d).

Dans un graphe orienté et pondéré, différents concepts sont associés aux chemins qui le composent. Premièrement, soit c un chemin de G tel que $c = (s_1, s_2, ..., s_k)$, le poids $P(c)$ du chemin c est défini comme la somme du poids $P(a)$ de chaque arête associée (Équation I.3). Deuxièmement, on définit aussi le chemin *le plus court* entre deux sommets comme le chemin de poids minimal parmi tous ceux existants.

$$P(c) = P(a_1) + P(a_2) + ... + P(a_k) = P(s_1, s_2) + P(s_2, s_3) + ... + P(s_{k-1}, s_k) \qquad \text{(I.3)}$$

I.5.2 Modélisation sous forme de graphe

Comme nous l'avons défini précédemment, la modélisation sous forme de graphe offre une abstraction et une formalisation mathématique utile à diverses problématiques dans des domaines d'application divers et variés. Les graphes sont des outils extrêmement polyvalents pour modéliser des problèmes du « monde réel » en problèmes mathématiques. Néanmoins cette modélisation n'est pas toujours évidente. Elle nécessite un processus de formulation du problème concerné à partir de la théorie des graphes. Le graphe généré est alors défini par différentes caractéristiques qui facilitent plus ou moins l'étude de ce même problème. Parmi celles-ci, on dénote les caractéristiques **inhérentes** à la modélisation sous forme de graphe, tel que les sommets et les arêtes qui le composent, mais aussi des caractéristiques **complémentaires**, telles que l'orientation des arêtes ou leur pondération.

Afin de modéliser un graphe adapté pour répondre à la problématique de l'étude concernée, il est nécessaire de définir ses caractéristiques en amont de sa génération. La difficulté dans cet exercice est de définir des caractéristiques suffisamment génériques pour englober les besoins de modélisation de l'étude, sans pour autant l'être de trop, pour ne pas impacter la formalisation mathématique et l'analyse que l'on souhaite en extraire.

Concernant les caractéristiques inhérentes du graphe à générer, il est nécessaire de définir ce que l'on souhaite représenter au travers des différents **sommets** qui le composent. Différents types de sommets peuvent être définis au sein d'un même graphe selon les besoins de l'étude. Néanmoins, il est toujours nécessaire de garder un certain niveau de cohérence vis-à-vis de l'analyse mathématique qui en résulte, comme avec les potentiels chemins du graphe. De même, les **arêtes** qui unissent les sommets entre eux ont un rôle tout aussi prépondérant. Il est alors primordial de définir ce que ce lien représente dans le graphe généré. Tout comme les sommets, plusieurs types d'arêtes peuvent être définis au sein d'un même graphe. Là aussi, un certain niveau de cohérence est de mise quant aux potentiels résultats mathématiques qui en résultent. De nombreuses études, caractérisées par divers domaines d'application, ont proposé différentes représentations des sommets et des arêtes d'un graphe selon les besoins associés. Par exemple, un modèle de graphe a été proposé pour faciliter la représentation et l'analyse des unités stratigraphiques [51] dans un site de fouille archéologique [GMV+12]. Le graphe généré est composé de sommets représentant les différentes unités stratigraphiques, et d'arêtes associées aux relations entre ces mêmes unités stratigraphiques (couvre, remplit, s'appuie, coupe, lie, etc.).

51. Découpage pour définir des séquences de dépôt

Les potentielles caractéristiques complémentaires du graphe sont tout aussi importantes que celles inhérentes à ce type de modélisation. Bien qu'elles ne soient pas obligatoires, elles apportent des éléments de réponses pour la formulation de certains problèmes dans la théorie des graphes. Parmi ces caractéristiques complémentaires, on distingue notamment l'**orientation** des arêtes. Cette orientation est différemment mise à profit selon le domaine d'application de l'étude. Elle peut à la fois caractériser un lien physique, une connexion, une relation, une influence, ou bien-sûr une **dépendance**, d'un sommet du graphe par rapport à un autre. L'orientation des arêtes est primordiale dans l'analyse du graphe généré puisqu'elle impacte directement ses chemins. La **pondération** des arêtes est une autre caractéristique majeure possédant une forte influence sur l'analyse résultante du graphe concerné. Elle permet de définir une **magnitude** pour chaque arête (généralement orientée) qui témoigne de sa criticité, d'une distance, ou encore de la valeur d'une caractéristique commune entre les sommets associés. Cette pondération est définie selon le contexte d'application du graphe, mais aussi selon les analyses que l'on souhaite en faire. En biologie cellulaire, Behnam Neyshabur *et al.* ont par exemple utilisé la théorie des graphes pour analyser les réseaux d'interaction entre protéines [NKHA13]. Les protéines sont alors représentées sous forme de sommet, et les interactions entre elles sous forme d'arc. Dans un autre domaine de recherche, Zafar Saeed *et al.* ont utilisé un modèle de graphe pour la détection d'évènements à partir de l'analyse de contenu de *tweets* [SARX19]. Le graphe pondéré proposé modélise un agrégat d'un certain nombre de tweets où chaque sommet représente un mot, et chaque arête une cooccurrence entre deux mots. La pondération des arêtes est alors définie à partir du nombre de cooccurrences dans l'ensemble des tweets considérés pour la génération du graphe.

La formulation d'un problème réel à partir de la théorie de graphes nécessite donc de définir un certain nombre de caractéristiques du graphe à générer. La définition de ces caractéristiques peut être résumée à partir d'un processus composé de différentes étapes :

1. **Quels éléments du problème devraient être représentés par des sommets ?**
2. **Quels liens entre ces éléments devraient être représentés sous forme d'arêtes ?**
3. **Le problème étudié nécessite-t-il de définir un paramètre d'orientation des arêtes ? Si cela est le cas, pourquoi et comment ?**
4. **Le problème étudié nécessite-t-il de définir un paramètre de pondération des arêtes en complément de leur orientation ? Si cela est le cas, pourquoi et comment ?**
5. **En complément des paramètres déjà définis, le problème étudié nécessite-**

t-il de définir des paramètres supplémentaires aux sommets ou aux arêtes du graphe concerné ? Si cela est le cas, lesquels ?

L'ensemble de ce processus itératif est illustré dans la Figure I.16. Il permet de définir un graphe adapté à la représentation, l'analyse et la résolution du problème concerné. Une fois les caractéristiques du graphe définies, celui-ci peut être généré et traité à partir de différents outils. Nous présenterons dans une section suivante un bref état de l'art des outils existants, adaptés à notre problématique d'étude.

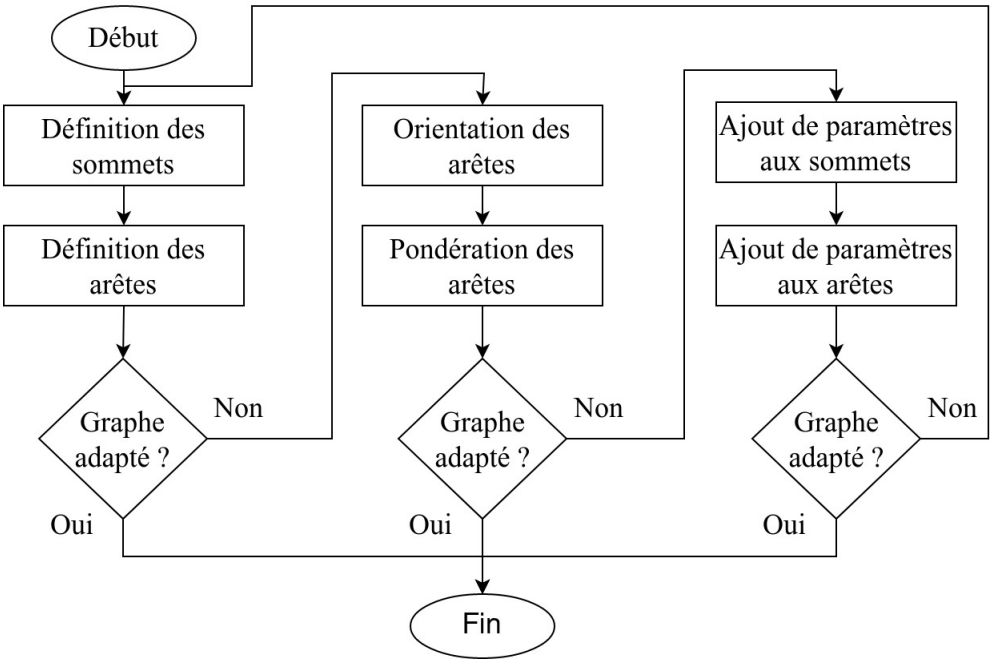


FIGURE I.16: Processus de modélisation sous forme de graphe

I.5.3 Algorithmes de graphe

Les algorithmes de graphe représentent un sous-ensemble des outils d'analyse de graphes, qui caractérisent les approches basées sur la théorie des graphes pour analyser des données connectées. L'objectif de ces outils est d'identifier de façon algorithmique des sous-structures, ou des propriétés, du graphe étudié [vL90]. Ainsi, ces algorithmes permettent de répondre à des questions telles que « Le graphe G possède-t-il la propriété P ? » en fournissant les solutions mathématiques adaptées. Divers types d'application sont associés à ce concept d'algorithmes de graphe, on dénote principalement la consultation de données du graphe, l'utilisation de statistiques de base, l'exploration visuelle du graphe, ou encore l'incorporation de données issues du graphe dans des processus d'analyse externes [HN19]. Ces

algorithmes constituent l'une des approches les plus performantes pour analyser des données connectées, car les calculs mathématiques qui en résultent sont spécifiquement conçus pour être réalisés sur des relations entre diverses entités.

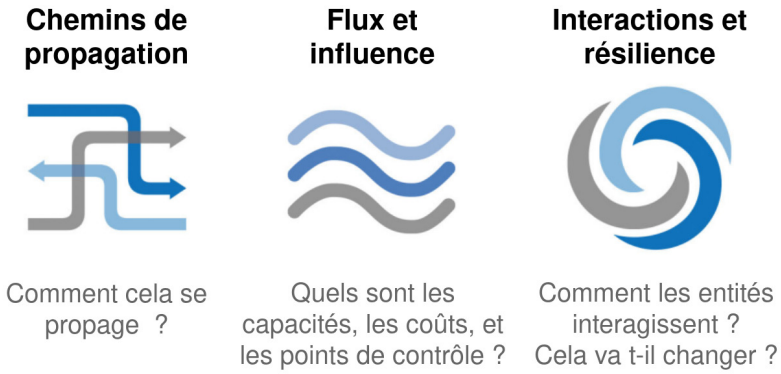


FIGURE I.17: Types de question auxquelles l'analyse des graphes répond [HN19] (adapté)

L'analyse des graphes, au travers d'algorithmes, permet de répondre à un certain nombre de problématiques issues de cas d'application divers et variés (Figure I.17). Dans le cadre de ces travaux de thèse, nous nous intéressons plus particulièrement à l'étude de la propagation à partir de différents **chemins de propagation**. De ce fait nous nous sommes plus particulièrement focalisés sur les algorithmes de parcours de graphe, et plus particulièrement aux algorithmes de *Breadth First Search (BFS)*[52] [Lee61] et de DFS[53][Koz92]. La principale différence entre ces deux algorithmes réside dans la façon de parcourir le graphe. Le BFS utilise une structure de données sous forme de file (« premier arrivé, premier sorti ») , tandis que le DFS se base sur une pile (« dernier arrivé, premier sorti »). En résumé, le BFS est utile pour trouver le chemin le plus court d'une source vers une destination unique, tandis que le DFS est davantage performant pour traverser le plus d'arêtes possible pour atteindre le sommet de destination[54].

L'objectif de ces travaux étant d'obtenir, et d'évaluer l'ensemble des chemins potentiels de propagation d'anomalies, nous nous intéresserons exclusivement à l'algorithme de DFS dans la suite de ce manuscrit. Le DFS est reconnu comme une technique extrêmement efficace pour résoudre divers problèmes liés aux graphes [Eve11]. Son principe est relativement simple, la recherche de chemin est initiée depuis un sommet donné puis ses voisins sont parcourus un à un pour obtenir le plus long chemin possible avant de revenir au sommet précédent. Ce

52. Parcours en largeur.
53. Parcours en profondeur
54. *Difference between BFS and DFS*. GeeksforGeeks. Consulté le 26 octobre 2021. `https://www.geeksforgeeks.org/difference-between-bfs-and-dfs/`

type d'algorithme a initialement été formulé dès le XIX^{e} siècle comme stratégie de solution de labyrinthe. Un exemple d'application de cet algorithme est présenté dans la Figure I.18. Dans cet exemple un seul chemin est parcouru, le score associé à celui-ci est calculé à partir de la somme des pondérations de chaque arête traversée.

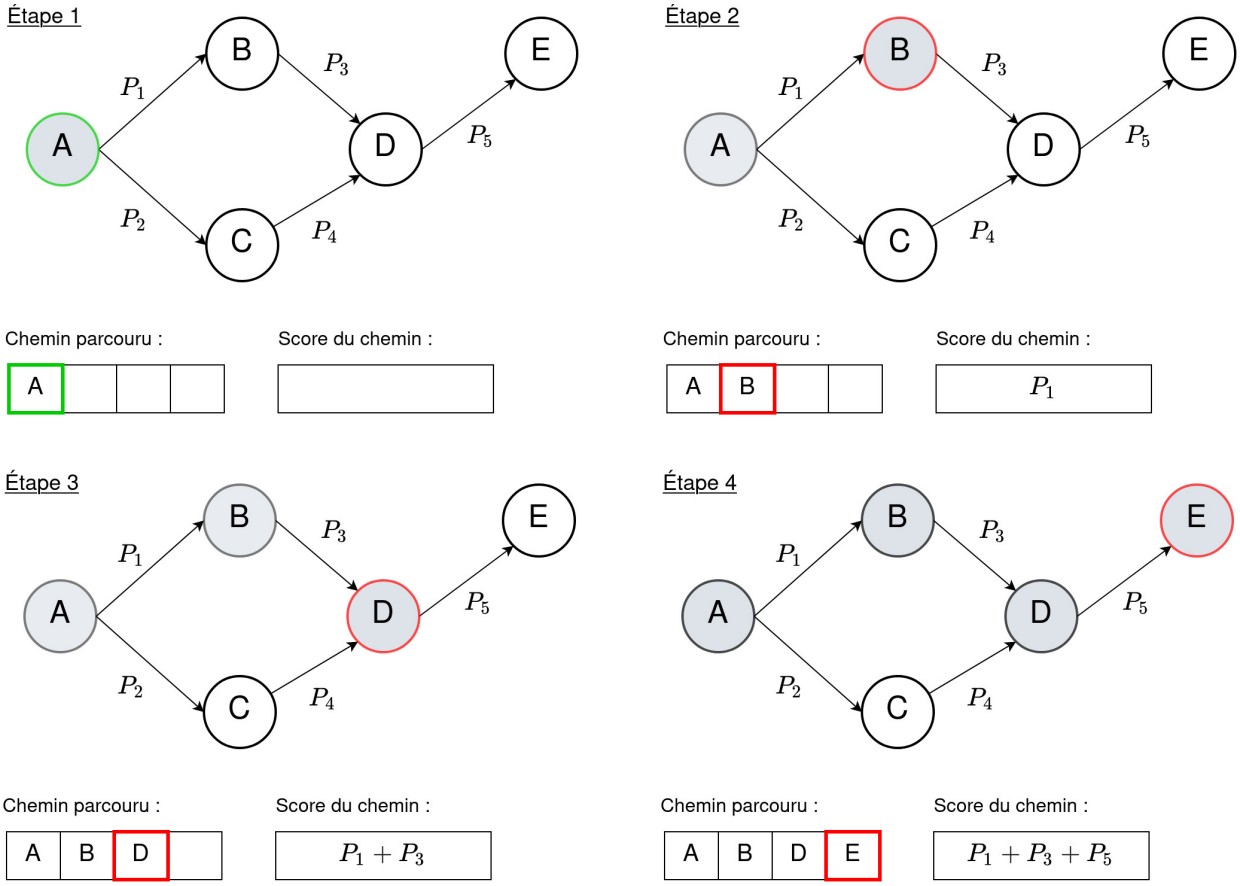


FIGURE I.18: Exemple d'application de l'algorithme de DFS

I.6 Conclusion

Comme nous l'avons vu dans ce chapitre, l'importance du secteur maritime est immense. Cette tendance ne semble pas s'inverser, et ce malgré la crise sanitaire. En accord avec la diversité de ce secteur d'activité, les navires employés se distinguent par des caractéristiques et propriétés spécifiques, adaptées aux missions qui leur sont attribuées. On distingue principalement parmi celles-ci une forte hétérogénéité des systèmes maritimes embarqués, associée à un haut de niveau de dépendance. Comme cela a été exposé, les contraintes inhérentes au domaine d'application maritime ne font qu'exacerber la criticité de la cybersécurité de

ces systèmes. Les problématiques résultantes sont considérées au niveau du cadre législatif international, et d'autant plus au niveau national. Depuis plusieurs années, la France a pleinement pris conscience de l'importance stratégique de la cybersécurité maritime et insuffle dans ce sens différentes solutions adaptées aux besoins sectoriels. Nous avons présenté ensuite plusieurs modèles et méthodes d'évaluation du cyber-risques maritimes, comme un élément majeur de la gestion globale du risque.

Les CPS ont été présentés comme un cas particulier de système d'information maritime assurant des fonctions vitales pour les navires. Leurs principales caractéristiques et propriétés ont été examinées pour comprendre l'importance de leur étude, notamment en matière de cybersécurité. Cet enjeu majeur est intimement lié aux différentes vulnérabilités de ces systèmes, exploitables par diverses cyberattaques. Les principales méthodes de détection d'anomalies dans ces systèmes ont également été détaillées à partir de leurs apports et limitations. Nous avons alors plus particulièrement justifié le choix d'utilisation dans la suite de ces travaux de la méthode de détection par évaluation de la qualité.

Nous avons par la suite davantage détaillé la littérature relative à l'analyse de la propagation d'anomalies dans les systèmes. Il était alors primordial de définir dans un premier temps la notion de « dépendance » associée cette problématique, car sa définition dans la littérature semble parfois floue. Nous avons par la suite détaillé les solutions majeures pour répondre à la problématique d'analyse de la propagation d'anomalies, qui sont précisément : l'analyse structurelle, la modélisation mathématique, et les graphes d'attaques. Les apports et les limitations de chacune de ces solutions ont été explicitement présentés. Enfin nous avons présenté le concept de « défaillances en cascade », un problème relatif à la propagation globale d'anomalies dans un système concerné. L'analyse résultante nous a permis de souligner l'apport de l'analyse structurelle, et des graphes d'attaques, pour répondre à la problématique d'évaluation de la propagation d'anomalies dans un système donné.

Ainsi, la discipline de la théorie des graphes a été détaillée. Comme nous avons pu le caractériser, la structure des graphes est un apport majeur pour l'analyse de la propagation d'anomalies. Les propriétés d'abstraction et de formalisation mathématiques de ce type de modélisation sont des atouts indéniables pour l'étude de cette problématique. La mise en œuvre d'un graphe nécessite cependant la prise en compte de différentes caractéristiques que nous avons précisées.

La considération de la problématique d'évaluation de la propagation d'anomalies dans les CPS maritimes n'est pas suffisamment traitée par la communauté scientifique au vu

des conséquences potentielles qui peut en résulter. Nous avons détaillé dans ce chapitre les différentes solutions existantes pour répondre à cette problématique. Celles-ci présentent un certain nombre de limitations telles que l'absence de représentation visuelle du système, ou encore une évaluation exclusivement basée sur des métriques statiques ou topologiques. La limitation principale de ces méthodes réside néanmoins dans la déconsidération de la détection des anomalies. En adéquation avec ces limitations, nous proposons dans le chapitre suivant une méthode innovante d'évaluation de la propagation d'anomalies dans les CPS maritimes qui s'appuie sur un nouveau modèle de graphe multicouche.

Chapitre II

Méthodologie pour l'évaluation de la propagation d'anomalie dans un CPS maritime

Sommaire

Ce chapitre introduit une nouvelle méthodologie pour évaluer la propagation d'anomalies dans un CPS maritime à partir d'un modèle de graphe adapté. Tous les éléments qui ont mené à cette méthodologie sont présentés afin de comprendre la problématique traitée et la structure du modèle résultant.

II.1 Principes de base

Nos travaux de recherches présentés dans ce chapitre ont l'objectif de proposer des solutions pour répondre à la problématique suivante : **comment évaluer la propagation d'anomalies dans un système cyber-physique maritime ?**

Pour répondre à cette problématique, nous avons identifié trois points de recherche majeurs à traiter :

1. La modélisation structurelle du CPS pour fournir une représentation mathématique, mais aussi visuelle, adaptée à notre problématique. Cette modélisation doit comprendre les sous-systèmes qui composent le CPS, ainsi que les nombreuses dépendances qui le définissent.
2. Une méthode d'évaluation du niveau de menace associé aux dépendances dans le CPS. Cette méthode devra faire partie prenante de la modélisation proposée pour les CPS.
3. Une méthode d'évaluation de la propagation d'anomalies basée sur les deux premiers points.

Comme présenté dans le chapitre I, plusieurs travaux de la littérature scientifique du domaine amènent des éléments de réponses à notre problématique. L'évaluation de la pro-

pagation d'anomalies dans les CPS a déjà été traitée à partir d'analyses structurelles, de modélisation mathématique, ou encore grâce à des graphes d'attaques.

À partir de ces travaux existants, nous pouvons construire une liste de limitations qui nous permettra de comparer les solutions proposées par nos travaux. Cette liste est présentée ci-dessous :

1. Modélisation structurelle du CPS :
   (a) Modèle spécifique à un domaine d'application.
   (b) N'intègre pas les variables du système.
   (c) Modèle non générique.
2. Méthode d'évaluation de la propagation :
   (a) Ne fournit pas de représentation visuelle du système considéré.
   (b) Approche basée sur des métriques d'évaluation statiques.
   (c) Ne considère pas de méthode de détection d'anomalies.

Pour traiter ces objectifs et limitations, un nouveau modèle de représentation de CPS a été proposé. Dans ce modèle le CPS est représenté sous forme d'un graphe 3-couches, adapté à ses caractéristiques. Le graphe généré permet à la fois la modélisation des sous-systèmes du CPS, ses variables, ainsi que les différentes dépendances entre ceux-ci. Au-delà du modèle mathématique proposé, cette représentation est aussi adaptée pour fournir une visualisation cohérente du système.

En complément, une méthode innovante de pondération des dépendances dans un CPS a été développée. Celle-ci propose d'évaluer le niveau de menace associé à chaque sous-système du CPS étudié au travers d'un certain nombre de métriques objectives basé sur les caractéristiques, les contraintes et les risques associés à ce type de système. Pour chaque sous-système, le poids obtenu est reporté sur l'ensemble des dépendances qui en émergent. L'évaluation de la propagation d'anomalies est ensuite calculée à partir d'un algorithme de parcours de chemin. Le résultat obtenu comprend alors une liste des chemins de propagations potentiels, ainsi qu'un score associé à chaque chemin traduisant quantitativement le niveau d'impact de celui-ci sur l'ensemble du système.

Les propositions introduites avec cette méthodologie sont résumées dans la liste ci dessous. Cette liste cherche à répondre aux limitations identifiées dans les études de l'état de l'art.

1. Identification des dépendances dans les systèmes maritimes :
   (a) Représentation générique des dépendances principales.
   (b) Caractérisation des dépendances induites par les CPS maritimes.
2. Modélisation structurelle du CPS :
   (a) Représentation des différents sous-systèmes, des variables, et les dépendances entre ceux-ci.
   (b) Représentation mathématique et visuelle du CPS.
   (c) Modèle générique pour tout type de domaine d'application.
3. Évaluation de la propagation d'anomalies :
   (a) Initiée par la détection d'une anomalie.
   (b) Basée sur un algorithme de parcours de graphe.
   (c) Développement d'une méthodologie de pondération des arêtes.
   (d) Calcul d'un score d'impact des chemins de propagation générique.

Afin d'appliquer le modèle ainsi présenté, un certain nombre d'hypothèses doivent être prises en compte :

1. Nous supposons que le lien entre les éléments du CPS, représenté par une dépendance, entraîne une propagation de l'anomalie.
2. La propagation de l'anomalie est impactée par l'élément traversé. Elle peut ainsi être plus ou moins accentuée selon les caractéristiques de l'élément, son rôle opérationnel, et les moyens déjà employés pour limiter le risque de propagation.
3. Il est supposé que l'utilisateur implémentant la méthodologie proposée possède une connaissance poussée du CPS concerné. Cette connaissance comprend l'ensemble de l'architecture du système au travers des divers éléments interconnectés qui le composent.

Dans les sections et sous-sections suivantes, nous présentons plus en détail les éléments de réponse associés à la problématique de l'évaluation de la propagation d'anomalies dans un CPS maritime.

II.2 Définitions contextuelles

Le travail proposé aborde la problématique de l'évaluation de la propagation d'anomalies dans les CPS. Ainsi la compréhension de cette thèse nécessite la définition d'un ensemble de termes associés à la notion de *système*.

Plusieurs approches ont été proposées dans la littérature pour définir la notion de système. La définition la plus courante du mot système revient à *Jacques Lesourne* qui le définit comme « *un ensemble d'éléments en interaction dynamique* » [Les76]. Une seconde définition tout aussi répandue est proposée par Joël de Rosnay qui caractérise cette notion comme « *un ensemble d'éléments en interaction dynamique, organisé en fonction d'un but* » [DR14]. Dans le cadre de ces travaux, nous nous sommes essentiellement basés sur la définition proposée par l'INCOSE (Définition I.7) présentée dans la section I.4.1.

Apparaît alors une notion supplémentaire à définir : la notion d'**élément** composant le système. L'organisation internationale de normalisation [1] a proposé dans la norme ISO/IEC 15288 [fS15], une norme technique d'ingénierie des systèmes qui couvre les processus et les étapes du cycle de vie, la définition suivante pour la notion d'élément du système :

Definition II.1. *Un **élément du système** est un membre d'un ensemble d'éléments qui constitue un système. Un élément de système est une partie discrète d'un système qui peut être mise en œuvre pour répondre à des exigences spécifiques. Un élément de système peut être un matériel, un logiciel, des données, des êtres humains, des processus, des procédures, des installations, des matériaux et des entités naturels, ou toute combinaison.*

De plus cette norme apporte une précision supplémentaire quant à l'emploi de ce terme pour un système de taille ou de complexité plus importante : « *Pour un système important ou complexe, un **élément de système** peut être considéré comme un système et sera lui-même composé d'éléments de système. Cette nature hiérarchique et contextuelle des termes système et élément de système permet d'utiliser le terme système pour désigner un composant discret ou un système complexe de systèmes géographiquement distribués* ».

Nous ajoutons à la Définition II.1 qu'un élément du système peut être caractérisé par une ou plusieurs variables mesurables. Nous définissons alors l'ensemble des variables associées aux éléments du système à partir des éléments de réponses introduits par Y. Wang *et al.* [WXZ+14] :

Definition II.2. *Une **variable système** est une variable associée à un ou plusieurs éléments du système. L'ensemble de ces variables caractérise l'état du système concerné à tout instant t.*

Dans le cadre des travaux présentés, il est essentiel de représenter les différents liens existants entre les variables système. Ces relations sont alors caractérisées à partir du concept

1. *International Organization for Standardization (ISO)*

de *corrélation*. Notre étude intégrera ce concept tel qu'il est défini dans domaine de la statistique :

Definition II.3. *La **corrélation** entre plusieurs variables est une notion de liaison qui contredit leur indépendance.*

Dans la suite de nos travaux de thèse présentés dans les sections suivantes, nous proposons une modélisation innovante de CPS. En accord avec l'objectif associé, seul un ensemble des propriétés d'un CPS est représenté au travers de la modélisation formulée. Cet aspect de la modélisation introduit la notion *d'abstraction* que nous utilisons à partir de la définition suivante [VPQVS16] :

Definition II.4. *Une **abstraction** d'un objet ne reflète que les aspects (ou propriétés) de cet objet considérés comme essentiels pour certains objectifs, tout en ignorant, ou en rejetant, les aspects considérés comme non pertinents pour ces mêmes objectifs.*

II.3 Approche générale

Afin de répondre à la problématique identifiée, et aux différentes questions de recherche qui en découlent, nous allons dans un premier temps définir le cadre de l'étude et présenter l'approche générale qui en résulte.

II.3.1 Problématique générale

L'augmentation de la taille et de la complexité des navires modernes entraînent une recrudescence de l'utilisation de différents systèmes IT et OT (section I.2). Pour garantir le succès de la mission qui lui est attribuée, le statut opérationnel d'un navire doit être assuré en temps réel au travers du contrôle et de la surveillance d'une multitude de **systèmes interdépendants**. Structurés en plusieurs boucles fonctionnelles, ces systèmes permettent d'assurer toutes les fonctions associées au navire telles que la navigation, la propulsion, la communication, et toutes les autres fonctions nécessaires à la vie à bord. En raison d'un manque de considération de leur sécurité dès leur conception, et à cause l'utilisation de technologies propriétaires, les systèmes maritimes sont vulnérables pendant tout le cycle de vie du navire (section I.1.3). A cela s'ajoute le fait que les processus de correctifs et de mise

à jour sont extrêmement complexes à mettre en œuvre pour atténuer le risque associé à ces vulnérabilités [SDF18].

De par l'interdépendance croissante entre les systèmes embarqués à bord, une attaque visant un système quelconque pourrait aisément se propager et impacter de nombreux autres systèmes. L'ensemble du navire pourrait même être impacté et ainsi compromettre la mission qui lui attribuée, ou pire, mettre en danger l'équipage et les passagers à bord. En outre, de multiples menaces physiques et cyber, favorisées par des vulnérabilités inhérentes aux systèmes maritimes, pourraient entraîner la propagation d'anomalies et générer des conséquences critiques pour le navire [JTP16]. L'identification et l'évaluation de la propagation d'anomalies dans les systèmes maritimes apparaissent donc comme une problématique majeure pour garantir la sécurité des navires.

II.3.2 Des systèmes maritimes interdépendants

De par ces caractéristiques de composition d'une multitude d'éléments qui interagissent entre eux, et d'après la définition proposée par James Ladyman *et al.* [LLW12], un navire moderne est définissable comme un système complexe. La plupart des systèmes complexes comprennent de multiples sous-systèmes et couches de connectivité. Ces systèmes sont généralement regroupés en différents réseaux à partir de multiples interactions entre eux. Un navire est ainsi défini par différents réseaux interconnectés, composés d'une multitude de systèmes interdépendants structurés en boucle fonctionnelle. Un navire est alors définissable à partir du concept de réseaux multicouches [BBC+14]. Les réseaux multicouches permettent de définir explicitement les diverses interactions qui définissent un système interconnecté. Chaque couche représentant un réseau particulier, constitué de différents éléments (systèmes, sous-systèmes, équipements, ou composants) qui interagissent entre eux. Ces différents réseaux interagissent eux aussi par le biais d'interaction entre éléments de différentes couches (Figure II.1). Chaque élément d'un réseau multicouche peut être associés à différents types d'interactions, définies selon le domaine d'application.

En raison des nombreux systèmes interdépendants qui le composent, un navire est aussi définissable à partir de la notion de **système de systèmes**. MITRE, une organisation à but non lucratif américaine, définit cette notion comme : *un ensemble de systèmes interdépendants, intégrés au sein d'un système plus important pour offrir des capacités*

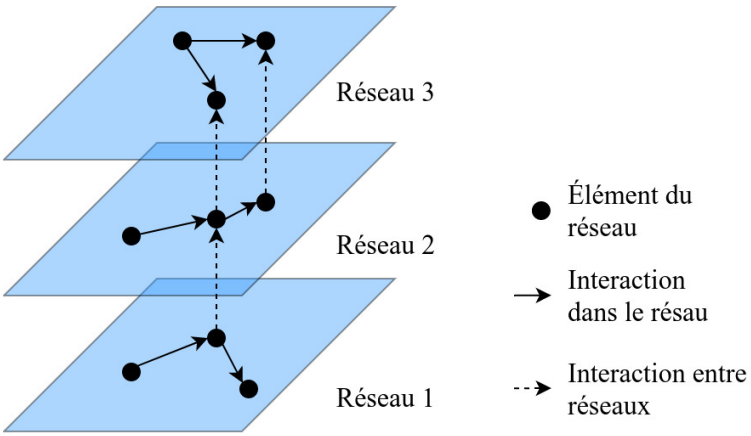


FIGURE II.1: Illustration de réseaux multicouches

uniques.[2] [Reb14]. Ces systèmes interagissent les uns avec les autres par le biais de multiples dépendances et interdépendances (Définition I.8), afin de garantir le bon fonctionnement du navire et la réussite de la mission. Conformément à la notion de système précédemment définie dans la section I.4.1, un navire est composé par deux types principaux de dépendances à différents niveaux d'abstraction et de perspective. Premièrement, depuis une perspective interne, il existe différentes dépendances entre les composants d'un même système (Figure I.8 (a)). Deuxièmement, à partir d'une perspective externe où un système est considéré comme un ensemble unifié (Figure I.8 (b)), un navire est défini comme un *SoS* composé de systèmes dépendants et interdépendants. L'ensemble de ces systèmes et sous-systèmes, ainsi que leurs dépendances, sont associés à différentes couches de réseau qui composent le navire.

Comme indiqué précédemment ces dépendances sont particulièrement critiques, elles peuvent produire des défaillances en cascade et potentiellement impacter l'ensemble du navire [ZJJZ13]. Il apparaît alors évident que la caractérisation et l'analyse de ces dépendances sont un besoin majeur, non seulement pour les navires, mais aussi pour l'ensemble du domaine maritime. Pour cela nous avons identifié trois principaux défis :

- **Chaque couche de dépendances doit être modélisée depuis une perspective interne et externe.**
- **Plusieurs modèles doivent être employés pour couvrir l'hétérogénéité des systèmes et sous-systèmes, ainsi que leurs dépendances, en matière de caractéristiques, de fonctions et de criticité.**
- **La caractérisation et l'analyse des dépendances entre les systèmes maritimes doivent être considérées durant l'ensemble du cycle de vie du**

2. A set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities.

navire. De la conception, à la phase opérationnelle, en passant par le développement, les dépendances doivent être prises en compte à partir de différents modèles adaptés.

Tous ces aspects devraient être réunis dans une solution unifiée, suffisamment générique pour couvrir l'ensemble des besoins associés aux disparités de caractéristiques inhérentes aux différents types et classes de navires.

II.3.3 Identification des dépendances génériques entre les systèmes maritimes

Nous proposons ici une première analyse concernant la problématique des dépendances entre les systèmes maritimes qui composent un navire. Cette première analyse est ainsi constituée d'une définition et représentation des principales dépendances, en respectant la perspective interne et externe des systèmes [PMLJP21]. Au travers de cette représentation générique, nous définissons une ligne directrice pour initier d'autres représentations et évaluations des dépendances à des niveaux d'abstraction plus ou moins élevés.

Les systèmes maritimes [BIM20], constituant un navire, sont regroupés en plusieurs boucles fonctionnelles et associés à des dépendances et interdépendances à plusieurs niveaux d'abstraction. Deux types de dépendances sont ainsi définis : entre des systèmes d'un bloc fonctionnel donné et entre des systèmes de blocs fonctionnels différents. Cinq groupes fonctionnels critiques ont été identifiés (Figure II.2) :

Les systèmes de plateforme (1.1-1.6) assurent différentes fonctions vitales du navire au travers de nombreuses dépendances internes et externes. Ils sont composés de nombreux **sous-systèmes** qui interagissent perpétuellement entre eux à partir de plusieurs types de dépendances associées à tout ICS : des commandes de contrôle d'un automate vers un actionneur, des mesures de capteur vers un automate, ou encore des échanges d'informations entre deux automates, etc. À titre d'exemple nous fournissons une illustration de ces dépendances à partir d'un système de plateforme générique (**1.2**). Ils sont aussi associés à différentes dépendances externes majeures entre eux, qui permettent leurs bons fonctionnements (ex : le système de production d'électricité aliment en énergie les autres systèmes de plateforme).

Les systèmes de passerelle (2) sont reliés à plusieurs autres blocs fonctionnels complémentaires du navire, et ce, à partir de diverses dépendances qui sont autant de source de risque. Par exemple, les composants qui constituent la *surface situation awareness* re-

cueillent des informations, au travers de dépendances, depuis **les systèmes de communication (5)** tels que l'AIS, le GNSS, le radar, etc., et les affichent sur un ECDIS. Une autre dépendance clé est représentée par les **systèmes de passerelle intégrés(2.2)** (*Integrated Bridge Systems (IBS)*) qui combinent le contrôle et la surveillance des systèmes de navigation avec celles des **systèmes de plateforme (1)**.

Différents **systèmes IT** sont utilisés à bord pour fournir une connexion à distance à d'autres systèmes embarqués. En résultent de nombreuses dépendances hautement vulnérables. Les **systèmes de communication (5)** fournissent Internet, à partir d'une connexion satellitaire ou d'un réseau cellulaire (3G, 4G, 5G) en navigation côtière, aux **systèmes de divertissement (3.1)** utilisés par l'équipage et les passagers. Aussi, des **applications bureautiques (3.2)** installées sur des systèmes tiers permettent la surveillance à distance, la collecte des données, ainsi que la maintenance, des **systèmes de plateforme (1) et de passerelle (2)**.

Enfin, différents **systèmes IT et OT spécifiques** sont utilisés selon la mission attribuée au navire. Comme nous l'avons vu dans la section I.2.1, cela concerne les navires civils comme militaires. Parmi l'ensemble de ces systèmes, on notera par exemple les systèmes utilisés pour la gestion de la cargaison des cargos, ou les systèmes d'armes des navires militaires. De multiples dépendances résultent entre ces systèmes spécifiques et les autres **blocs fonctionnels du navire**.

De par leur caractéristique de contrôle d'opérations physiques à partir de commandes numériques, une majeure partie des systèmes OT d'un navire moderne peut être définie comme des CPS. En raison de leur criticité, dans la suite de ces travaux nous traiterons de la problématique de dépendance associée aux CPS maritimes, et plus particulièrement de l'évaluation de la propagation d'anomalies.

II.3.4 Formalisation mathématique de la problématique

Dans l'objectif de fournir une formalisation et une représentation mathématique adéquates à la problématique de cette thèse, nous initions nos travaux de recherche à partir du postulat suivant : un CPS est composé d'un ensemble de sous-systèmes dépendants ou interdépendants (Définition I.6) auxquels sont associées un certain nombre de variables. À partir des propriétés des graphes précédemment définies dans la section I.5.2, nous pouvons affirmer que ce type de modélisation est particulièrement appropriée à notre problématique.

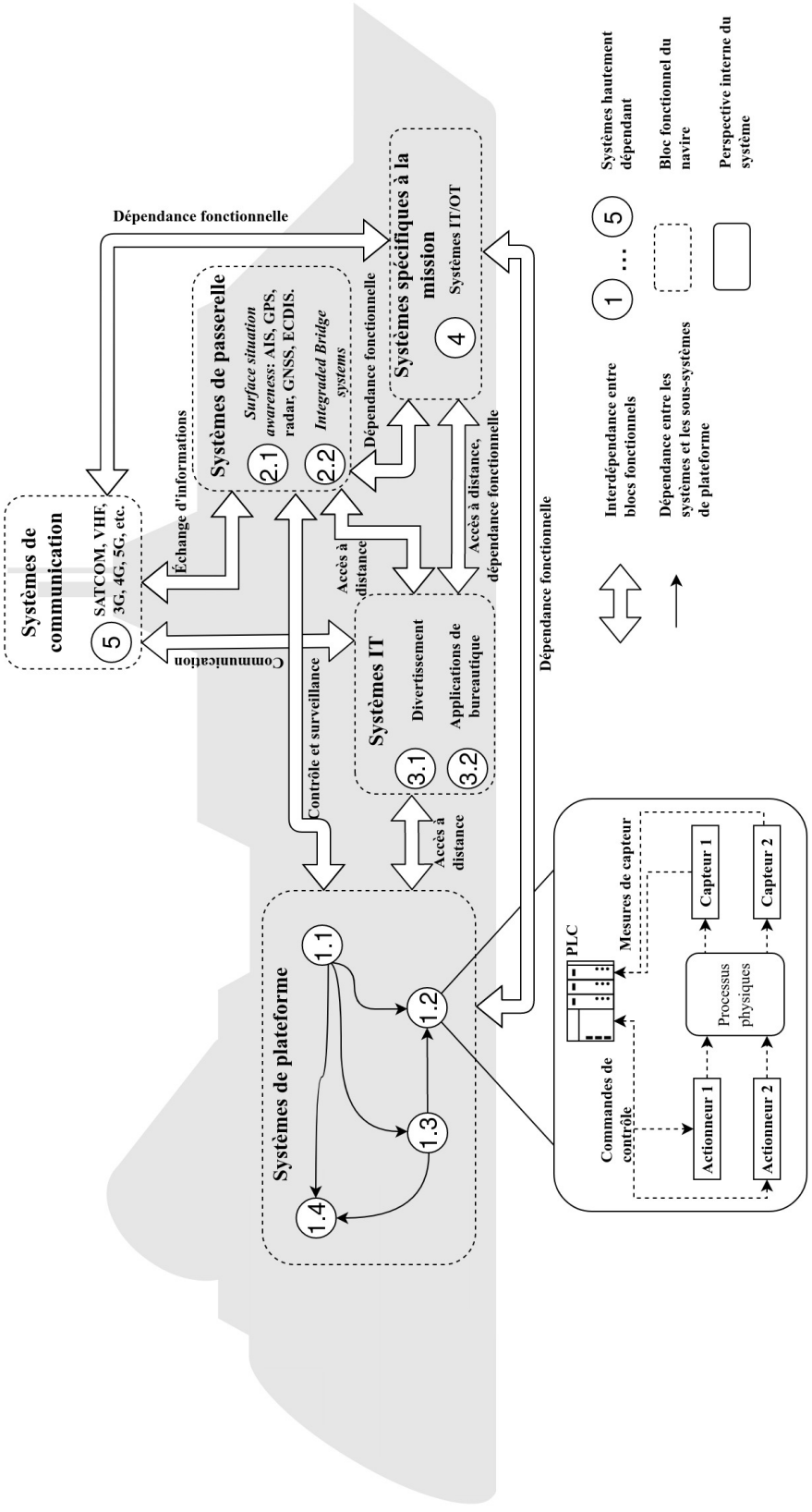


FIGURE II.2: Dépendances majeures entre les systèmes maritimes

Pour définir un modèle de graphe adapté, nous avons utilisé le processus présenté dans cette même section. Ainsi, nous avons implémenté ce processus pour définir les caractéristiques principales du modèle de graphe souhaité :

1. **Quels éléments du problème devraient être représentés par des sommets ?**
   Au vu de la problématique et de la définition d'un CPS, il apparaît évident de représenter les sous-systèmes du CPS à partir des sommets du graphe. Néanmoins, les variables associées au CPS sont tout aussi importantes. Il est donc nécessaire de les modéliser elles aussi sous forme de sommet.
2. **Quels liens entre ces éléments devraient être représentés sous forme d'arêtes ?**
   Au vu des réponses apportées à la question précédente, les arêtes du graphe doivent être utilisées pour schématiser les dépendances entre les sous-systèmes du CPS. En représentant les variables sous forme de sommet, il est aussi nécessaire de définir un type d'arête spécifique aux liens entre celles-ci.
3. **Le problème étudié nécessite-t-il de définir une orientation des arêtes ? Si cela est le cas, pourquoi et comment ?**
   D'après la définition de la notion de « dépendance» (Définition I.8), celle-ci se caractérise par un lien unidirectionnel d'un élément vers un autre. En accord avec cette définition, il est nécessaire de définir une orientation aux arêtes entre les sommets des sous-systèmes. Par souci de cohérence, l'ensemble des arêtes du graphe doivent être orientées. Elles seront donc considérées comme des arcs.
4. **Le problème étudié nécessite-t-il de définir un paramètre de pondération des arêtes en complément de leur orientation ? Si cela est le cas, pourquoi et comment ?**
   Afin de fournir une analyse représentative et quantitative de la propagation d'anomalie, il est pertinent de définir une magnitude à chaque dépendance entre les sous-systèmes. Pour cela, une méthode de pondération doit être définie en accord avec les spécificités du domaine d'application. Cela concerne exclusivement les arcs entre les sommets de sous-systèmes du CPS.
5. **En complément des paramètres déjà définis, le problème étudié nécessite-t-il de définir des paramètres supplémentaires aux sommets ou aux arêtes du graphe concerné ? Si cela est le cas, lesquels ?**
   Différents types de sommets et d'arêtes sont nécessaires dans le graphe envisagé. Il est donc primordial de définir un certain nombre de paramètres aux sommets et arcs du graphe considéré.

Comme nous l'avons détaillé précédemment dans la section II.3.2, la notion de réseaux multicouches est particulièrement adaptée aux navires modernes composés de réseaux dépendants et interdépendants. De même, comme il a été détaillé dans la section I.4.2, la représentation de la problématique des dépendances dans les CPS sous forme de graphe multicouche est une solution particulièrement viable. De ce fait, il est pertinent de définir un certain nombre de couches dans le modèle de graphe souhaité. Ces couches peuvent être définies à partir de caractéristiques immuables et représentatives des systèmes cyber-physiques. Cela améliorera à la fois la clarté de la représentation, mais aussi les possibles analyses qui en résultent.

II.3.5 Méthodologie générale

L'objectif de ces travaux est de fournir une méthodologie adaptée pour analyser la propagation d'anomalie dans les CPS. La méthodologie formulée dans cette thèse se caractérise par un certain nombre d'étapes essentielles. La distinction de ces étapes facilite la compréhension de l'approche, ainsi que son implémentation dans divers cas d'études relatifs aux CPS. Ces étapes sont divisées en deux catégories majeures. Premièrement, nous distinguons les étapes nécessaires à la modélisation du graphe représentatif du CPS étudié. Deuxièmement, le modèle résultant est utilisé pour évaluer la propagation d'anomalies.

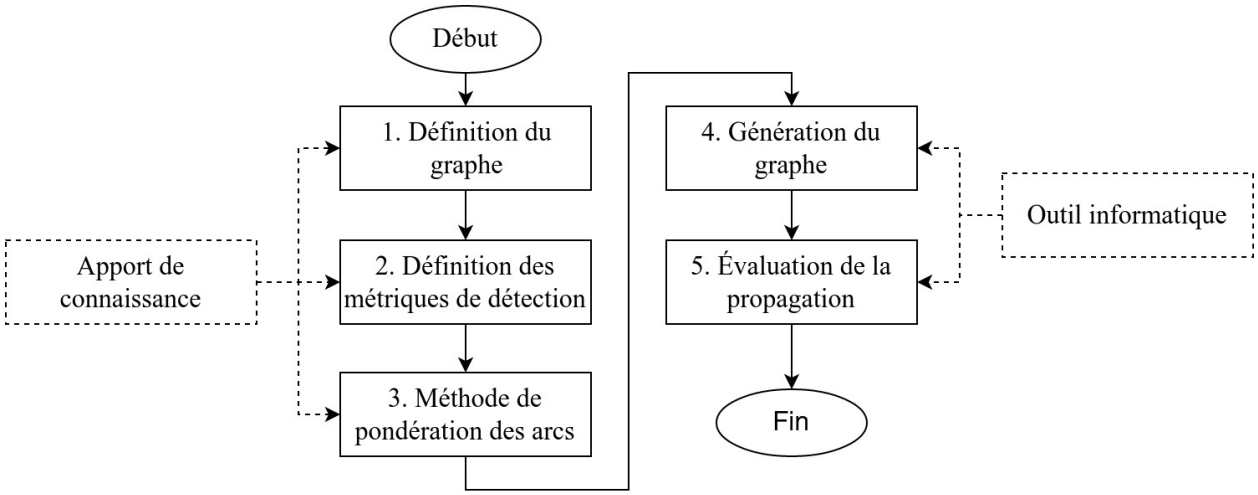


FIGURE II.3: Processus de réalisation des étapes de la méthodologie proposée

La méthodologie proposée est constituée des étapes suivantes (Figure II.3) :

1. **Définition du graphe** à partir des caractéristiques du CPS étudié. Il s'agit d'expliciter les différents éléments du système nécessaires à la modélisation sous forme de

graphe. Cela concerne les sous-systèmes, et les dépendances qui composent le CPS. L'apport de la connaissance d'un expert est nécessaire pour réaliser cette étape.

2. **Définition des métriques de détection** qui seront utilisées pour initier l'évaluation de la propagation d'anomalies dans le graphe. La pertinence et les performances des métriques de détection sont cruciales dans la suite de l'étude. De ce fait, le rôle d'un expert du domaine est là aussi prépondérant.
3. Réalisation de la **méthode de pondération des arcs** à partir de l'évaluation des risques des éléments du CPS étudié. L'évaluation quantitative des chemins de propagations résulte essentiellement des pondérations obtenues à la fin de cette étape. Sa bonne réalisation, par un expert ayant une connaissance adéquate du système, est primordiale vis-à-vis de la pertinence des résultats obtenus dans les étapes suivantes.
4. Lorsque l'ensemble des caractéristiques et propriétés du graphe ont été définies, sa **génération** est possible. Afin de faciliter cette étape, un outil informatique a été spécifiquement développé.
5. **L'évaluation de la propagation des anomalies** est réalisée grâce à un algorithme de parcours de graphe qui calcule les différents chemins potentiels de propagation. Un score d'impact est aussi calculé pour chaque chemin à partir des pondérations définies dans l'étape n° 3. L'outil informatique proposé permet d'automatiser l'évaluation de la propagation lorsqu'une anomalie est détectée grâce aux métriques définies dans l'étape n° 2.

Nous détaillerons plus précisément chacun des constituants de ces étapes dans les sections suivantes de ce chapitre.

II.4 Modélisation structurelle du CPS maritime

Afin de répondre à la problématique d'analyse et étude de la propagation d'anomalies dans les CPS, il est dans un premier temps nécessaire de définir une modélisation structurelle adaptée à l'objectif de ces travaux tout en considérant les spécificités et contraintes inhérentes aux CPS. L'abstraction proposée doit à la fois fournir un modèle mathématique adapté à l'intégration de diverses méthodologies d'analyse de la propagation, mais aussi un outil de visualisation claire pour schématiser les différents éléments et dépendances d'un tel type de système.

II.4.1 Définition d'un système cyber-physique

Un CPS se caractérise essentiellement par le suivi et le contrôle d'un processus physique à partir de différents éléments, aussi appelés *sous-systèmes*, contrôlés numériquement. Comme illustré dans la Figure II.4, un certain nombre de capteurs mesurent des données à partir de leur environnement physique et les transmettent à un programme de contrôle embarqué. Ce programme est exécuté au sein d'un automate programmable industriel qui supervise et contrôle le processus physique en générant des décisions de contrôle locales, proportionnelles aux données mesurées reçues [GPGV14]. Des commandes de contrôle sont dérivées de ces décisions et transmises aux actionneurs. Comme nous l'avons défini dans la section I.3.2, ce processus est surveillé et contrôlé à distance par un SCADA ou un DCS selon le cas d'application. En conséquence, les sous-systèmes qui définissent un CPS sont regroupés en deux couches principales selon leurs caractéristiques et propriétés :

— **Une couche numérique**, pour les sous-systèmes qui intègrent des capacités de calcul numérique et/ou de réseau. On y retrouve par exemple les différents postes informatiques, les serveurs, ou encore les divers équipements utilisés pour la gestion du réseau informatique, etc.

— **Une couche physique**, composée des capteurs et actionneurs qui interagissent avec un processus physique. Comme un capteur de niveau de réservoir, une vanne électronique, ou bien un moteur, etc.

Les deux couches interagissent entre elles par l'intermédiaire de deux flux de données : les variables mesurées par les capteurs, et les variables de contrôle associées aux commandes de contrôle. Ces deux flux de données majeures décrivent l'état du CPS à tout instant et sont les cibles principales des perturbations, générées par une anomalie dans le domaine cyber-physique.

Cette vision des CPS nous permettra de proposer, dans la section suivante, la définition d'une abstraction en adéquation avec les caractéristiques et contraintes inhérentes de ces systèmes.

II.4.2 Éléments structurels du modèle de graphe

Pour la suite de ces travaux, nous considérons que tout CPS étudié est défini à partir d'un graphe orienté G composé d'un nombre fini de *nœuds* V et de *relations* E. La définition de ces deux éléments structurels est inhérente aux besoins énoncés quant à la caractérisation

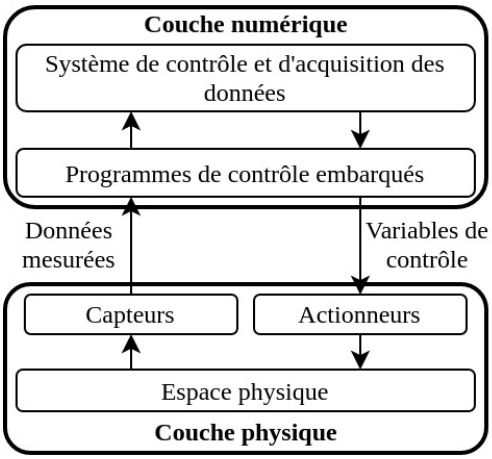


FIGURE II.4: Schéma de l'architecture de contrôle dans un CPS

de différents paramètres pour les sommets et arêtes du modèle de graphe souhaité. Une illustration de ces éléments est présentée dans la Figure II.5. Chacun de ces éléments peut être caractérisé par un nombre fini d'attributs.

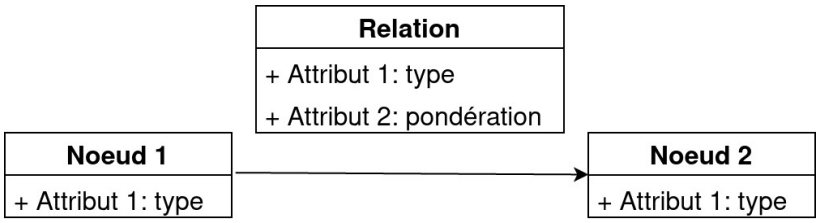


FIGURE II.5: Éléments structurels du graphe

Un *nœud* est une entité structurelle associée à chaque sommet du graphe. Il se caractérise ainsi par une liste de différents attributs définis selon l'application souhaitée. Dans ces travaux, nous définissons initialement un attribut principal qui est le *type* du nœud. Nous détaillerons par la suite l'ensemble des types de nœud considéré. De même, un certain type de nœuds se verra attribuer un autre attribut que nous préciserons dans la suite de ce chapitre.

Une *relation* est une entité structurelle, associée à chaque arc du graphe, qui lie 2 nœuds entre eux. Toute relation est orientée et composée d'une liste d'attributs potentiels. En accord avec le modèle de graphe souhaité, nous considérons initialement deux attributs : le type de la relation et la valeur de sa pondération. Dans la suite de ces travaux, nous préciserons les types de relations considérés, ainsi que la méthode de définition de leur pondération.

II.4.3 Modèle de graphe proposé

Le modèle de graphe proposé est défini à partir du couple présenté dans l'équation II.1. Il est composé de trois couches, indépendantes mais communicantes. Les deux premières couches sont définies à partir des caractéristiques propres des CPS présentées précédemment. Sont distinctement regroupés sur la première couche et deuxième couche les sous-systèmes numériques et physiques du CPS. La troisième couche du modèle est quant à elle associée aux variables système qui décrivent l'état courant du CPS avec des données mesurées par des capteurs, des variables de contrôle transmises aux actionneurs, ou encore des variables internes associées à un ou plusieurs sous-systèmes.

$$G = (V, E) \tag{II.1}$$

Le graphe G alors généré est composé de deux sous-graphes distincts :

— G_1 : le sous-graphe des sous-systèmes numériques et physiques du CPS, associé aux deux premières couches du modèle proposé.

— G_2 : le sous-graphe des variables systèmes associé à la troisième couche du modèle.

Chacun des sous-graphes possédant des caractéristiques propres, tant au niveau des nœuds que des arêtes, que nous présenterons dans les sous-sections suivantes. Le graphe G est alors défini comme suit : $G = \{G_1, G_2\}$.

II.4.4 Sous-graphe des sous-systèmes du CPS

Soit un CPS composé de N éléments, physiques ou numériques, qui interagissent entre eux. Chaque élément du système est représenté par un nœud s_i avec $i = 1, ..., I$. À partir du sous-graphe G_1, le système étudié est alors représenté comme un graphe orienté composé de I nœuds. Les relations r_j du graphe, avec $j = 1, ..., J$, caractérisent quant à elles les J dépendances entre les éléments du système. Le sous-graphe G_1 est illustré dans la Figure II.6 et défini par l'équation II.2.

$$G_1 = \{s_i, r_j\} \tag{II.2}$$

La relation qui associe deux nœuds du sous-graphe G_1 caractérise une dépendance entre les deux éléments associés. En accord avec la définition de la notion de dépendance, proposée

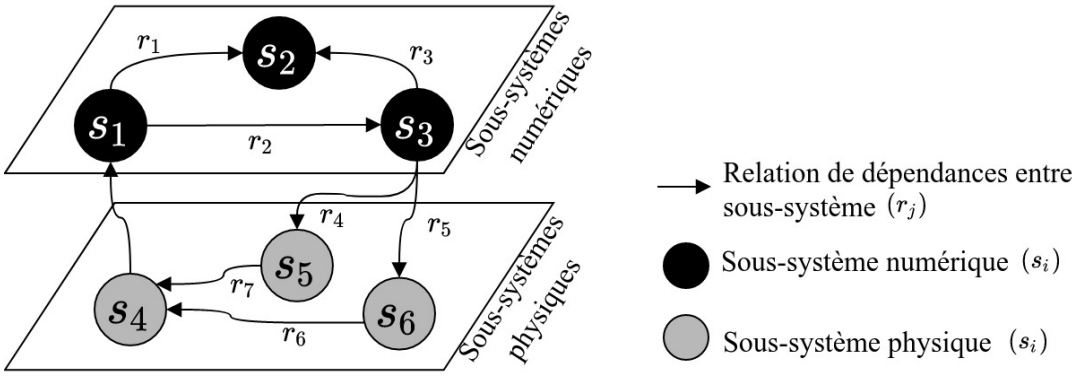


FIGURE II.6: Sous-graphe des sous-systèmes physiques, numériques, et leurs dépendances

dans la section, celle-ci peut traduire différents types de liens :

- Une **dépendance numérique**, pour caractériser les échanges d'informations ou un lien de connexion entre sous-systèmes et composants numériques. Ce type de dépendance regroupe les différentes liaisons de communication ainsi que les normes et protocoles associés. Sont regroupées les liaisons filaires (série, Ethernet, fibre optique, etc.), et sans fil au travers des communications radio (cellulaires, Bluetooth, WiFi, etc.).
- Une **dépendance physique**, associée à un transfert physique entre deux sous-systèmes impliqués dans un processus physique.
- Une dépendance en lien avec la transmission de **mesures de capteur** pour le suivi d'un processus physique.
- Une dépendance associée à la transmission de **commandes de contrôle** de l'automate vers les actionneurs pour le suivi du processus physique.

Nous supposons que tous ces types de dépendances influent tout autant sur la propagation d'anomalie dans le système étudié. Par conséquent dans le reste de cette étude elles seront représentées dans le sous-graphe G_1, composé des sous-systèmes du CPS, comme un même ensemble R de relations de dépendances r_j entre deux nœuds s_i d'un même CPS.

II.4.5 Sous-graphe des variables du CPS

Comme défini précédemment, le CPS est composé d'un ensemble V de variables mesurables qui décrivent son état à tout instant t. Chacune de ces variables est représentée par un nœud v_k avec $k = 1, ..., K$. Ces variables peuvent être corrélées entre elles par un ensemble C

de relations de corrélation tel que défini précédemment (Définition II.3). La représentation du système étudié est alors complétée par un second sous-graphe orienté G_2 défini par un ensemble de nœuds v_k et de relations de corrélations c_l, avec $l = 1, ..., L$, entre celles-ci (équation II.3). Le sous-graphe associé est présenté dans la Figure II.7.

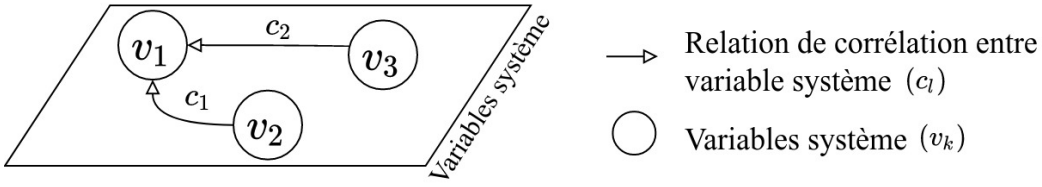


FIGURE II.7: Sous-graphe des variables système

$$G_2 = \{v_k, c_l\} \tag{II.3}$$

Pour définir des types de corrélation entre les variables d'un CPS, nous nous sommes basés sur les travaux de Yong Wang *et al.* [WXZ+14] et Dennis Volpano *et al.* [VIS96] qui apportent des éléments de réponses quant aux diverses dépendances entre les variables d'un système. Yong Wang *et al.* définissent une corrélation (équation II.4) entre diverses variables lorsque l'état actuel d'une d'entre elles (v_k) dépend de la valeur d'une ou plusieurs autres ($v_m, v_n...$) . Dennis Volpano *et al.* ont quant à eux formalisé des liens *explicites* (i.e. $x = y+5$) et *implicites* (i.e. $x = 5$, si $y > 0$) entre les variables d'un programme de contrôle de système.

$$v_k = f(v_m, v_n...) \tag{II.4}$$

Dans le cadre du modèle proposé dans ces travaux de thèse, nous caractérisons deux types principaux de corrélation entre deux variables v_j et v_m :

— Une corrélation **structurelle** lorsque la variation de la valeur d'une variable v_m entraîne proportionnellement une variation de valeur d'une variable v_j.

— Une corrélation **conditionnelle** lorsque la variation de la valeur d'une variable v_m entraîne une variation spécifique de la valeur d'une variable v_j.

Lorsqu'il existe une de ces corrélations entre deux variables, une relation de corrélation est schématisée depuis la variable qui influe sur la valeur de la seconde.

Dans les travaux présentés, nous nous intéressons davantage à la considération de l'influence d'une variable sur une autre plutôt qu'au type d'influence en lui-même. De ce fait, nous considérerons par la suite ces deux types de corrélation au même titre. Dans le modèle

de graphe proposé, ces corrélations sont représentées sous forme d'un ensemble C de relations de corrélation c_l (structurelle ou conditionnelle) liant deux nœuds de variable système v_k de la troisième couche du modèle.

II.4.6 Construction des relations

La principale difficulté de cette méthode réside dans l'identification de ces relations, que ce soit pour le sous-graphe des sous-systèmes ou des variables du CPS. La solution la plus simple serait de les définir lors du processus de conception du système. Néanmoins, cela n'est pas réalisé automatiquement.

Pour déterminer les relations dans le sous-graphe des sous-systèmes du CPS, l'implication d'un expert du domaine est essentielle. Ces relations sont principalement implicites et nécessitent une véritable expertise métier pour obtenir une représentation du CPS cohérente et adaptée. Cette expertise doit réunir toutes les connaissances nécessaires durant l'ensemble du cycle de vie du système, de la conception à la phase opérationnelle. Les relations entre les nœuds du sous-graphe G_1 sont alors construites selon les connaissances du système obtenues.

Pour identifier et définir les relations entre les variables du sous-graphe des variables système, une autre approche doit être utilisée lorsque celles-ci ne sont pas définies en amont lors de la conception du système. Par exemple, une méthode conventionnelle de modifications des commandes de contrôle peut être appliquée pour modifier la valeur d'une variable de contrôle à la fois et observer l'impact de ce changement sur les autres variables. Les arêtes orientées du sous-graphe sont construites en conséquence depuis la variable modifiée vers la ou les variable(s) altérées. Le système est alors réinitialisé et une autre variable est modifiée. Ce processus itératif est poursuivi jusqu'à ce que toutes les relations de corrélation entre les variables soient identifiées.

II.4.7 Relations entre les sous-graphes

Comme défini précédemment, la modélisation du CPS fournit un graphe lui-même composé de deux sous-graphes, G_1 associé aux sous-systèmes numériques et physiques de la première et deuxième couche du modèle, et G_2 défini par les variables systèmes de la troisième couche du modèle. Chacun de ces sous-graphes est généré de manière indépendante et possède des composants différents, tant au niveau des arêtes que des nœuds. La distinction

de ces deux sous-graphes fournit néanmoins une modélisation conforme aux caractéristiques propres aux CPS concernant la dualité de domaines physiques et numériques. Le premier sous-graphe permet de définir distinctement chaque sous-système physique et numérique tout en les unifiant au travers de relations de dépendances. De surcroît, le deuxième sous-graphe fournit une caractérisation des variables système et de leurs relations de corrélation.

Dans un CPS, toute variable le définissant peut-être associé à un ou plusieurs sous-systèmes. Le modèle proposé retranscrit cette caractéristique au travers de relations d'association entre les variables système de la troisième couche et les sous-systèmes des première et seconde couches. Ce type de relation lie les deux sous-graphes G_1 et G_2 entre eux. Ainsi, les sous-systèmes s_i du CPS sont associés aux variables système v_k les définissant au travers d'un ensemble A de relations d'association a_u. Nous verrons par la suite que cette relation est d'autant plus importante, car elle amorce le processus d'évaluation de la propagation d'anomalies dans le système.

Les nœuds et relations qui composent les sous-graphes G_1, associés aux sous-systèmes physiques et numériques, et G_2, associés aux variables système, sont décrits dans la Table II.1. Les relations qui lient ces deux sous-graphes sont présentées dans la Table II.2. L'association des deux sous-graphes, ainsi que de leurs composants, est illustré dans la Figure II.8.

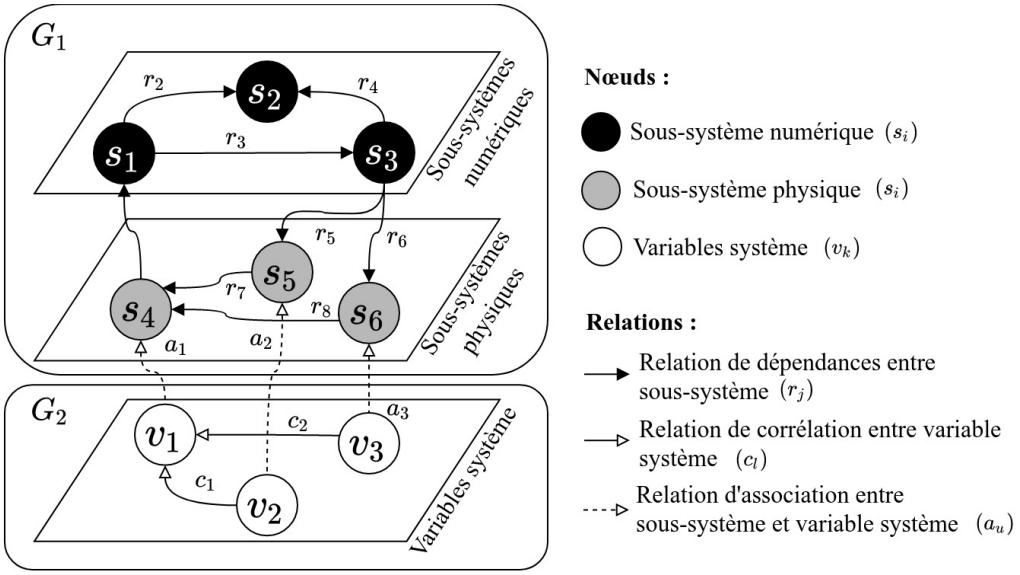


FIGURE II.8: Association des deux sous-graphes

TABLE II.1: Description des deux sous-graphes générés

	Nœuds		Relations	
Sous-graphe	Définition	Type	Définition	Type
G_1	$S = \{s_i\}$ $i = 1, ..., I$	Sous-système physique Sous-système numérique	$R = \{r_j\}$ $j = 1, ..., J$	Dépendances
G_2	$V = \{v_k\}$ $k = 1, ..., K$	Variable système	$C = \{c_l\}$ $l = 1, ..., L$	Corrélation

TABLE II.2: Description du lien entre les deux sous-graphes

	Relation	
	Définition	Type
Lien entre G_1 et G_2	$A = \{a_u\}$ $u = 1, ..., U$	Association

II.4.8 Cas d'exemple

L'ensemble de la méthode de génération du graphe 3-couches est illustrée ici à partir d'un exemple générique de modélisation d'un CPS chargé du contrôle d'un processus physique (Figure II.9). Un capteur C1 transforme l'état d'une grandeur physique, associée au processus physique, en données mesurées. Ces données sont récupérées par le PLC1 puis transmises au PLC2, responsable du fonctionnement des actionneurs A1 et A2. Selon la valeur de la mesure transmise, les actionneurs sont allumés ou éteints en conséquence et induisent une variation de l'état du processus physique. L'ensemble du processus est supervisé et contrôlé à distance grâce à un système *SCADA* qui reçoit les valeurs de mesure du capteur et l'état des actionneurs.

Les différents sous-systèmes sont modélisés au sein du sous-graphe G_1 sous forme d'un ensemble S de $I = 6$ nœuds des sous-systèmes physiques ou numériques, tel que défini dans l'équation suivante :

$$S = \{SCADA, PLC1, PLC2, C1, A1, A2\} \tag{II.5}$$

Ces sous-systèmes sont reliés entre eux par un ensemble R de $J = 6$ relations de

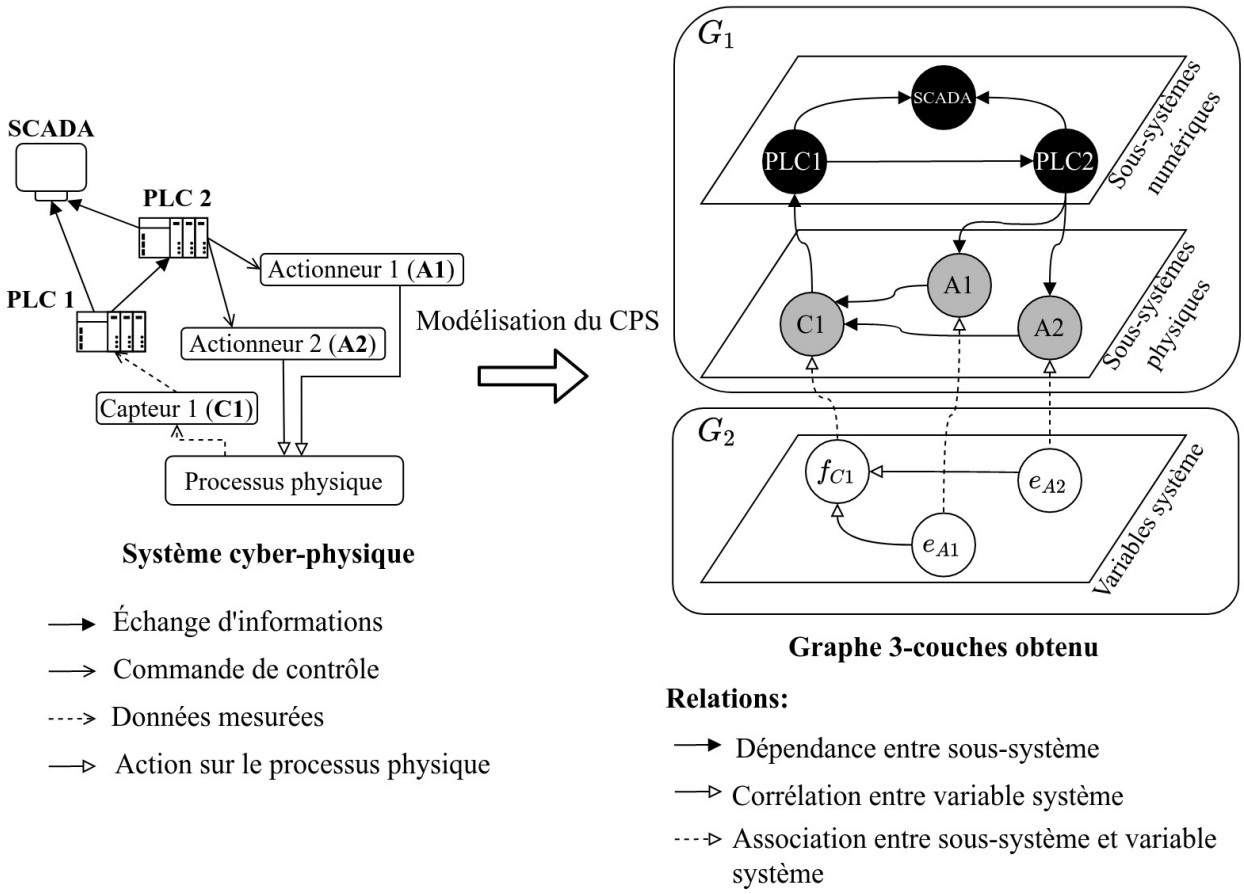


FIGURE II.9: Modélisation du CPS en graphe 3-couches

dépendance :

$$R = \{PLC1 \rightarrow SCADA, PLC1 \rightarrow PLC2, PLC2 \rightarrow SCADA, C1 \rightarrow PLC1, PLC2 \rightarrow A1, PLC2 \rightarrow A2\} \quad \text{(II.6)}$$

Différents sous-systèmes du CPS étudié sont définis par une ou plusieurs variables. Chaque actionneur est défini par une variable d'état binaire e. Le capteur est quant à lui associé à une variable f traduisant une grandeur du processus physique. Le sous-graphe G_2 est alors composé d'un ensemble V de $K = 3$ nœuds de variables système, tel que :

$$V = \{f_{C1}, e_{A1}, e_{A2}\} \quad \text{(II.7)}$$

Ces variables sont reliées entre elles à partir d'un ensemble C de $L = 2$ relations de

corrélation structurelles ou conditionnelles :

$$V = \{e_{A1} \rightarrow f_{C1}, e_{A2} \rightarrow f_{C1}\} \tag{II.8}$$

Les sous-graphes G_1 et G_2 sont liés l'un a l'autre au travers d'un ensemble A de $U = 3$ relations d'association entre les variables système v_k et les sous-systèmes s_i :

$$A = \{f_{C1} \rightarrow C1, e_{A1} \rightarrow A1, e_{A2} \rightarrow A2\} \tag{II.9}$$

II.4.9 Intégration de la méthode de détection

Lorsque le graphe est généré, diverses métriques de détection basées sur différentes méthodes de détection y sont intégrables. Cette intégration permet une visualisation et une représentation claire des métriques choisies pour la détection d'anomalies au sein du CPS. Ces métriques peuvent aussi être impliquées dans diverses méthodes d'analyse du graphe, notamment pour l'analyse et l'évaluation de la propagation d'anomalies dans un CPS maritime. La polyvalence et la généricité de la méthode proposée octroient l'intégration de différents types d'attributs supplémentaires aux nœuds. Les métriques de détection sont définies comme des attributs supplémentaires des nœuds de variables système de la troisième couche du modèle.

Des données et informations étant constamment échangées entre les sous-systèmes et composants d'un CPS, nous exploiterons exclusivement des métriques de détection basées sur l'analyse de la qualité des données et des informations. Ces mesures de qualité des données et des informations sont associées au modèle de graphe proposé par l'intermédiaire de leur intégration à chaque nœud de variable système. Parmi les quatre types d'évaluation de la qualité définis par le modèle DIKW, comme présenté dans la section I.3.4, nous avons choisi d'en étudier deux d'entre elles :

— $\overrightarrow{DQV}$: le vecteur d'évaluation de la qualité des données
— $\overrightarrow{IQV}$: le vecteur d'évaluation de la qualité des informations

L'évaluation de la qualité d'un sous-système, associée à un flux de données comportant Q imperfections, est définie par des métriques d'évaluation de la qualité des données d_b. Les informations produites sont examinées sur D dimensions à partir de différentes métriques d'évaluation de la qualité des informations i_e. Les vecteurs respectifs $\overrightarrow{DQV}$ et $\overrightarrow{IQV}$ se ca-

ractérisent ainsi :

$$\overrightarrow{DQV} \in \{d_1 ... d_Q\} \tag{II.10}$$

$$\overrightarrow{IQV} \in \{i_1 ... i_D\} \tag{II.11}$$

L'évaluation de la qualité (QE) est alors sous forme vectorielle $\overrightarrow{QE}_{v_k}$ composée du vecteur d'évaluation de la qualité des données $\overrightarrow{DQV}$ et de l'information $\overrightarrow{IQV}$ (équation II.12).

$$\overrightarrow{QE}_{v_k} = \{\overrightarrow{DQV}_{v_k}, \overrightarrow{IQV}_{v_k}\} \tag{II.12}$$

Comme le montre la figure II.10, ces évaluations de la qualité sont intégrées au sein du graphe comme attribut de chacune des v_k variables système correspondantes. Il est important de souligner que selon le cas d'étude, seul un sous-ensemble des dimensions de la qualité des données et des informations est indépendamment évalué pour chaque variable du système.

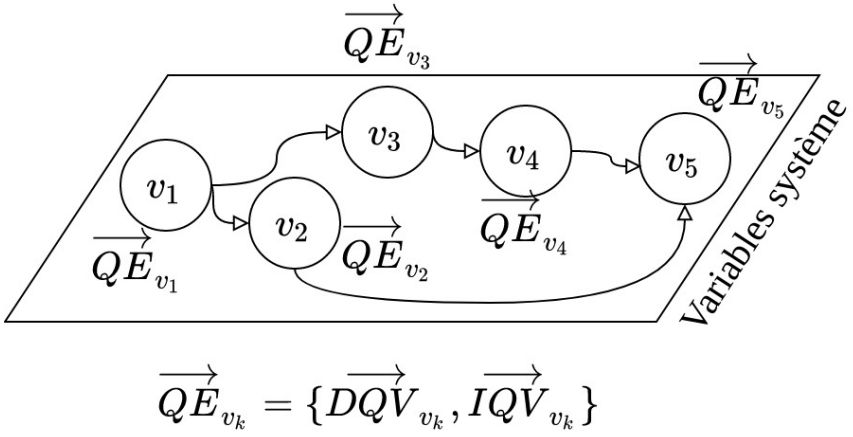


FIGURE II.10: Intégration de l'évaluation de la qualité dans le graphe

II.5 Évaluation de la propagation d'anomalies

La problématique initiale de cette thèse est de fournir une méthode d'évaluation de la propagation d'anomalies dans les CPS maritimes. Pour y répondre, nous avons dans un premier temps développé une modélisation structurelle du CPS sous forme de graphe orienté

multicouche, représentant ses composants et les diverses dépendances associées. Dans les sections suivantes, nous allons détailler la méthode d'évaluation de la propagation à partir des calculs de chemins de propagations potentiels. Grâce à la formulation d'une méthode de pondération des relations de dépendances du modèle de graphe, nous sommes à même de fournir une évaluation quantitative de chaque chemin en calculant un score d'impact.

II.5.1 Objectif

Comme présenté dans la section I.2, la complexité des systèmes maritimes ne cesse et ne cessera de s'accroître dans le futur. Cela s'explique principalement par leur forte numérisation pour répondre aux besoins opérationnels de missions toujours plus diverses et variées. Cette complexité est principalement associée à un niveau de dépendance entre les systèmes maritimes embarqués toujours plus croissant. La démocratisation des navires autonomes, ainsi que l'utilisation de véhicules sans pilotes, accentue d'autant plus cette croissance et les différents besoins qui en résultent. Pour assurer les performances et la sécurité globale du navire, il est nécessaire de mettre en place des méthodes et outils adaptés pour caractériser, analyser et atténuer les risques associés à ce fort niveau de dépendances. Cela doit être réalisé durant l'ensemble des phases du cycle de vie du navire. Nos travaux s'inscrivent dans la démarche du maintien de sécurité numérique du système maritime par la définition d'une méthode d'évaluation des chemins de propagation d'anomalies dans un CPS maritime pour les identifier, analyser, et quantifier. L'approche proposée s'inspire des travaux scientifiques relatifs à l'analyse de la propagation par graphes d'attaques, tel que cela a été identifié dans la section I.4 du chapitre I.

II.5.2 Méthode d'évaluation des chemins de propagation

L'abstraction mathématique offerte par la représentation du CPS sous forme de graphe se caractérise par sa polyvalence. Le graphe généré est ainsi exploitable dans diverses applications. Dans le cadre de ces travaux, nous l'avons utilisé pour obtenir les chemins de propagations d'anomalies, et évaluer quantitativement leur impact potentiel. Un chemin de propagation se caractérise par une succession de sous-systèmes ou composants liés entre eux par une quelconque relation pondérée. Le poids de la relation retranscrit la capacité d'un sous-système ou composant, physique ou numérique, à propager une anomalie et à impacter les autres sous-systèmes avec lesquels il interagit. Cette pondération est réalisée à partir

d'une méthode d'évaluation des risques que nous détaillerons par la suite.

Le principal défi pour cette évaluation de la propagation d'anomalies réside dans le fait de définir et de caractériser chaque chemin de propagation. L'analyse quantitative permet d'identifier et de comparer la criticité de ces chemins. Ce qui paraît simple et évident pour un graphe constitué d'une dizaine de nœuds et de relations peut rapidement se complexifier avec un graphe issu d'un CPS constitué de centaines de sous-systèmes et de dépendances associées. Afin de répondre à cette problématique, différents algorithmes basés sur la théorie des graphes fournissent les outils adaptés pour extraire les informations nécessaires à tout type d'étude et d'analyse. La méthode proposée d'évaluation de la propagation d'anomalie dans un graphe de CPS s'appuie majoritairement sur un algorithme d'exploration du graphe, et plus précisément de recherche de chemins. Comme nous l'avons explicité dans la section I.5.3, ce type d'algorithme explore les différentes routes entre un nœud initial et un nœud cible en parcourant les nœuds et relations qui les séparent. Ils sont généralement utilisés pour identifier et parcourir les chemins optimaux à travers un graphe, et cela pour diverses applications.

L'algorithme que nous avons développé dans le cadre de ces travaux utilise le DFS pour définir et caractériser les potentiels chemins de propagation d'anomalies du graphe à partir d'un nœud initiateur. Ce nœud est caractérisé par la détection d'une anomalie grâce à une métrique de détection définie comme attribut d'une variable système. Nous verrons par la suite que l'algorithme développé est exploité au travers de deux processus distincts d'évaluation de la propagation. Comme nous l'avons présenté dans la section I.5.3, le score associé à chaque chemin est égal à la somme des pondérations de chaque arête parcourue. En adéquation avec l'objectif de nos travaux, il est alors nécessaire de définir une pondération aux relations constituant le graphe multicouche orienté proposé. Nous détaillerons la méthodologie de calcul de pondération mise en place dans les sections suivantes.

II.5.3 Problématique de la pondération du graphe

Comme cela a été détaillé dans la section I.5.2, la pondération des arcs est une caractéristique majeure pour l'analyse résultante du graphe concerné. Cette pondération est définie comme une magnitude associée à chaque arc. Pour l'analyse que l'on souhaite obtenir du graphe multicouche proposé, la pondération des relations apparaît comme essentielle pour expliciter quantitativement la criticité de chacune d'entre elles.

La pondération d'un graphe est généralement définie à partir d'une caractéristique commune à chaque arc. Par exemple, pour un graphe représentant différentes villes et routes entre celles-ci, la pondération des arcs qui lient chaque ville peut être explicitée à partir de la distance réelle entre chacune d'entre elles. Pour les CPS, cela n'est pas aussi simple. Ce type de système se distingue en effet par une hétérogénéité inhérente de ses sous-systèmes, ainsi que des dépendances entre ceux-ci. Ces dépendances peuvent être fonctionnelles, ou encore caractériser l'échange de données ou d'informations au travers de liaisons de communications physiques ou numériques. Là encore, chaque type de communications se distingue par différentes propriétés comme les normes utilisées, les protocoles, ou encore les vitesses de débits. Il est alors difficile d'identifier et de définir une caractéristique commune à chacune d'entre elles pour déterminer une pondération aux relations du modèle de graphe proposé.

Parmi les travaux scientifiques existants qui traitent de la représentation des CPS sous forme de graphe, nous avons identifié deux types de méthode de pondération. L'emploi de chacune d'entre elles possède des bénéfices et des inconvénients. La première méthode, formulée par Koosha Marashi *et al.*, définit la pondération des arcs du graphe à partir de la variable de « degré d'influence », comprise dans l'intervalle $[0, 1]$. Ce poids est fixé de manière **subjective** à partir des connaissances d'un expert, de retour d'expériences ou de simulations, ou encore grâce à diverses informations extérieures [MSH16]. Une deuxième méthode caractérise la pondération de chaque arc du graphe en fonction de la **topologie** du sommet dont il résulte. Le poids est ainsi calculé en fonction de différentes métriques basées sur les caractéristiques topologiques du sommet [KK20].

Ces deux méthodes présentent le bénéfice d'être relativement à simples à définir. Néanmoins, elles sont associées à différents aspects qui impactent leur représentativité. Concernant la première méthode, celle-ci repose uniquement sur une connaissance externe subjective, donc extrêmement difficile à justifier. Tandis que la deuxième se base exclusivement sur la topologie du sommet pour déterminer sa criticité. Or la topologie d'un nœud n'est pas représentative de sa criticité opérationnelle.

Les méthodes de pondération existantes dans la littérature n'étant pas satisfaisantes, nous avons fait le choix de développer dans nos travaux de thèse une méthode spécifique. Celle-ci s'appuie sur une évaluation du niveau de menace des sous-systèmes d'un CPS. Chaque sous-système du CPS, représenté sous forme de nœud physique ou numérique dans notre modèle, sera ainsi évalué pour obtenir un poids qui sera associé à chaque relation de dépendance qui résulte de ce même nœud.

II.5.4 Définition de la méthode d'évaluation du niveau de menace

Nous proposons au travers de ces travaux une méthode d'évaluation du niveau de menace des sous-systèmes d'un CPS. Elle se base sur un ensemble de métriques objectives qui caractérisent les spécificités d'un CPS, et plus particulièrement un CPS maritime.

La méthode proposée s'appuie en partie sur les principes et caractéristiques de la méthode EBIOS [3] RM^4, une méthode de référence publiée par l'ANSSI [5] pour l'appréciation et le traitement des risques numériques. Cette méthode d'analyse de risque offre un outil de compréhension des risques numériques associés à une quelconque organisation. Elle repose sur 5 ateliers distincts [ANS19], réalisés par les décideurs et les acteurs opérationnels de l'organisation concernée. Le premier atelier vise à identifier l'objet de l'étude ainsi que le cadre temporel. Dans le deuxième atelier les différentes sources de risques, et leurs objectifs, sont identifiés et caractérisés. Le troisième atelier permet de définir l'écosystème de l'objet étudié pour établir une cartographie des menaces numériques extérieures. Dans l'atelier n°4, différents scénarios sont construits en exploitant les sources de risques précédemment identifiées. Pour finir, le dernier atelier consiste à synthétiser l'ensemble des risques étudiés dans les ateliers précédents pour les traiter à partir de mesures de sécurité. Cette méthode généraliste se caractérise par une forte adaptabilité afin d'être utilisée dans divers domaines d'application. Elle est principalement utilisée pour :

— Mettre en place ou renforcer un processus de management du risque numérique au sein d'une entité.
— Caractériser, apprécier et traiter les risques numériques relatifs à un système ou une entité.
— Définir des niveaux de sécurité numérique à atteindre pour un système ou un service indépendamment du secteur d'activité.

Comme toute méthode d'évaluation des risques, la véracité et la représentativité, de la méthode proposée repose essentiellement sur la collaboration de différents acteurs. Elle requiert des connaissances techniques, architecturales, mais aussi opérationnelles du système étudié.

3. Expression des Besoins et Identification des Objectifs de Sécurité
4. Risk manager
5. Agence nationale de la sécurité et des systèmes d'information

II.5.5 Réalisation de la méthode d'évaluation du niveau de menace

Le processus d'évaluation est réalisé pour chaque sous-système du CPS, numérique ou physique, des deux premières couches du modèle de graphes. Ces éléments ont été précédemment identifiés et définis lors du processus de génération du graphe. La troisième couche du modèle de graphe, caractérisant les variables système, n'est donc pas prise en compte.

La méthode d'évaluation proposée s'inspire de la méthode de l'atelier 3 d'EBIOS RM pour l'évaluation du niveau de menace des parties prenantes [Age18b]. Une partie prenante est définie comme un élément avec lequel l'objet étudié interagit directement ou indirectement pour réaliser ses missions et services. Ces interactions représentent des chemins d'attaques potentielles critiques pour l'objet de l'étude. Il est alors primordial de construire une cartographie de ces menaces afin de les identifier, les caractériser et les évaluer. Pour cela, l'ANSSI met à disposition une liste de parties prenantes à prendre en compte, et surtout, une méthode d'évaluation du niveau de menace. Cette méthode permet de caractériser et d'évaluer le niveau de menace induit par chaque partie prenante, en fonction de leurs caractéristiques et propriétés inhérentes, sur l'objet étudié [ANS19]. Elle repose sur des critères d'**exposition** (dépendance, pénétration) et de **fiabilité cyber** (maturité, confiance). Une métrique de cotation, composée de 4 niveaux, est associée à chaque critère. Le niveau de menace que représente une partie prenante vis-à-vis de l'objet de l'étude est alors calculé à partir de l'association de ces 4 critères (Figure II.11). Pour représenter le niveau de menace de chaque partie prenante vis-à-vis de l'objet d'étude, chaque niveau de menace calculé pour chaque partie prenante est répertorié au sein d'une cartographie radiale [6] avec l'objet de l'étude placé en son centre. Cette cartographie est composée de différentes zones de risques définis à partir de seuils de niveau de menace définis en amont.

La cartographie des menaces obtenue est ensuite utilisée au sein l'atelier 4 [Age18b], pour établir différents scénarios opérationnels. Cette démarche globale vise à identifier et évaluer des scénarios d'attaque représentés sous forme de graphe d'attaque composé d'enchaînement d'actions élémentaires sur des biens supports. Ces actions élémentaires sont définies selon une liste fournie par la méthode. Les graphes d'attaques obtenues sont par la suite évalués selon leur vraisemblance, i.e une évaluation qui reflète le degré de faisabilité ou de possibilité que l'attaque aboutisse. L'évaluation de la vraisemblance des graphes d'attaques peut être combinée à la gravité pour estimer le niveau de risque.

6. L'objet de l'étude est placé au centre de la cartographie, et les parties prenantes en périphérie plus ou moins lointaine selon leur niveau de menace associé.

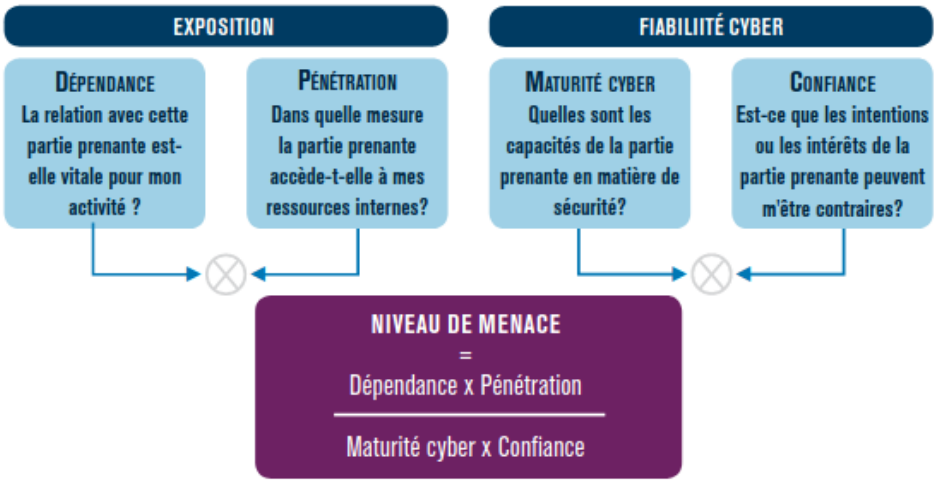


FIGURE II.11: Calcul du niveau de menace associé à une partie prenante [ANS19]

L'ANSSI insiste particulièrement sur la généricité de leur approche proposée pour l'évaluation du niveau de menace [ANS19]. Cette généricité s'applique à la fois pour la formule de calcul présentée dans la Figure II.11, ainsi que pour la définition des critères d'évaluation et de la métrique de cotation associée. La méthode proposée est donc adaptable à différents contextes d'activité et à différents objets d'étude.

De ce fait, nous avons adapté et complété cette méthode pour la transposer au domaine d'application d'un CPS maritime pour évaluer le niveau de menace de chacun de ses composants. Tel que défini dans la méthode EBIOS RM, le CPS global fait figure d'objet d'étude et ses sous-systèmes sont assimilables à des parties prenantes qui interagissent en son sein pour réaliser diverses missions et différents services. Notre méthode d'évaluation du niveau de menace d'un sous-système du CPS repose sur 4 critères d'évaluation adaptés aux caractéristiques et contraintes d'un CPS maritime. Tout comme celle proposée par EBIOS RM, cette évaluation repose sur des critères d'**exposition** qui tendent à accroître le niveau de risque et l'impact de la propagation vis-à-vis des vulnérabilités du système, et des critères **fiabilité cyber** qui l'atténuent. Des études scientifiques relatives à l'analyse du risque cyber-maritime ont déjà utilisé la notion d'exposition, définie par divers critères, pour quantifier la criticité de divers SIM. Victor Bolbot *et al.* [BTBV20], ainsi que le Bureau Veritas [7] [BV18], définissent l'exposition à partir des critères de **connectivité** et de **complexité**. Néanmoins, la notion de fiabilité cyber n'a pas encore été traitée sous la forme que nous la proposons.

7. Une société spécialisée dans les essais, l'inspection et la certification, qui opèrent dans divers domaines d'application, dont le maritime.

Les critères d'évaluation proposés dans ces travaux se caractérisent ainsi :

— Deux critères E_n, qui caractérisent respectivement la **connectivité** et la **connaissance** associée au CPS étudié. L'association de ces deux critères définit l'**exposition** du système quant à sa surface d'attaque et les conséquences potentielles.
— Deux critères FC_n, qui caractérisent respectivement le niveau de **supervision** associé au CPS et la **maîtrise** de celui-ci. L'association de ces deux critères définit la **fiabilité cyber** accordée au CPS étudié.

Chacun des critères E_n et FC_n est divisé en 2 paramètres $e_{n,1}$, $e_{n,2}$ (égalité II.13) et $fc_{n,1}$, $fc_{n,2}$ (égalité II.14) pour apporter davantage de précision quant à leur caractérisation.

$$E_n = \left\{e_{n,1}, e_{n,2}\right\}, n = [1,2] \;\; et \; n \in \mathbb{N} \tag{II.13}$$

$$FC_n = \left\{fc_{n,1}, fc_{n,2}\right\}, n = [1,2] \;\; et \; n \in \mathbb{N} \tag{II.14}$$

La méthode proposée d'évaluation du niveau de menace se caractérise par sa généricité. Elle nécessite, comme toute méthode relative à l'analyse de risque, une implémentation spécifique au domaine d'application et à l'objet de l'étude. Cette implémentation se caractérise par la définition d'une métrique de cotation, et des définitions associées, pour chaque paramètre. Elle doit ainsi être spécifiquement définie selon le domaine d'étude et les informations que l'on souhaite obtenir à l'issue du processus d'évaluation.

Dans le cadre de ces travaux nous avons implémenté cette méthode au travers d'une métrique de cotation composée de 4 niveaux de risques, et de définitions associées, spécifiquement identifiés pour la problématique des CPS maritimes. Chaque paramètre e et fc de chaque critère est associé à un niveau de cotation qui traduit quantitativement le niveau du paramètre en fonction des définitions proposées pour chaque niveau. On distingue ainsi 4 niveaux de cotation de 1 à 4. Le processus de cotation de chaque paramètre de chaque critère doit être répété pour chaque élément du CPS. L'ensemble de ces niveaux de cotations, et leurs définitions associées, sont rassemblés dans les tableaux II.3, II.4, II.5 et II.6.

Pour les paramètres du critère d'**exposition** : plus leur niveau de cotation est élevé, plus le système étudié est potentiellement exposé aux attaques et aux possibles conséquences en résultant. Pour les paramètres du critère de **fiabilité cyber** : plus leur niveau de cotation est élevé, plus les mesures mises en place vis-à-vis du système œuvrent à atténuer l'apparition

d'attaques ou défaillance, et à restreindre leurs possibles conséquences.

TABLE II.3: Cotation des paramètres du critère E_1

E_1 : Connectivité	$e_{1,1}$: Type de connexion	1 : Le sous-système n'échange aucune donnée/information complexe. Il est exclusivement défini par des connexions analogiques ou physiques (ex : ligne téléphonique, arbre de transmission relié à une hélice, câble électrique, etc.).
		2 : Le sous-système étudié est connecté à un ou plusieurs autres sous-systèmes/éléments par le biais de connexions numériques filaires unidirectionnelles. Toutes les communications ou échanges sont exclusivement initiés d'un sous-système vers l'autre. D'un point de vue logique/fonctionnelle le sous-système cible n'est pas connecté au premier.
		3 : Le sous-système étudié est interconnecté à un ou plusieurs autres sous-systèmes/éléments par le biais de connexions numériques filaires bidirectionnelles. La communication ou échange de données/informations peut être réalisée depuis n'importe quel des deux sous-systèmes impliqués.(câble ethernet, modbus, usb, etc.)
		4 : Le sous-système étudié est interconnecté à un ou plusieurs autres sous-systèmes/éléments par le biais d'un accès sans-fil (wi-fi, bluetooth, connexion satellitaire, 4G, etc.). Aucune restriction dans le sens des communications. Ce service confère à l'utilisateur un droit d'accès pour interagir avec le sous-système étudié. Cette interaction peut être passive (lecture de variable, contrôle de l'état, etc.) et/ou active (activation de processus, modification du sous-système, etc.).
	$e_{1,2}$: Privilèges/droits	1 : Le sous-système accède ou échange avec des terminaux utilisateur (poste de travail, téléphone mobile, etc.).
		2 : Le sous-système accède ou échange avec des réseaux composés de terminaux utilisateur (parc informatique, flotte de terminaux mobiles, etc.).
		3 : Le sous-système accède ou échange avec des serveurs métier (serveur de fichiers, bases de données, serveur web, serveur d'application, etc.).
		4 : À Accès ou échange avec des équipements d'infrastructure (annuaires, DNS, DHCP, commutateurs, pare-feu, hyperviseurs, baies de stockage, etc.).

TABLE II.4: Cotation des paramètres du critère E_2

E_2 : Connaissance	$e_{2,1}$: Internalisation	1 : Les éléments du sous-système ont été créés et assemblés en interne. Aucun élément du sous-système n'est sous-traité.
		2 : Élément du sous-système en partie sous-traité ou comprenant des composants sous-traités. Le sous-système est assemblé en interne.
		3 : Éléments du sous-système entièrement sous-traités à partir d'un cahier des charges fourni. Le sous-système est assemblé en interne.
		4 : Le sous-système est dit « sur étagère », il est générique et utilisé tel quel.
	$e_{2,2}$: Impact opérationnel	1 : Les conséquences sont négligeables pour le sous-système. Aucun impact opérationnel sur les performances de l'activité ou sur la sécurité des personnes et des biens. Le sous-système surmontera la situation sans trop de difficultés.
		2 : Les conséquences sont significatives mais limitées pour le sous-système. Dégradation des performances de l'activité, la mission n'est pas impactée. Celle-ci se déroule sans changements imposés mais plus de ressources vont devoir y être allouées. Le sous-système surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
		3 : Incapacité pour le sous-système d'assurer la totalité ou une partie de son activité. Les conséquences sont importantes pour le sous-système. Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. Le sous-système surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
		4 : Les conséquences sont désastreuses pour le sous-système. Son écosystème peut être impacté de façon importante, avec des conséquences éventuellement durables. Incapacité pour le sous-système d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens.Le sous-système ne surmontera vraisemblablement pas la situation.

TABLE II.5: Cotation des paramètres du critère FC_1

FC_1 : Supervision	$fc_{1,1}$: Contrôle des échanges	1 : Les données et/ou informations produites par le sous-système sont uniquement récupérables à partir d'un accès physique à celui-ci.
		2 : Les échanges sont réalisés à travers un tunnel chiffré (ex : VPN, SSL). Sont seulement réalisables les connexions depuis le premier sous-système vers le sous-système cible.
		3 : Les échanges sont réalisés à travers un tunnel chiffré (ex : VPN, SSL), sans restriction concernant la direction des échanges. Aucun autre échange n'est effectué lors d'une communication.
		4 : Les échanges sont réalisés à travers un tunnel chiffré (ex : VPN, SSL), sans restriction concernant la direction des échanges. Aucun autre échange n'est effectué lors d'une communication. Une connexion sans-fil est possible, mais exclusivement en utilisant un analyseur de trafic (ex : DMZ, Bastion, etc.).
	$fc_{1,2}$: Administration des échanges	1 : La gestion de privilèges est non définit pour le sous-système.
		2 : Le sous-système a accès à des terminaux utilisateurs avec des privilèges administrateur.
		3 : Un privilège de type administrateur est nécessaire au sous-système pour accéder/échanger avec les serveurs métiers.
		4 : Un privilège de type administrateur est nécessaire au sous-système pour manipuler, accéder, ou échanger avec avec des équipements d'infrastructure.

TABLE II.6: Cotation des paramètres du critère FC_2

FC_2 : Maîtrise	$fc_{2,1}$: Homologation	1 : Les règles d'hygiène informatique ne sont pas appliquées, ou appliquées ponctuellement, et non formalisées au sein de l'entreprise ou de la partie prenante. La capacité de réaction en cas d'incident est incertaine.
		2 : Les règles d'hygiène informatique et la réglementation sont prises en compte au sein de l'entreprise, mais pas chez le (ou les) sous-traitant(s) en charge du sous-système concerné. La sécurité numérique est conduite selon un mode réactif (retour d'expérience d'après attaque, caractérisation des mesures à mettre en place pour remédier à l'attaque).
		3 : Une politique globale est appliquée en matière de sécurité numérique. Les règles d'hygiène et la réglementation sont prises en compte au sein de l'entreprise et sont imposées au(x) sous-traitant(s) en charge du sous-système concerné. La sécurité numérique est assurée selon un mode réactif avec une recherche de centralisation et d'anticipation d'un certain nombre de risques.
		4 : Une politique globale est appliquée en matière de sécurité numérique. Les règles d'hygiène et la réglementation sont prises en compte au sein de l'entreprise et le(s) sous-traitant(s) en charge du sous-système concerné. La partie prenante met en œuvre une politique de management du risque. Cette politique est intégrée et se réalise de manière proactive.
	$fc_{2,2}$: Résilience	1 : En prenant compte les contraintes temporelles, aucune alternative n'est acceptable pour remplacer le sous-système impacté. Cela entraîne un arrêt durable de son exploitation et nécessite une intervention de maintenance externe. Une intervention physique est obligatoire. La mission est arrêtée et/ou compromise.
		2 : Le sous-système impacté entraîne un arrêt temporaire de la mission et/ou service. Une reprise de fonctionnement est possible dans un laps de temps long, et après la réalisation d'une procédure particulière par un expert du domaine (réparation, redémarrage, ou remplacement). Cette intervention est possiblement réalisable à partir d'un accès à distance. La pérennité de la mission dépend de l'intervention.
		3 : Une intervention est réalisable, dans une plage de temps acceptable, pour réparer, redémarrer ou remplacer le sous-système impacté. La gestion de cette remédiation nécessite un opérateur qualifié. La mission est légèrement impactée.
		4 : Le sous-système impacté est facilement remplaçable, ou possède une redondance. La duplication de celui-ci ou l'un de ses composants/fonctions critiques permet son rétablissement dans un laps de temps quasi nul. L'intervention nécessaire au rétablissement du service ne nécessite aucune compétence particulière. La mission n'est pas compromise.

II.5.6 Calcul du niveau de menace

Comme illustré dans la Figure II.12, chaque paramètre de chacun des critères E_n et FC_n sont associés par opposition. Les critères FC_n visant à compenser les critères E_n. Prenons par exemple un élément d'un CPS donné, le paramètre $e_{2,2}$ retranscrivant l'impact opérationnel potentiel en cas de défaillance de celui-ci sera compensé par le paramètre $fc_{2,2}$ de résilience opposée. Cette compensation est retranscrite mathématiquement dans le calcul du niveau de menace par un quotient du paramètre $e_{n,1}$ par le paramètre opposé $fc_{n,1}$, ainsi que le quotient du second paramètre $e_{n,2}$ par $fc_{n,2}$.

Cette opération est réalisée pour chacune des deux associations de critères : E_1 et FC_1, E_2 et FC_2. Les quatre quotients obtenus sont alors additionnés pour obtenir le niveau de menace de l'élément considéré. Ce processus est répété pour chaque sous-système physique et numérique du CPS étudié.

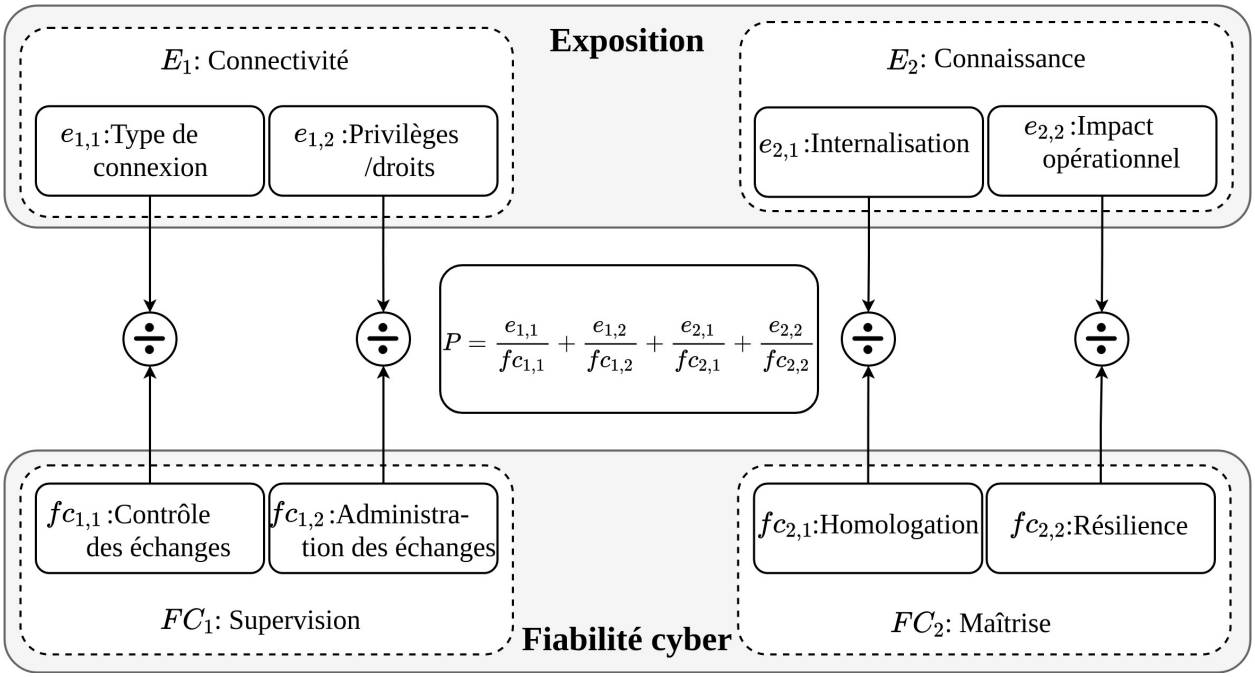


FIGURE II.12: Calcul du niveau de menace de propagation

II.5.7 Intégration dans le graphe

Une fois le processus d'évaluation du niveau de menace réalisé, on obtient ainsi pour chaque sous-système une pondération traduisant quantitativement la capacité de celui-ci à propager une anomalie et à impacter les autres sous-systèmes. La valeur obtenue est intégrée dans le graphe généré antérieurement. Comme illustré dans la Figure II.13, la pondération P_{s_i} obtenue pour chaque sous-système s_i est intégrée dans le graphe comme attribut de pondération de chaque relation à l'origine du nœud du sous-système associé vers un second nœud s_j. En conséquence, nous pouvons écrire l'égalité suivante : $P_{s_i} = P_{s_i \to s_j}$.

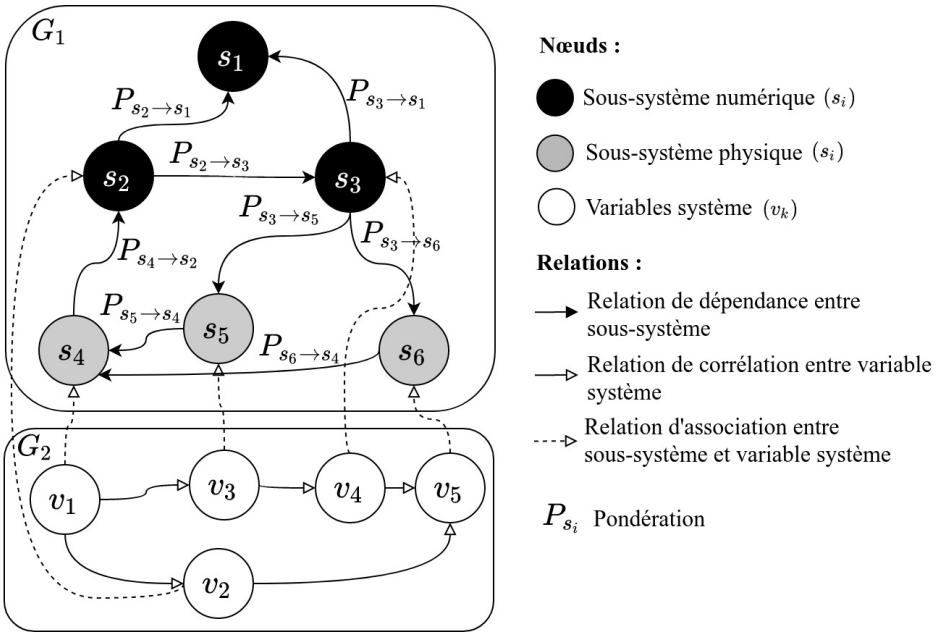


FIGURE II.13: Intégration des niveaux de menaces des sous-systèmes du CPS

La pondération des relations du graphe décuple ses possibilités d'analyse associées de par l'utilisation potentielle de différents algorithmes basés sur cette même pondération. La méthode de pondération présentée est particulièrement adaptée aux CPS, et plus particulièrement aux CPS maritimes. La polyvalence des éléments structurels du modèle de graphe permet cependant d'intégrer n'importe quel type de pondération issue de méthodes différentes.

II.5.8 Processus d'évaluation de la propagation

L'évaluation de la propagation dans le graphe est réalisée à partir de l'analyse quantitative des chemins de propagation extraits du graphe étudié. Afin de garder une certaine cohérence avec le modèle de graphe 3-couches généré, cette évaluation se compose de deux processus distincts, mais complémentaires :

1. Un premier processus basé sur l'étude des relations entre les variables système.
2. Et un deuxième qui fournit les chemins de défaillance des sous-systèmes du CPS.

Ces processus sont tous deux initiés par la détection d'une anomalie à partir des métriques de détection intégrées comme attribut des nœuds de la couche des variables système, comme présenté dans la section II.4.9. Des méthodes de détection efficaces, et adaptées aux spécificités des CPS, sont indispensables à l'évaluation de la propagation d'anomalies. Cela souligne toute l'importance du choix des métriques de détection.

Premier processus d'évaluation

Le premier processus d'évaluation de la propagation d'anomalies est caractérisé sur la troisième couche du modèle de graphe, c'est-à-dire la couche associée aux variables système. Il est exclusivement basé sur les caractéristiques du graphe définies par le modèle de dépendances des variables système proposé. Cette évaluation est initiée lorsqu'une anomalie a été détectée à partir d'une ou plusieurs métriques de détection associées à un nœud de variable système. Un algorithme de *Depth-First Search* fournit alors les différentes variables potentiellement impactées, au travers de différents chemins de propagation. L'un des avantages principaux de ce premier processus est la prédiction d'un éventuel impact d'une anomalie détectée sur une première variable sur une, ou plusieurs, autres variables. Lorsqu'une anomalie a un impact sur une autre variable système à un instant t_2, et si cet impact sur cette même variable a été préalablement identifiée par une précédente évaluation à un instant t_1, une vérification du temps d'impact est définie tel que dans l'équation II.15. Ce premier processus d'évaluation de la propagation est illustré dans la Figure II.14.

$$\Delta t = t_2 - t_1 \tag{II.15}$$

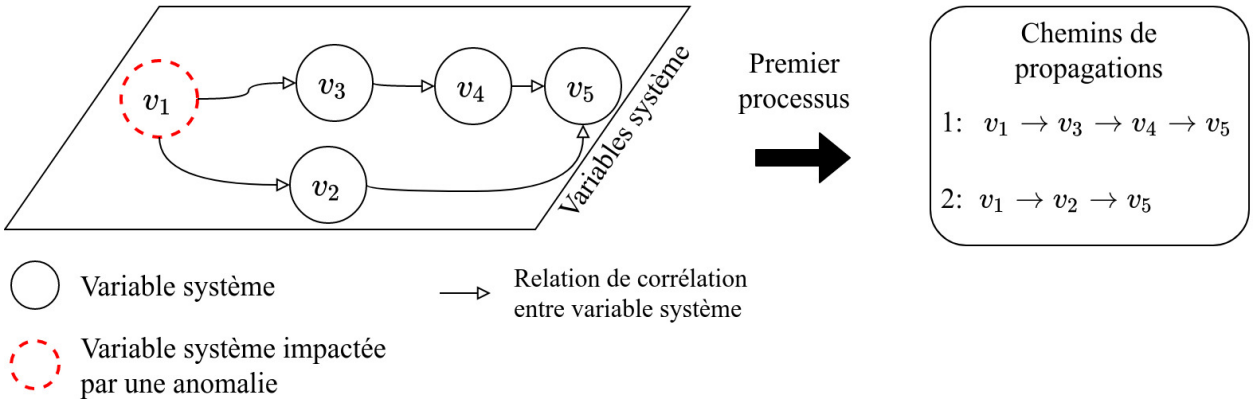


FIGURE II.14: Premier processus d'évaluation de la propagation sur la couche trois

Deuxième processus d'évaluation

Comme illustré dans la Figure II.15, le deuxième processus se caractérise quant à lui sur la première et deuxième couche du modèle de graphe proposé, spécifiant les sous-systèmes et composants physiques ou numériques du CPS étudié. Cette évaluation est aussi initiée lorsqu'une anomalie est détectée partir d'une ou plusieurs métriques de détection associées à un nœud de variable système, v_1 dans ce cas. Le même algorithme utilisé pour le premier processus fournit les chemins de propagations, correspondant aux chemins de défaillance, depuis le nœud du sous-système associé à la variable de nœud où l'anomalie a été initialement détectée, i.e. s_4. Un score d'impact de propagation PIS [8] est aussi calculé pour chaque chemin. Comme défini dans l'équation II.16, ce score est calculé comme la somme des poids P_{s_i} associés aux m nœuds s_i des sous-systèmes parcourus dans chaque chemin. Il représente l'impact possible d'une anomalie sur un chemin particulier du graphe. Ce deuxième processus fournit une analyse qualitative de la propagation de l'anomalie au travers des chemins des sous-systèmes potentiellement impactés. Mais aussi une analyse quantitative grâce au score d'impact de propagation associé à chaque chemin.

$$PIS = \sum_{i=1}^{m} P_{s_i} \; ; \; m > 0 \tag{II.16}$$

8. *Propagation Impact Score*

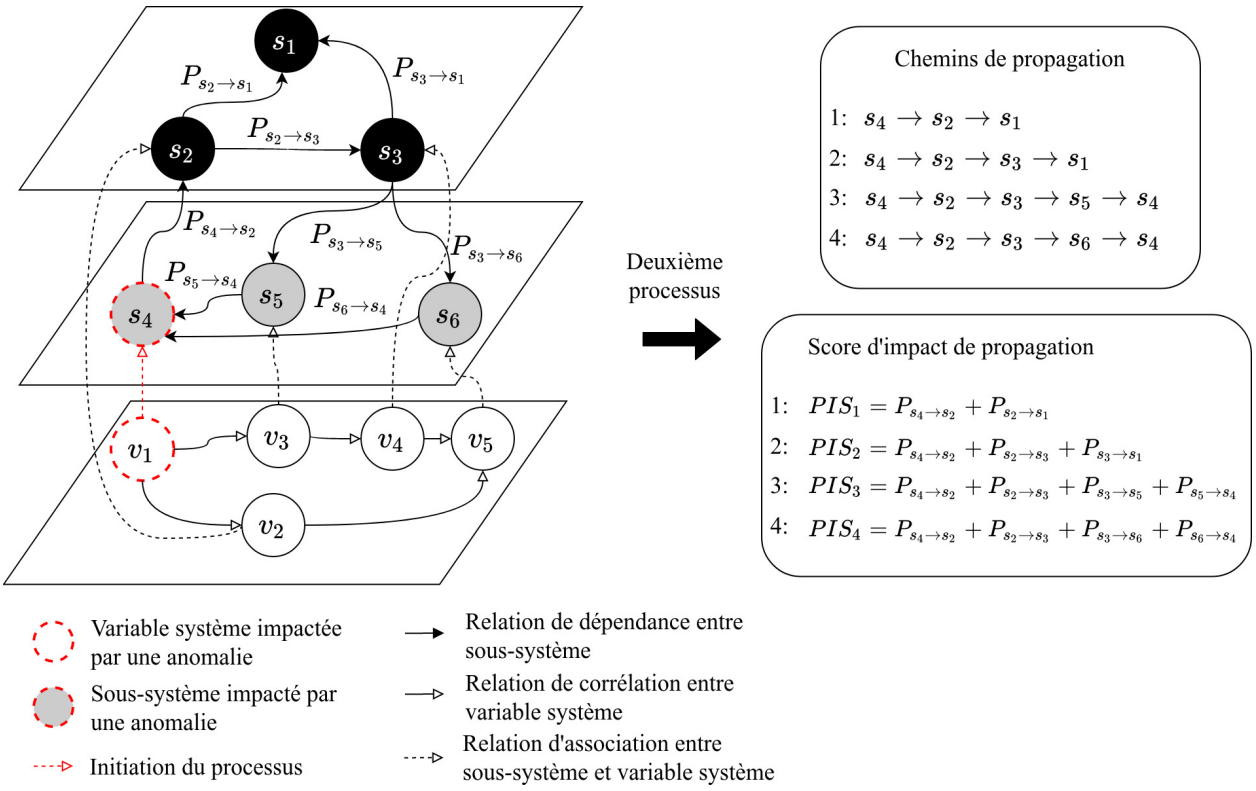


FIGURE II.15: Deuxième processus d'évaluation de la propagation d'anomalie

II.6 Conclusion

Il a été détaillé dans le chapitre I les différentes caractéristiques et contraintes des systèmes maritimes, et plus précisément des CPS maritimes. Parmi les nombreuses problématiques liées à ce type de système, l'évaluation de la propagation est l'une des plus critiques si l'on considère les potentielles conséquences qui en résultent. La revue de littératures dans ce domaine de recherche a permis d'identifier les différentes solutions de modélisation structurelle formulées pour traiter de cette problématique, ainsi que les méthodologies employées pour évaluer quantitativement les chemins de propagations d'anomalie.

À partir de ces travaux existants, nous avons fait le choix de modéliser le CPS maritime sous forme de graphe orienté multicouche, dont les spécificités sont particulièrement adaptées aux caractéristiques de ce type de système. Le modèle de graphe proposé se compose de 3 couches principales : sous-systèmes numériques, sous-systèmes physiques, et variables système. Chaque sous-système du CPS modélisé, ainsi que chacune de ses variables, est alors représenté sous forme de nœuds. Différentes relations associent les nœuds spécificiés. Parmi celles-ci, on dénote les relations de dépendances entre les nœuds associés aux sous-systèmes

physiques ou numériques, les relations de corrélation entre les nœuds de variables système, et les relations d'association entre les nœuds de sous-système et de variable. Cette modélisation offre à la fois une représentation visuelle claire du CPS, et une abstraction mathématique adaptée pour traiter de la problématique d'évaluation de la propagation dans ce type de système.

Une nouvelle méthode d'évaluation du niveau de menaces des éléments du CPS a aussi été formulée pour fournir une pondération au graphe proposé. Le graphe modélisé a ensuite été mis à profit pour évaluer quantitativement les potentiels chemins de propagation d'anomalies dans le système. Deux processus d'évaluation de la propagation ont été définis en adéquation avec les propriétés des couches composant le graphe.

Aussi, toutes les étapes des méthodologies proposées, de modélisation et d'évaluation des chemins de propagations, ont été détaillées. Cela facilite leur implémentation et leur utilisation pour d'autres recherches scientifiques traitant de la problématique des dépendances dans les CPS.

Cette méthodologie s'inspire des travaux scientifiques existants tout en proposant une approche innovante, facilement reproductible et personnalisable. Nous avons ainsi formulé une modélisation fusionnant les éléments du CPS et ses variables d'état pour soumettre une méthode d'évaluation des chemins de propagation la plus complète et représentative possible. Le tout en considérant les contraintes et caractéristiques inhérentes à ce type de système, qui sont d'autant plus exacerbées dans le secteur maritime.

Dans le chapitre suivant, cette méthodologie sera appliquée à deux cas d'étude différents. Chacun d'entre eux se caractérise par une application maritime spécifique et représentative. Cela permettra ainsi d'évaluer la pertinence et la validité des méthodologies proposées.

Chapitre III

Application de la méthode

Sommaire

Ce chapitre présente deux cas d'étude qui servent à valider l'application de l'approche présentée dans le chapitre précédent. Le premier s'appuie sur un prototype de système cyber-physique maritime composé de sous-systèmes réels et simulés. Le deuxième est défini par la simulation d'un réseau d'eau *intelligent* à partir de différents outils *open-source*.

III.1 Introduction

Afin de valider notre modèle, nous avons dans un premier temps recherché des *datasets* publiques composés de données issues de CPS. L'idéal aurait été de confronter notre méthodologie d'évaluation des risques de propagation à des données issues d'un CPS maritime composé de différents systèmes interconnectés regroupant toutes, ou du moins une majeure partie, des fonctions assurées par un navire. Néanmoins ce type de *dataset* demeure complexe à produire de par l'ensemble de systèmes et composants nécessaires, ainsi que par l'hétérogénéité de leurs fonctions et de leurs caractéristiques. De plus, récupérer des données réelles issues de navires demeure impossible en raison de problématiques de confidentialité ou de propriété de la donnée.

L'inexistence d'un jeu de données publiques de ce type a motivé la production de notre propre *dataset* à partir de systèmes réels. La plateforme d'expérimentation mise à notre disposition au sein de la chaire de cyberdéfense des systèmes maritimes a permis de combler ce besoin et de faciliter les simulations informatiques. Nous avons ainsi produit un premier jeu de données à partir de systèmes assurant une fonction critique du navire : sa propulsion. L'objectif était d'y associer progressivement d'autres systèmes interconnectés en charge d'autres fonctions essentielles à bord. Ce qui aurait permis au final d'obtenir un *dataset* composé de données au plus proches de ce qu'on pourrait obtenir à partir d'un navire réel.

Cet objectif a malheureusement été ralenti par la crise sanitaire, limitant l'accès phy-

sique à la plateforme pendant plusieurs mois au cours de la deuxième et troisième année de thèse. Nous avons ainsi été dans l'obligation de reprendre nos recherches sur les *datasets* publics existant afin de confronter notre méthode à un système plus complexe et varié que celui étudié pour le premier jeu de données issues de la plateforme. Là encore, nous avons recentré notre recherche sur un *dataset* issu de systèmes interconnectés, assimilables à une ou plusieurs fonctions inhérentes du navire. La principale problématique concernant les jeux de données étudiés fut le manque d'explicitation des dépendances entre les systèmes à l'origine de la production de données composant les *datasets*. Nous avons finalement trouvé un *dataset* créé à partir de la simulation d'un réseau de distribution d'eau *intelligent*, assimilable à celui que l'on retrouve à bord d'un navire. Ce jeu de données étant généré à partir d'un outil de simulation, nous avons fait le choix d'apprendre à l'utiliser afin de pleinement le maîtriser pour en produire nos propres *datasets*.

Le modèle et la méthode décrits précédemment ont ainsi été confrontés à deux cas d'études. Le premier est basé sur le *dataset* créé à partir d'une plateforme maritime, et le deuxième sur les jeux de données produits grâce à l'outil de simulation. Ces deux cas d'étude sont décrits et étudiés en détail dans les sections suivantes. Par la suite, deux outils de génération et d'interaction avec les graphes sont présentés et comparés afin de choisir le plus approprié pour ces travaux.

En complément, un outil informatique a spécifiquement été développé pour de faciliter l'implémentation et l'interaction avec le modèle de graphe proposé pour traiter de la problématique de l'évaluation de la propagation. Il facilite ainsi la génération du graphe et l'extraction de diverses métriques à partir d'un processus d'interaction que nous présentons dans la section suivante.

III.2 Premier cas d'étude : le *Naval Cyber Range*

Cette section décrit l'expérimentation réalisée sur une plateforme présente au sein de l'École Navale, qui simule le fonctionnement d'un navire. Nous y présentons les caractéristiques et fonctionnalités de la plateforme, les différents scénarios étudiés, l'implémentation du modèle de graphe 3-couches proposé, et enfin les résultats obtenus quant à l'évaluation de la propagation d'anomalie en son sein.

III.2.1 Description et architecture du *Naval Cyber Range*

La plateforme présentée a été développée au sein de l'École Navale. Elle est partie prenante du projet européen H2020 *Foresight*[1] qui vise à rassembler des plateformes d'expérimentation pour améliorer la formation du personnel confronté à des problématiques de cybersécurité industrielle. Ces plateformes d'expérimentation, aussi appelées *cyber-range*, apportent des solutions de simulation pour couvrir des besoins d'analyse et d'étude en matière de cybersécurité de domaines à enjeux critiques. Ainsi, l'écosystème de *cyber-range* proposé à partir de ce projet offre des possibilités de simulation dans le domaine du transport aérien, de la distribution d'électricité et du naval.

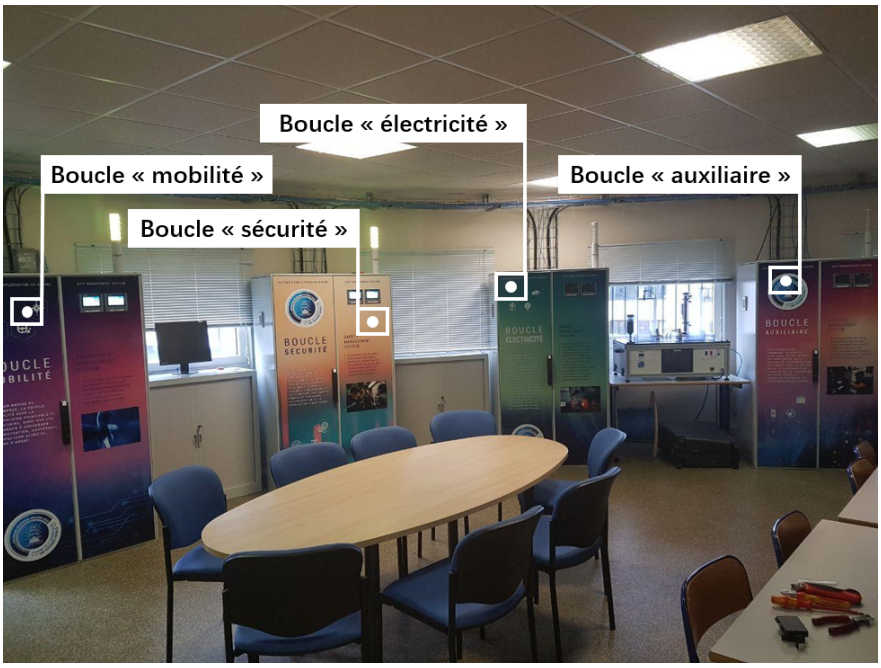


FIGURE III.1: Aperçu du *Naval Cyber Range* et de ses quatre boucles

L'École Navale a acquis différents équipements qui ont permis d'étendre ses capacités, en termes de représentation et simulation du fonctionnement d'un navire générique civil. L'ensemble de ces équipements est regroupé au sein d'une plateforme d'expérimentation. Le *Naval Cyber Range* est constitué de plusieurs sous-systèmes réels ou simulés qui assurent différentes fonctionnalités du navire pour fournir un outil d'expérimentation le plus réaliste possible. Cette plateforme n'est pas seulement destinée à la formation, c'est aussi un atout majeur pour la recherche scientifique dans le domaine de la cybersécurité maritime. De par les difficultés à obtenir des *datasets* maritimes composés de donnés réalistes, en quantité

1. Foresight. Consulté le 02 juin 2021.`https://foresight-h2020.eu/`

suffisante, et non protégées, cet aspect de la plateforme d'expérimentation est d'autant plus important.

Une modélisation de l'architecture technique de ce prototype de navire générique a été proposée par Olivier Jacq [Jac21b] dans le cadre de ses travaux de thèse. On aperçoit ainsi dans la Figure III.3 que l'architecture du *cyber range* est composée, tout comme un navire réel, de différents systèmes *IT* et *OT* (défini précisément en section I.2.1) nécessaires à son bon fonctionnement. Dans le cadre de nos travaux, nous nous intéressons exclusivement aux systèmes *OT* de la plateforme, catégorisés en 3 types principaux : systèmes de passerelle, de contrôle industriel et de communication.

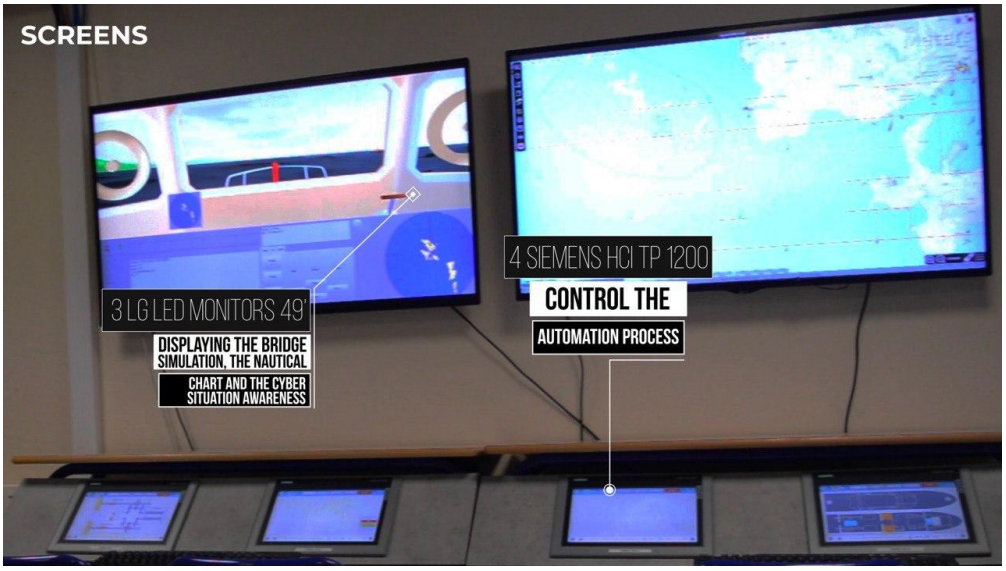
Les **sous-systèmes dits de « passerelle »** utilisés au sein de la plateforme sont similaires à ceux présents dans une passerelle de navire de taille moyenne. On y distingue des capteurs GNSS[2], AIS, ainsi que les différentes antennes associées. Ces éléments sont reliés à des connexions aux standards NMEA 0183 et 2000. Divers écrans sont également utilisés pour l'affichage du système de cartes électroniques et la visualisation du simulateur de navigation 3D. Ces sous-systèmes sont présentés dans la Figure III.2.

À bord, différents systèmes de plateforme assurent des tâches de productions industrielles essentielles au bon fonctionnement du navire et à la garantie de conditions de vie optimales pour l'équipage et les potentiels 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 *cyber range* sont organisés en quatre boucles réseaux selon leurs rôles fonctionnels au sein du navire simulé. Comme présenté dans la Figure III.1, on distingue les boucles « mobilité », « sécurité », « électricité », et « auxiliaire ». Chacune de ces boucles réseaux assurant diverses fonctionnalités plus ou moins critiques du navire :

- La boucle « mobilité » contrôle la propulsion principale et auxiliaire, ainsi que les appareils de manoeuvre utilisés pour : la stabilisation, le gouvernail, le propulseur azimutal, ou encore la ligne d'arbre.
- La boucle « sécurité » assure la détection et protection contre les incendies et voies d'eau. Pour cela elle gère l'ouverture et la fermeture des vannes, des portes, ainsi que la mise en marche de la ventilation et de la production d'eau froide.
- La boucle « électricité » produit et fournit de l'énergie à haute tension à bord. Quelles que soient les sources de production (turbines, groupes électrogènes, batteries, etc.), l'électricité est convertie et distribuée dans tout le navire à partir de

2. Géolocalisation et Navigation par un Système de Satellites

(a) De gauche à droite : récepteur GPS, connecteur NMEA 0183 et bus NMEA 2000, et récepteur AIS



(b) Écrans de visualisation

FIGURE III.2: Sous-systèmes « passerelle » du navire simulé

tableaux de distribution.

— La boucle « auxiliaire » est quant à elle en charge des commandes de toutes les servitudes de bord, i.e. les réseaux et systèmes essentiels au fonctionnement du bateau et à sa vie à bord. On y retrouve par exemple, la gestion du carburant, de l'air, ou encore de l'huile. Cette boucle est aussi responsable de la gestion de ressources vitales pour les personnes embarquées, telles que la production et distribution de

l'eau, le traitement des eaux usées, ou encore la réfrigération des vivres.

Pour assurer les fonctions qui leur sont attribuées, chacune de ces boucles est composée de divers capteurs et actionneurs réels ou simulés. La simulation de ces sous-systèmes présente de nombreux avantages dans le cadre des expérimentations réalisées au sein du *cyber range*. Premièrement cela facilite grandement 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 présente une moindre complexité tant au niveau du câblage que de son utilisation. Deuxièmement, l'utilisation de sous-système simulé offre la possibilité de générer des changements d'état dans des environnements « statiques » où le processus physique, lié au sous-système concerné, n'évoluerait pas dans la réalité. Cela permet aussi de fournir des capacités de répétabilités accrues à la plateforme d'expérimentation. Cette caractéristique est primordiale par rapport aux utilisations de la plateforme, tant pour la formation que pour la recherche scientifique. Pour finir, l'emploi d'un sous-système simulé permet de réduire les coûts d'acquisition là où certains sous-systèmes coûtent plusieurs centaines à plusieurs milliers d'euros.

L'ensemble de ces capteurs et actionneurs, réels ou simulés, est relié à un ou plusieurs automates programmables industriels. Ils sont chargés de fournir des ordres de commandes aux actionneurs, proportionnellement aux valeurs des mesures de capteurs reçues, à partir de programmes embarqués.

Le troisième type de sous-systèmes OT employés au sein de la plateforme regroupe les **sous-systèmes de « communication »**. Ils sont associés à la réception et l'envoi d'informations depuis un lien par satellite vers l'extérieur du navire. Cette liaison est définie par de fortes contraintes liées à ses caractéristiques et son utilisation. Parmi ces contraintes on citera notamment une bande passante limitée, des délais de connexion importants et des pertes temporaires de liaison.

III.2.2 Choix de l'étude de la boucle « mobilité »

Dans le cadre de ces travaux de thèse, nous nous sommes particulièrement intéressés à la boucle « mobilité » du *cyber range*. Celle-ci assure une fonction essentielle du navire, si ce n'est vital : se déplacer sur l'eau. Parmi l'ensemble des systèmes employés pour assurer la motricité du navire, on distingue principalement deux catégories : les systèmes de propulsion pour les déplacements sur, ou dans l'eau selon le type de bâtiment, et les systèmes utilisés pour les manoeuvres spécifiques. De nos jours, la propulsion principale et auxiliaire d'un

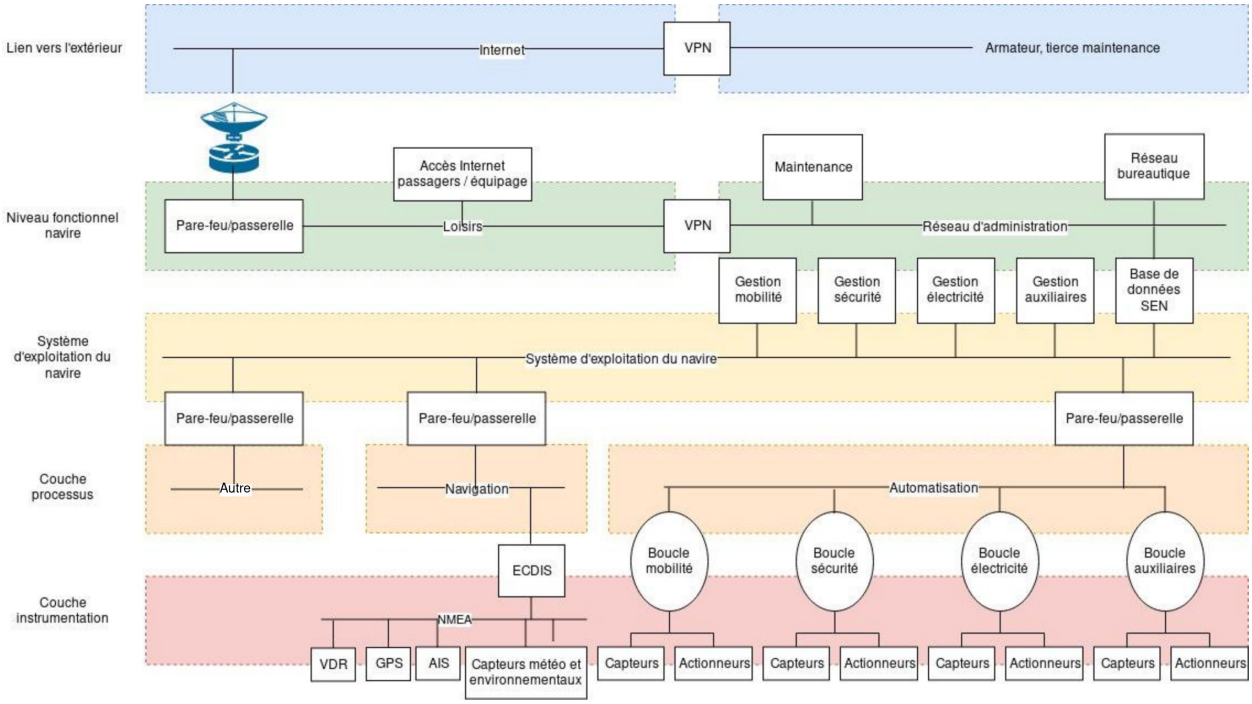


FIGURE III.3: Modélisation technique du prototype de navire générique civil [Jac21b]

navire ne se limite pas à la réalisation de son bon déplacement. Ces systèmes doivent aussi fournir un niveau de sécurité et résilience suffisant, tout en garantissant une rentabilité optimale. De nombreux types de systèmes de propulsion existent [3], définis par différentes caractéristiques qui doivent satisfaire les exigences et besoins associés au cas d'utilisation du navire.

D'autres systèmes liés à la manoeuvre du navire sont utilisés dans des conditions précises pour répondre à des besoins opérationnels spécifiques et temporaires, mais qui n'en sont pas moins critiques. Un navire peut être par exemple obligé de manoeuvrer à l'arrivée ou au départ d'un port, lors de la traversée d'un canal, ou encore dans une zone de trafic dense. La majorité des collisions et échouements ont lieu durant les opérations de manoeuvre. Ces phases de la mission sont alors considérées, tant du point de vue du navire que du marin, comme les plus critiques [4].

L'apparition d'une anomalie sur l'un de ces systèmes liés à la mobilité du navire peut en-

3. Different Types of Marine Propulsion Systems Used in the Shipping World. Marine Insight. Consulté le 02 juin 2021. https://www.marineinsight.com/main-engine/different-types-of-marine-propulsion-systems-used-in-the-shipping-world/

4. A Detailed Explanation of How a Ship is Manoeuvered to a Port. Marine Insight. Consulté le 02 juin 2021. https://www.marineinsight.com/guidelines/a-detailed-explanation-of-how-a-ship-is-manoeuvered-to-a-port/

gendrer des conséquences colossales pour le navire lui-même, mais aussi potentiellement pour les bâtiments et installations portuaires à proximité. Récemment, le méga porte-conteneurs *MV Ever Given* s'est échoué à l'intérieur du canal de Suez tout en bloquant le trafic dans les deux sens [5]. Cet accident serait dû à une erreur humaine, mais on peut facilement imaginer qu'une cyberattaque, ou un dysfonctionnement visant un des systèmes de mobilité dans des conditions opérationnelles spécifiques auraient pu avoir les mêmes effets. Concernant les sous-marins, une anomalie au niveau du système de propulsion serait par exemple de faire caviter l'hélice et provoquer l'émission d'indiscrétions acoustiques. Sa position pourrait ainsi être découverte, ce qui augmenterait considérablement sa vulnérabilité face à l'ennemi, et le placerait dans une situation défavorable pour l'emploi de ses systèmes d'armes.

III.2.3 Prototype d'expérimentation d'un CPS maritime

Comme énoncé précédemment, l'approche proposée a été confrontée à un prototype de CPS maritime simplifié, composé d'un système de gestion de la propulsion de la boucle « mobilité », connecté à un système de gestion de l'énergie et du carburant, appartenant respectivement à la boucle « électricité » et la boucle « auxiliaire ». Ce système cyber-physique, représenté dans la Figure III.4, est composé de sept sous-systèmes dont cinq physiques : un réservoir de carburant T1 associé à, un réservoir d'huile T2, une vanne V, un moteur M, et une hélice P. Ces sous-systèmes sont contrôlés et surveillés par un sous-système numérique : un automate programmable industriel de la marque Siemens. Un autre système numérique est utilisé au sein du CPS. Il s'agit d'un module d'entrée/sortie (module E/S), noté I, placé entre l'automate et les différents actionneurs et capteurs. Il est en charge de la transmission des commandes de contrôle du *PLC* vers les actionneurs et les valeurs mesurées par les capteurs vers l'automate.

Le moteur fournit, par l'intermédiaire de l'arbre de transmission, la puissance nécessaire à la rotation de l'hélice, en accord avec la commande de contrôle de vitesse de rotation h_r reçue. Ce transfert d'énergie génère une augmentation de la température t_m du moteur. Pour la compenser, l'ouverture o_v de la vanne est proportionnellement contrôlée pour réguler le refroidissement du moteur et maintenir le système à un niveau de performance optimal. L'augmentation de la vitesse de rotation de l'hélice entraîne également une diminution du

5. Mega Container Ship Blocks Suez Canal After Grounding Sideways, Blocks Traffic From Both Direction. Marine Insight. Consulté le 02 juin 2021. https://www.marineinsight.com/shipping-news/mega-container-ship-blocks-suez-canal-after-grounding-sideways-blocks-traffic-from-both-direction/

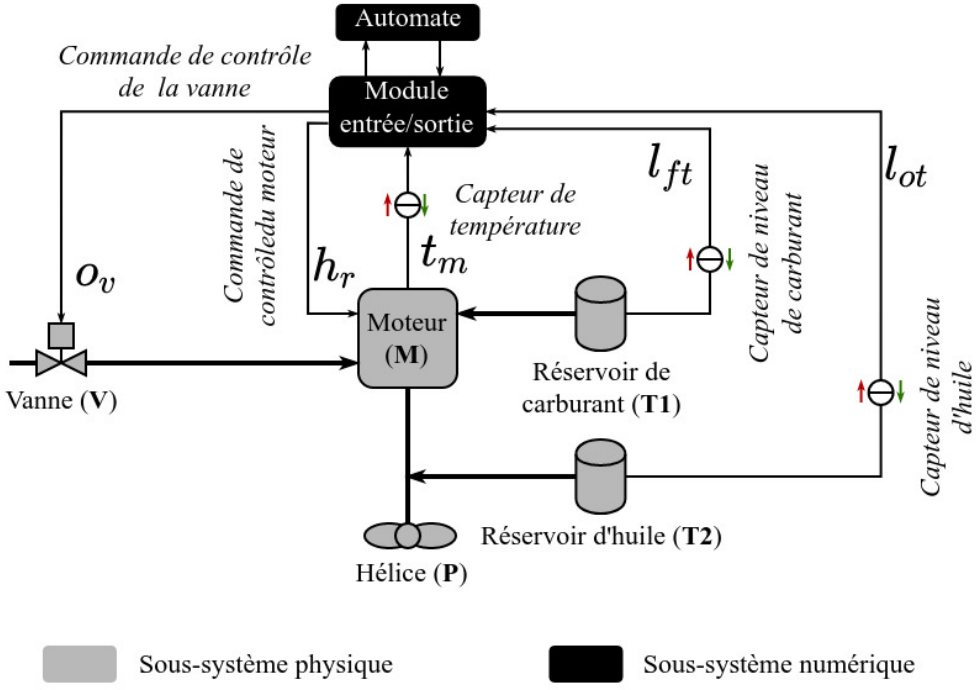


FIGURE III.4: Système simplifié de gestion de la propulsion connecté à un système de gestion de l'énergie et du carburant

niveau l_{ft} de réservoir de carburant, utilisé pour la combustion, et du niveau l_{ot} de réservoir d'huile, utilisée pour la lubrification de l'arbre de transmission.

Pour générer toutes les données requises, certains sous-systèmes du prototype créé ont été simulés à partir de cartes à microcontrôleur de la marque Arduino. Nous les avons programmées pour générer ou recevoir des signaux analogiques et ainsi simuler le comportement de différents capteurs et actionneurs. Les cartes Arduino sont directement reliées à l'automate au travers du module E/S pour recevoir ses commandes de contrôle ou lui transmettre les valeurs mesurées des capteurs simulés. Chaque signal analogique, associé à chaque variable système simulée, est généré à partir de fonctions composées de diverses variables système (Table III.1). Ces fonctions retranscrivent mathématiquement les différentes dépendances structurelles et opérationnelles des variables du système de propulsion étudié.

TABLE III.1: Variables système associées au prototype de système de propulsion

	Variables système				
	Commande de contrôle du PLC		**Variables de capteurs simulés**		
	o_v	h_r	t_m	l_{ft}	l_{ot}
Sous-système	V	P	M	T1	T2
Corrélation structurelle [1]	n/a	n/a	$t_m(t) = 23 - 0.25 \times o_v(t)$ $+0.62 \times h_r(t)$	$l_{ft}(t) = l_{ft}(t-1)$ $-0.001 \times h_r(t)$	$l_{ft}(t) = l_{ft}(t-1)$ $-0.0005 \times h_r(t)$
Corrélation conditionnelle [1]	$o_v(t) = 0$ si $h_r(t) = 0$	n/a	n/a	$l_{ft}(t) = l_{ft}(t-1)$ si $h_r(t) = 0$	$l_{ot}(t) = l_{ot}(t-1)$ si $h_r(t) = 0$
Plage de valeur nominale	$0 \rightarrow 100$ (%)	$0 \rightarrow 100$ (%)	$23 \rightarrow 83$ (°C)	$2 \rightarrow 100$ (%)	$2 \rightarrow 100$ (%)

[1] : Tel que défini dans la section II.4.5

III.2.4 Génération du graphe

Un processus basé sur l'exploitation du driver Neo4j (section III.4) permet de générer le graphe 3-couches associé au prototype de CPS maritime. Il est ainsi défini par deux sous-graphes des sous-systèmes (G_1) et variables (G_2) du CPS. La description du graphe généré et de ses composants est réalisée en trois parties :

1. La description du sous-graphe des sous-systèmes G_1,
2. celle du sous-graphe des variables G_2
3. et le lien entre les deux.

Sous-graphe des sous-systèmes du CPS (G_1)

Le premier sous-graphe G_1 est composé des ensembles de nœuds $S_{physique}$ et $S_{numerique}$, modélisant respectivement les sous-systèmes physiques et numériques (Équations III.1 et III.2).

$$S_{physique} = \{M, V, P, T1, T2\} \tag{III.1}$$

$$S_{numerique} = \{PLC, I\} \tag{III.2}$$

Ces nœuds sont reliés entre eux par l'intermédiaire de $L = 11$ relations de dépendances définies dans un ensemble R (Équation III.3). Cet ensemble est défini à partir des caractéristiques du prototype de CPS maritime telles que présentées précédemment.

$$\begin{aligned} R = \{&PLC \rightarrow I, I \rightarrow PLC, I \rightarrow V, I \rightarrow M, M \rightarrow I, T1 \rightarrow I, \\ &T2 \rightarrow I, V \rightarrow M, M \rightarrow P, M \rightarrow T1, M \rightarrow T2\} \end{aligned} \tag{III.3}$$

L'ensemble de ces relations de dépendances ont été définies à partir de la connaissance de l'architecture du CPS étudié.

Sous-graphe des variables systèmes du CPS (G_2)

Le sous-graphe G_2 est quant à lui composé par les variables systèmes définies sous forme d'un ensemble V de $K = 5$ nœuds v_k appartenant à la troisième couche du modèle (Éq. III.4). Ces nœuds modélisent l'ensemble des variables, simulées ou non, associées aux sous-systèmes du CPS.

$$V = \{o_v, h_r, t_m, l_{ft}, l_{ot}\} \tag{III.4}$$

Ces nœuds de variables système sont reliés entre eux à partir d'un ensemble C de $L = 5$ relations de corrélation (Éq. III.5), structurelles ou conditionnelles. Ces relations sont présentées dans la Table III.1.

$$C = \{o_v \rightarrow t_m, h_r \rightarrow t_m, h_r \rightarrow o_v, h_r \rightarrow l_{ft}, h_r \rightarrow l_{ot}\} \tag{III.5}$$

Liens entre les deux sous-graphes

Les sous-graphes G_1 et G_2 sont reliés entre eux par un ensemble A de $U = 5$ relations d'association de nœud de variables systèmes v_k aux nœuds de sous-système s_i (Équation III.6).

$$A = \{o_v \rightarrow V, h_r \rightarrow P, t_m \rightarrow M, l_{ft} \rightarrow T1, l_{ot} \rightarrow T2\} \tag{III.6}$$

Le graphe obtenu, composé des différents nœuds et relations présentés ci-dessus, est schématisé dans la Figure III.5.

III.2.5 Scénarios d'expérimentation

L'objectif principal des scénarios d'expérimentation mis en place à partir du prototype de CPS maritime est de perturber le système de propulsion. Pour cela, quatre scénarios d'expérimentation ont été réalisés, chacun étant caractérisé par une cyberattaque spécifique introduite à partir de la couche numérique du prototype de CPS maritime. Chacune de ces attaques impacte un des critères de sécurité (confidentialité, intégrité, et disponibilité). En

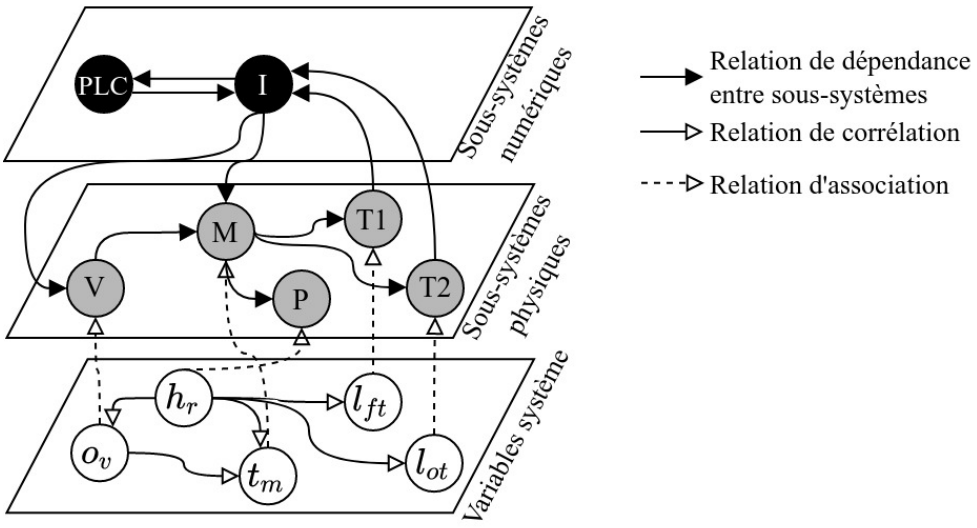


FIGURE III.5: Graphe généré à partir du système étudié

plus de ces scénarios d'attaque, un scénario en fonctionnement nominal a été effectué. Les caractéristiques de chacun des scénarios sont regroupées dans la Table III.2. Chaque scénario joué génère un ensemble de données stocké dans un fichier log au format CSV.

TABLE III.2: Scénarios d'expérimentation sur le prototype de CPS maritime

	Description de l'attaque			
Scénario	**Type**	**Variable système visée**	**Couche impactée**	**Critère de sécurité impactée**
1	Scan de port et DoS	n/a	Numérique	Confidentialité et Disponibilité
2	*PLC stop*	n/a	Numérique	Intégrité
3	*MiTM*[1]	o_v	Liaison numérique-physique	Intégrité
4	*MiTM*	h_r	Liaison numérique-physique	Intégrité

[1] : *Man in the middle*

Le **premier scénario** est défini par une attaque caractérisée par deux étapes de réalisation : un balayage de port puis une attaque par déni de service. Dans un premier temps un ordinateur relié à la couche **numérique** du CPS réalise un balayage de ports afin de trouver des ports libres. La majorité des attaques impliquant un réseau de communication

sont initiées par une étape de reconnaissance. L'une des méthodes les plus démocratisées est l'analyse des 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 recherches scientifiques ont proposé des méthodes de détection basées sur diverses approches telles que l'analyse des statistiques du trafic réseau [SCYY16], ou encore l'utilisation de réseaux neuronaux pour classifier les échanges dans le réseau [HK20]. Dans notre cas l'identification des ports ouverts est réalisée à partir l'outil *open source* Nmap. La **confidentialité** des paramètres du système ainsi impactée, les ports ouverts trouvés sont autant de points d'entrée potentiels pour effectuer des attaques supplémentaires sur le CPS. La seconde partie du scénario consiste à réaliser une attaque par déni de service pour inonder de requêtes l'automate 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 hping, un outil permettant de générer des paquets réseau de divers protocoles. Cette attaque devrait rendre indisponible l'automate. Toute commande de contrôle envoyée depuis le SCADA vers l'automate ne devrait avoir aucun effet sur les actionneurs. Et inversement, tous les changements des valeurs mesurées par les capteurs simulés ne devraient pas pouvoir être observables au niveau du SCADA.

Dans le **deuxième scénario**, une cyberattaque altère **l'intégrité** 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 utilisé, celui peut alors exploiter une vulnérabilité associée pour injecter un *payload*[6] et générer l'arrêt de l'automate. Cette approximation sur les connaissances de l'attaquant par rapport à l'automate est réaliste puisque les signatures réseau de ces dispositifs sont facilement reconnaissables dès lors que l'on analyse les échanges dans le réseau concerné. De plus, l'objectif de ces expérimentations est d'étudier les conséquences d'une telle attaque sur le système, et non pas d'étudier la faisabilité de celle-ci. Pour choisir et configurer la charge utile visant à générer la commande d'arrêt de l'automate l'attaquant utilise un module spécifique de Metasploit, une infrastructure logicielle dédiée à la pénétration des systèmes informatiques. Le module utilisé permet de facilement générer la commande *PLC stop* adaptée pour arrêter l'automate et le rendre indisponible. En conséquence, les actionneurs ne devraient plus recevoir de commandes de contrôles transmises par le PLC. De même, les valeurs mesurées par

6. Charge utile

les capteurs devraient être transmises à l'automate mais non lues par celui-ci, et donc non prises en compte dans l'architecture de contrôle. Par la suite, l'automate est remis en service par une commande *PLC start*.

Pour le **troisième et quatrième scénario**, une attaque *Man-in-The-Middle* (MiTM) est réalisée. Ce type de *deception attack*[7] vise à altérer **l'intégrité** des informations transitant dans le système. Dans ce cas de figure l'attaquant s'insère dans une liaison d'échange d'informations entre deux dispositifs pour écouter ces échanges et les reproduire frauduleusement en y injectant de fausses données ou de fausses commandes de contrôle. Une méthode de détection de ce type de cyberattaque a été proposée pour les CPS industriels [EKT16]. Elle se base sur la définition d'un modèle de comportement normal du système à partir du machine learning pour caractériser un certain nombre d'*outliers*[8] à comparer avec les valeurs expérimentales. Dans le cadre de ce scénario les attaques MiTM sont directement générées dans le code de programmation des cartes Arduino simulant différents capteurs et actionneurs. A un instant t, les commandes de contrôle envoyées par l'automate seront frauduleusement modifiées dans le programme. Pour le scénario 3, les commandes envoyées par l'automate pour contrôler l'ouverture o_v de la vanne seront modifiées à un instant t dans le programme. Pour le scénario 4, c'est la commande de vitesse de rotation h_r de l'hélice qui est visée par cette attaque.

III.2.6 Détection d'anomalies

La détection d'anomalies dans le graphe est réalisée à partir de différentes métriques d'analyse de la qualité. Cela est caractérisé par 2 étapes :

1. Définition des métriques de mesure de la qualité
2. Intégration au sein du graphe

Ces étapes sont présentées ci-après et nous permettent de définir tous les éléments nécessaires pour les appliquer à notre cas d'étude.

Définition des métriques de mesure de la qualité

Différents sous-systèmes du prototype de CPS maritime sont associés à divers flux de données de commandes de contrôle des actionneurs ou de valeurs mesurées par les capteurs. Pour détecter des anomalies au sein de ces flux de données, diverses mesures d'analyse

7. Attaque par « tromperie »
8. Valeurs aberrantes

de la qualité ont été choisies dans l'ensemble des métriques proposées dans les travaux de Pedro Merino Laso *et al.* [LBP16]. Ce choix de métrique a été fait par les caractéristiques intrinsèques des données enregistrées, ainsi que par leurs conditions d'enregistrement. Ainsi, seul un ensemble d'imperfections et de dimensions peut être mesuré. L'analyse de ces données se fait *à posteriori*, grâce aux fichiers log générés par chacun des scénarios.

Pour le cas d'étude du prototype maritime, les mêmes métriques d'analyse de la qualité des données et des informations ont été choisies pour chaque sous-système associé aux flux de données correspondant à chaque variable système. Ces mesures de la qualité sont regroupées en dimensions et définies sous forme vectorielle telles que présentées dans la section I.3.4. Elles sont par la suite directement intégrées au sein du graphe 3-couches généré (section II.4.9). Pour chaque métrique choisie, une description complète ainsi qu'un exemple de mesure à un instant t est fourni. Nous avons dans un premier temps évalué la qualité des données enregistrées à partir d'une seule métrique :

— Une donnée est considérée comme incomplète (i_{inc}) quand un attribut pertinent ou une valeur manque. Une valeur manquante peut être due à une valeur qui n'existe pas ou qui n'a pas été enregistrée. La métrique i_{inc} associée à cette mesure de la qualité prend alors la valeur « $true$ ». Inversement, lorsque que la donnée est complète i_{inc} est définie par la valeur « $false$ ».

Un exemple d'évaluation de la qualité des données pour un sous-système du prototype de CPS maritime associé à un flux de données est présenté ainsi :

$$\vec{DQV} = \{i_{inc} = false\} \tag{III.7}$$

Pour l'évaluation de la qualité des informations, 2 dimensions, dont une contextuelle et une extrinsèque, ont été identifiées. Elles sont définies comme suit :

— Dimension contextuelle : les informations erronées correspondent aux valeurs impossibles du sous-système. Lorsqu'elles sont identifiées, la métrique associée passe de la valeur « $false$ » à la valeur « $true$ ».

— Dimension extrinsèque : la cohérence de l'information est mesurée comme la différence entre la valeur théorique attendue et la valeur mesurée et enregistrée. La valeur théorique peut être définie de deux manières différentes selon si la variable système à laquelle elle est associée est une commande de contrôle ou une mesure de capteur simulé. Si c'est une commande de contrôle, la valeur théorique est définie comme la valeur fixée par le SCADA. Si c'est une mesure de capteur simulé, la valeur théorique est calculée à partir des équations présentées dans la

Table III.1.

L'évaluation de la qualité des informations est alors définie sous forme vectorielle telle que :

$$\vec{IQV} = \left\{ \begin{array}{ll} \text{contextuelles} & \{cd_{err} = false\}, \\ \text{extrinsèques} & \{ed_{coh} = 2\} \end{array} \right\} \quad \text{(III.8)}$$

Intégration des métriques au sein du graphe

Une fois les évaluations de la qualité définies pour chaque variable système du prototype du CPS maritime, celles-ci sont intégrées au sein de la troisième couche du graphe généré. Cette intégration est réalisée par l'association des vecteurs d'évaluation $\overrightarrow{QE}_{v_k}$ de la qualité aux attributs des nœuds variables système v_k concernés (section II.4.9). La Figure III.6 schématise cette intégration pour le cas d'étude du prototype de CPS maritime.

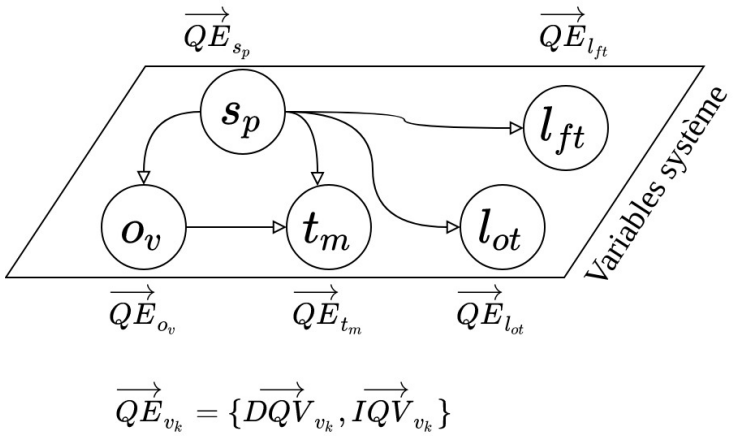


FIGURE III.6: Intégration de l'évaluation de la qualité dans la troisième couche du graphe associé au prototype de CPS maritime

III.2.7 Analyse des métriques du graphe

Une fois que le graphe 3-couches a été généré, nous avons tiré profit de cette modélisation pour étudier le niveau de centralité de proximité de chaque nœud. Cela fournit un indicateur représentatif quant à l'appétence d'un nœud donné à impacter les autres. Tel que présenté dans la Table III.3, le nœud du module E/S directement relié à l'automate possède le score de centralité le plus important pour les sous-systèmes numériques. Ce qui souligne l'importance de la fonction de contrôle réalisée par l'automate dans le système.

Concernant les sous-systèmes physiques, le nœud associé au moteur est défini par le score le plus élevé. Là aussi cela met en évidence le rôle opérationnel majeur de ce sous-système dans la réalisation de la mission associée au CPS : assurer la propulsion. Pour les variables système, c'est la commande de vitesse de rotation de l'hélice (h_r) et la température du moteur (t_m) qui obtiennent les scores les plus élevés. Ce qui accentue d'autant plus l'importance du moteur au niveau de la globalité du système.

Une des hypothèses pour vérifier la pertinence et la représentativité de ces scores sera de comparer le niveau d'impact de l'anomalie sur le système global en fonction du sous-système initialement visé par celle-ci.

TABLE III.3: *Closeness centrality* des nœuds du graphe

	Sous-systèmes numériques		Sous-systèmes physiques					Variables système				
Nœud	E/S	PLC	M	P	T1	T2	V	h_r	t_m	l_{ot}	l_{ft}	o_v
Score de centralité	**0.611**	0.392	**0.688**	0.524	0.524	0.524	0.524	**0.550**	**0.550**	0.478	0.478	0.500

III.2.8 Résultats

Une fois les métriques d'analyse de la qualité définies et intégrées au sein du graphe, les scénarios d'expérimentations définis dans la section III.2.5 ont été réalisés pour vérifier la cohérence et la pertinence de l'approche proposée. Les flux de données et d'informations correspondants ont été enregistrés en deux points différents au sein du prototype d'expérimentation : -un premier point d'enregistrement des données réseaux effectué par un ordinateur externe relié au réseau informatique du prototype de CPS maritime, -un deuxième point d'enregistrement des variables systèmes (commandes de contrôle et données de capteurs) réalisé par un nano ordinateur de type *Raspberry Pi* relié aux cartes *Arduino* réceptionnant les commandes de contrôles de l'automate et simulant les divers capteurs et actionneurs.

Le processus de détection d'anomalie est initié par le commencement du processus d'évaluation de la qualité lorsque les capteurs mesurent des **données**, sous la forme d'une séquence binaire incompréhensible. Par la suite, diverses **informations** sont définies lorsque les données sont décodées par le protocole correspondant et que le contexte associé donne

un sens aux valeurs. Les résultats obtenus pour les 4 scénarios d'expérimentation, plus un scénario en fonctionnement nominal, sont résumés dans la Table III.4. Chaque ligne correspond à l'évaluation de la qualité pour un scénario donné. Celle-ci est réalisée selon les vecteurs de mesures de qualité $D\vec{Q}V$ et $I\vec{Q}V$ pour les cinq variables système : la température du moteur (t_m), la vitesse de rotation (h_r), l'ouverture de la vanne (o_v), le niveau du réservoir de carburant (l_{ft}) et le niveau du réservoir d'huile (l_{ot}).

Fonctionnement nominal

Les mesures d'évaluation de la qualité sont définies pour chaque variable système comme suit : i_{inc} pour l'évaluation de la qualité des données, cd_{err} et ed_{coh} pour l'évaluation de la qualité des informations. Un exemple de mesures associées à un fonctionnement nominal du système est décrit dans la première ligne de la Table III.4. Les données relatives à chaque variable système étant complètes la métrique d'évaluation des données erronées est définie telle que : $i_{inc} = false$. De même, les informations transmises relatives aux variables système sont comprises dans une plage de valeurs possibles : $cd_{err} = false$. La valeur de la cohérence de l'information est définie comme la valeur attendue de la variable système associée moins la valeur mesurée. Par expérimentation, un décalage nominal de 2% a été observé entre les valeurs attendues et mesurées des commandes de contrôle h_r et o_v. Par conséquent, la valeur nominale de la métrique ed_{coh} a été fixée à 2% pour ces variables systèmes ($ed_{coh} = 2$). Concernant les variables système restantes (t_m, l_{ft}, et l_{ot}), la valeur attendue et la valeur mesurée doivent être égales. On définit ainsi leur métrique de cohérence des informations en fonctionnement nominal telle que : $ed_{coh} = 0$.

Premier scénario

Comme il est indiqué dans la seconde ligne de la Table III.4, les attaques de scan de port avec *Nmap* et de *DoS* ne sont pas détectées. Aucune dimension de la qualité des variables système mesurées n'est altérée. Néanmoins on remarque sur la Figure III.7 deux augmentations inhabituelles du nombre de paquets échangés au cours du scénario. La première augmentation correspond aux paquets générés par le scan de port. La deuxième, bien plus conséquente que la première, coïncide avec l'attaque par déni de service qui génère énormément de paquets supplémentaires pour noyer la communication dans le réseau.

TABLE III.4: Évaluation de la qualité pour le prototype de CPS maritime

	Variables système et vecteurs de mesures de qualité associés									
	t_m		h_r		o_v		l_{ft}		l_{ot}	
	$\overrightarrow{DQV}$	$\overrightarrow{IQV}$	$\overrightarrow{DQV}$	$\overrightarrow{IQV}$	$\overrightarrow{DQV}$	$\overrightarrow{IQV}$	$\overrightarrow{DQV}$	$\overrightarrow{IQV}$	$\overrightarrow{DQV}$	$\overrightarrow{IQV}$
Scénario	$\{i_{\text{inc}}\}$	$\{cd_{\text{err}}, ed_{\text{coh}}\}$	$\{i_{\text{inc}}\}$	$\{cd_{\text{err}}, ed_{\text{coh}}\}$	$\{i_{\text{inc}}\}$	$\{cd_{\text{err}}, ed_{\text{coh}}\}$	$\{i_{\text{inc}}\}$	$\{cd_{\text{err}}, ed_{\text{coh}}\}$	$\{i_{\text{inc}}\}$	$\{cd_{\text{err}}, ed_{\text{coh}}\}$
Nominal	{false}	{false,0}	{false}	{false,2}	{false}	{false,2}	{false}	{false,0}	{false}	{false,0}
Scan de port	{false}	{false,0}	{false}	{false,2}	{false}	{false,2}	{false}	{false,0}	{false}	{false,0}
PLC Stop	{false}	{false,**9**}	{**true**}	{**true**,**50**}	{**true**}	{**true**,**50**}	{false}	{false,**−2**}	{false}	{false,**−2**}
Attaque *MiTM* sur h_r	{false}	{**true**,**19**}	{false}	{false,**50**}	{false}	{false,**50**}	{false}	{false,**−2**}	{false}	{false,**−2**}
Attaque *MiTM* sur o_v	{false}	{false,**−19**}	{false}	{false,2}	{false}	{false,**50**}	{false}	{false,0}	{false}	{false,0}

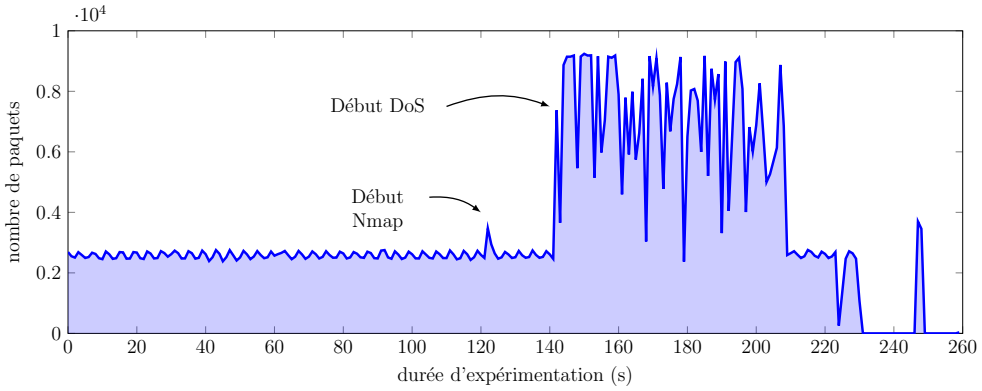


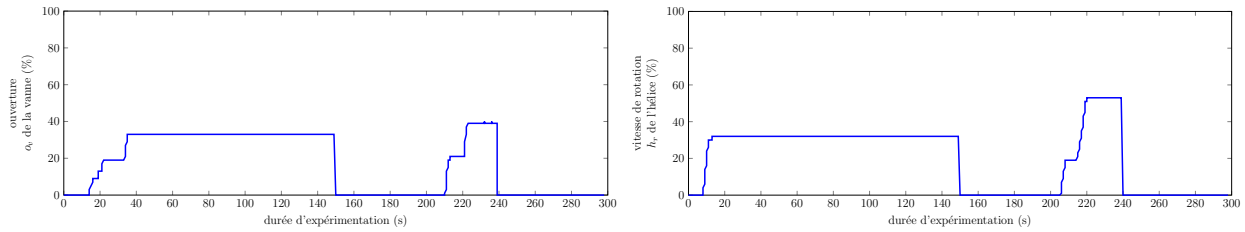
FIGURE III.7: Premier scénario : nombre de paquets échangés en fonction du temps

Deuxième scénario

Dans le scénario suivant, les valeurs de consignes de h_r et o_v sont fixées à 0% puis graduellement augmentées jusqu'à atteindre la valeur de 30%. L'attaque du *PLC stop* est ensuite injectée à $t + 150s$ (Figure III.8) et entraîne une dégradation des transmissions des données et informations. En conséquence, les vecteurs d'évaluation de la qualité sont définis comme suit : $D\vec{Q}V = \{i_{inc} = true\}$ et $I\vec{Q}V = \{cd_{err} = true, ed_{coh} = 30\}$. Comme l'indiquent les évaluations de la qualité respectives, cette anomalie s'est ensuite propagée et a impacté trois autres variables système. Lorsque h_r a été défini à 30%, il était prévu de mesurer une température et une diminution des niveaux des réservoirs de carburant et d'huile spécifiques. À cause de l'arrêt de l'automate, le moteur n'a plus reçu de commande de contrôle et s'est arrêté. Grâce aux dépendances entre variables système (Tab. III.1), et en connaissant les valeurs attendues de h_r et o_v, il a été possible de déterminer les valeurs attendues de t_m, l_{ft}, et l_{ot}. La valeur mesurée de température du moteur est ainsi inférieure de 9°C par rapport à celle attendue. On définit ainsi le vecteur d'évaluation de la qualité d'information telle que : $I\vec{Q}V = \{cd_{err} = false, ed_{coh} = 9\}$. Pour les niveaux des réservoirs, les valeurs mesurées de l_{ot} et l_{ft} n'étaient elles aussi plus cohérentes par rapport à celles attendues, leur évaluation de la qualité de l'information étant définie par $I\vec{Q}V = \{cd_{err} = false, ed_{coh} = -2\}$. Les valeurs des variables t_m, l_{ft}, et l_{ot} sont illustrées dans la Figure C.1 présente en Annexe C.

Troisième scénario

Pour le troisième scénario, les valeurs de consignes de vitesse de rotation h_r de l'hélice et l'ouverture o_v de la vanne sont fixées à 50%. L'attaque *MiTM* prend effet à $t + 50s$ pour



(a) Ouverture o_v de la vanne (b) Vitesse de rotation h_r de l'hélice

FIGURE III.8: Résultats du scénario *PLC stop*

modifier la valeur de la commande de contrôle de h_r à 0% (Figure III.9).Cette altération de l'intégrité de l'information entraîne une dégradation de l'évaluation de la qualité des informations pour la température du moteur (t_m), de l'ouverture de la vanne (o_v), et des niveaux des réservoirs (l_{ft}, l_{ot}). La température attendue du moteur, en accord avec l'équation mathématique qui la régit, est de 42°C. Or, la valeur mesurée est de 23°C. L'évaluation de sa qualité d'information est définie tel que : $\vec{IQV} = \{cd_{err} = false, ed_{coh} = 19\}$. Pour l'ouverture de la vanne, sa valeur mesurée doit être de 0% si la vitesse de rotation de l'hélice est nulle (Tab. III.1), en conséquence $\vec{IQV} = \{cd_{err} = false, ed_{coh} = 50\}$. Une même dégradation de la cohérence des informations est observée pour les niveaux des réservoirs : $\vec{IQV} = \{cd_{err} = false, ed_{coh} = -2\}$. Les valeurs des autres variables o_v, t_m, l_{ft}, et l_{ot} au cours du scénario, sont présentées en Annexe C (Figure C.2).

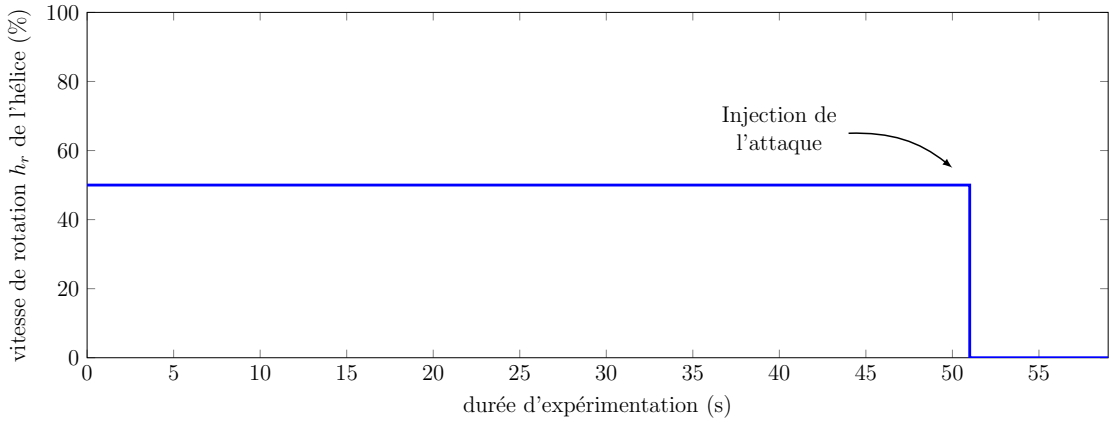


FIGURE III.9: Vitesse de rotation h_r de l'hélice dans le troisième scénario

Quatrième scénario

Pour le quatrième scénario, la valeur de consigne de la vitesse de rotation h_r de l'hélice est fixée à 60%, et celle de l'ouverture o_v de la vanne à 80%. Une *MiTM* prend effet à $t+26s$ pour modifier la valeur de la commande de contrôle de o_v à 0% (Figure III.10). Cela engendre une unique dégradation de l'évaluation de la qualité des informations de la température t_m du moteur. La valeur attendue étant de 40 °C, et celle mesurée de 59 °C, le vecteur d'évaluation associée est défini comme suit : $\vec{IQV} = \{cd_{err} = false, ed_{coh} = -19\}$. Les valeurs des autres variables h_r, t_m, l_{ft} et l_{ot} sont illustrées en Annexe C (Figure C.3).

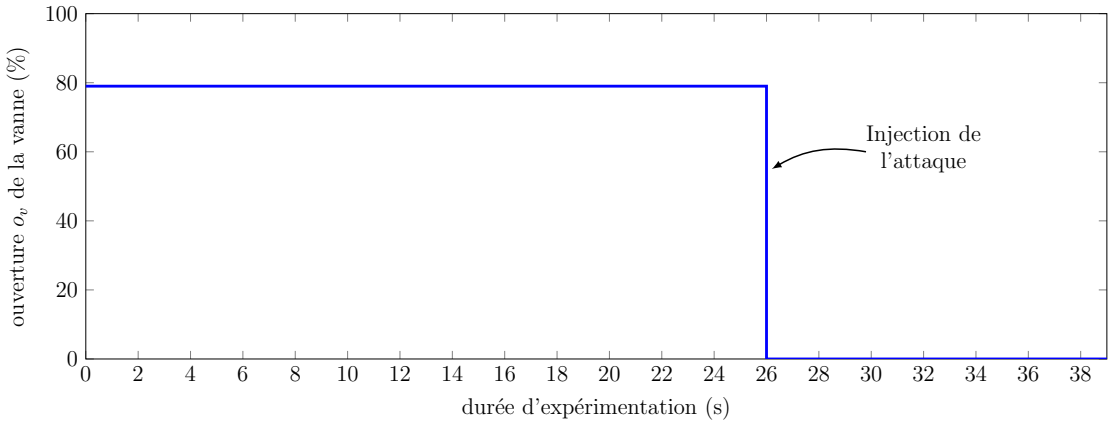


FIGURE III.10: Ouverture o_v de la vanne dans le quatrième scénario

III.2.9 Discussion des résultats

Dans ce cas d'étude nous avons restreint la méthodologie proposée en section II.3.5 à ses deux premières étapes (définition du graphe et définition des métriques de détection) afin analyser la faisabilité et la représentativité de la modélisation d'un CPS sous forme de graphe multicouche avant de réaliser les étapes suivantes. Le graphe ainsi généré fournit une représentation cohérente, ainsi qu'une représentation mathématique adaptée qui génère un certain nombre de métriques pertinentes pour l'analyse des relations dans le système étudié. En complément, nous nous sommes concentrés sur l'analyse de la centralité de proximité des nœuds pour identifier ceux les plus à même de propager une anomalie. De nombreuses autres métriques basées sur les caractéristiques du graphe peuvent être étudiées.

Les résultats expérimentaux ont montré que **trois des quatre anomalies**, injectées à partir des différents scénarios, ont pu être détectées. Les résultats obtenus vis-à-vis de

la quantité des dimensions dégradées par l'anomalie en fonction du nœud visé confirment notre hypothèse sur la pertinence de l'analyse préliminaire des graphes. En effet, les nœuds critiques initialement identifiés par la mesure de centralité de proximité correspondent à ceux qui ont le plus impacté le système en favorisant la propagation de l'anomalie. Concernant l'attaque de scan de port suivi du *DoS*, celle-ci n'a pas été détectée, car les dimensions de qualité des données et de l'information évaluées ne tenaient pas compte de l'augmentation du volume du trafic réseau. Une métrique d'évaluation de la qualité des informations basée sur les données réseau aurait facilement détecté ces anomalies.

L'approche proposée à partir de cas d'étude est néanmoins quelque peu limitée par le fait qu'il soit difficile de vérifier automatiquement l'exhaustivité des relations entre les variables système, si cette information n'est pas fournie dans la conception du système. De plus le choix et l'affectation des dimensions de l'évaluation de la qualité doivent être en accord avec les caractéristiques de chaque sous-système impliqué.

Le cas d'étude présenté est lui aussi restreint par les limitations inhérentes au prototype de CPS maritime. Bien que la simulation des capteurs et actionneurs présente de nombreux avantages, celle-ci cantonne les possibilités d'expérimentations car le comportement de ces sous-systèmes, en réponse à certaines anomalies, peut être difficile à simuler de manière réaliste. Par exemple, un dysfonctionnement lié à un composant extérieur au sous-système sera difficilement reproductible par simulation. De plus, la simulation de ces sous-systèmes entraîne une restriction du choix des métriques de l'évaluation de la qualité puisqu'un certain nombre sont basées sur les caractéristiques propres à ceux-ci. Le cas d'étude est aussi restreint par le nombre de sous-systèmes, et variables associées, composant le prototype de CPS maritime. Il sera intéressant de confronter l'approche proposée à un système cyber-physique composé d'un plus grand nombre de sous-systèmes et de dépendances.

Cette première expérimentation a permis de souligner la cohérence et l'apport du modèle de graphe 3-couches proposé. Elle valide ainsi une première étape de la méthodologie formulée pour l'évaluation de la propagation d'anomalies dans les CPS maritimes. Afin de valider la totalité de la méthodologie, celle-ci sera par la suite confrontée à un réseau de distribution d'eau *intelligent*. Contrairement au premier un cas d'étude, nous réaliserons l'entièreté de ses étapes.

III.3 Deuxième cas d'étude : le réseau de distribution d'eau *intelligent*

Nous présentons dans cette section l'expérimentation réalisée à partir d'un outil de simulation de réseau de distribution d'eau *intelligent*. Dans un premier temps, nous introduisons les problématiques liées à la distribution de l'eau, notamment à bord d'un bateau, puis nous décrivons l'outil de simulation utilisé. Pour terminer, nous précisons les différents scénarios étudiés, l'implémentation de la méthodologie d'évaluation de la propagation d'anomalie, et les résultats obtenus

III.3.1 Problématique de la distribution de l'eau

Importance de la gestion de l'eau

Depuis plusieurs années, différents États s'accordent sur la définition d'actifs vitaux pour le fonctionnement de la société ou de l'économie, et dont la protection demeure un enjeu critique. Les réflexions autour de la protection de ces actifs se sont principalement démocratisées dans les années 2000 avec la parution aux États-Unis de la directive présidentielle n°7 [Pre03] sur la sécurité intérieure. Celle-ci vise à identifier et hiérarchiser les infrastructures critiques contre les attaques terroristes. En Europe, le Programme Européen pour la Protection des Infrastructures Critiques [9] est lancé en 2004 par le Conseil européen. En résulte la directive 2008/114/CE [Eur08] du Conseil Européen du 8 décembre 2008 relative au recensement et la désignation des infrastructures critiques européennes pour évaluer la nécessité d'améliorer leur protection. En France, des OIV sont identifiés à partir d'un décret [10] comme des organisations dont les activités sont vitales ou dangereuses à la nation. Pour faire face aux nouvelles menaces cyber auxquelles ils sont exposés, le cadre législatif associé aux OIV s'est renforcé avec l'article 22 de la loi de programmation militaire [11] qui impose à ces opérateurs le renforcement de la sécurité de leurs systèmes d'information critiques. Dans cette continuité, le cadre législatif s'est encore une fois étendu avec le décret

9. European Programme for Critical Infrastructure Protection

10. Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale. JORF. Consulté le 05 mai 2021. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000634536/

11. Article 22 de la loi n° 2013-1168 du 18 décembre 2013. JORF. Consulté le 05 mai 2021.https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000028338907?r=fTBzVqx2C3/

n°2018-384 du 23 mai 2018 [12] visant à transposer la directive européenne NIS à partir de la création d'un cadre réglementaire pour renforcer la cybersécurité des OSE qui sont essentiels au fonctionnement de l'économie et de la société.

L'ensemble de ces textes peuvent parfois différer sur l'identification de certains actifs mais s'accordent néanmoins sur une grande majorité. Étant une ressource vitale pour la population, la gestion de l'eau est l'un de ces actifs communément caractérisés. Le secteur de l'eau implique un nombre d'acteurs importants intervenant tout au long du processus de sa gestion. Cela comprend à la fois sa production, sa distribution, la construction et maintenance des réseaux, son assainissement, mais aussi la fabrication des différents équipements associés.

Plus récemment, l'eau a démontré un tout autre intérêt qu'au travers de son utilisation et de sa consommation. Dans le cadre de la pandémie mondiale associée au coronavirus SARS-CoV-2, l'analyse de la quantification de ses génomes dans les eaux usées apparaît comme un moyen efficace pour surveiller la dynamique de la propagation du virus [WWFR+21]. C'est notamment la stratégie employée par les marins-pompiers de Marseille pour fournir un indicateur supplémentaire pour l'analyse de sa circulation (Figure III.11).

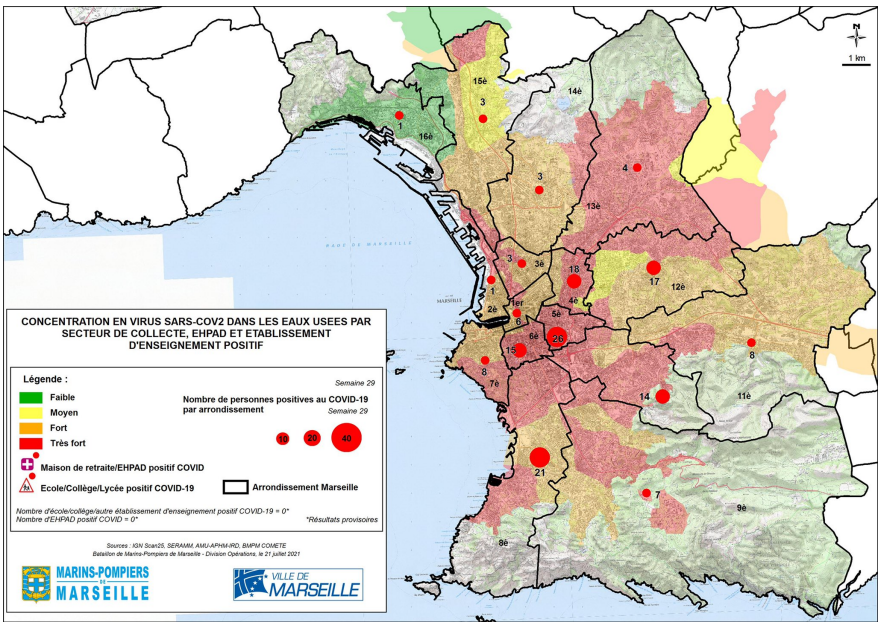


FIGURE III.11: Cartographie du taux de concentration en virus SARS-CoV-2 dans les eaux usées de la ville de Marseille (source : Twitter Marins-Pompiers de Marseille)

12. Décret n°2018-384 du 23 mai 2018. JORF. Consulté le 05 mai 2021.https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036939971//

Numérisation des réseaux de distribution d'eau

Autrefois, les réseaux de distribution d'eau étaient complètement isolés du monde numérique et des menaces associées. Ils ont par la suite subi une numérisation progressive avec l'arrivée de nouveaux équipements et composants informatiques. L'utilisation du cyberespace a ainsi permis d'améliorer les performances inhérentes au réseau dans le contrôle du processus physique, mais aussi dans sa surveillance et sa gestion à distance. De par de cette dualité entre le monde physique et le monde numérique, ces nouveaux réseaux de distribution d'eau *intelligents* sont définis comme des systèmes cyber-physiques. Le secteur de l'eau est vulnérable à une variété d'attaques physiques, par la contamination de l'eau au travers de différents agents mortels, mais aussi à différents types de cyberattaques. En effet, la numérisation des réseaux de gestion de l'eau augmente considérablement le nombre de menaces auxquelles doit faire face le système. Récemment, un cyberattaquant a accédé à distance à une station de traitement des eaux d'une ville de Floride [13]. Il a ainsi multiplié le niveau d'hydroxyde de sodium présent dans l'eau potable par 100, ce qui aurait pu engendrer de graves conséquences sur la population si l'eau avait été consommée. La réalisation de ces attaques aurait un impact direct sur le consommateur via la consommation de l'eau contaminée, mais aussi indirecte via une répercussion des conséquences sur la santé publique et l'économie. Des actifs vitaux tels que les moyens de luttes contre les incendies, les services de santé, ainsi que d'autres secteurs dépendants et interdépendants, comme la production d'énergie, l'alimentation et l'agriculture, seraient fortement impactés par la dégradation ou l'arrêt des services et ressources fournis par le secteur de l'eau.

Gestion de l'eau à bord d'un navire

À bord d'un navire de la gestion de l'eau est un enjeu majeur dont la criticité est accrue par les contraintes inhérentes au domaine maritime. Les restrictions physiques complexifient la mise en place du réseau, sa surveillance, ainsi que sa maintenance. Comme tout autre système vital à bord, le réseau de distribution d'eau doit être fortement résilient pour endurer des durées de missions, allant de quelques heures à plusieurs mois, sans maintenance à terre. L'eau douce peut être obtenue à bord grâce des réservoirs remplis à terre, ou en mer à partir d'un navire ravitailleur. Néanmoins, la majorité des navires, plus particulièrement les navires qui transportent un certain nombre de personnes à bord, embarquent

13. 'Dangerous Stuff' : Hackers Tried to Poison Water Supply of Florida Town. The New York Times. Consulté le 05 mai 2021. https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html

un système de désalinisation de l'eau de mer pour accroître leur autonomie en mer. Ce qui est d'autant plus important selon la mission pour laquelle le navire est employé. Ces systèmes utilisent principalement trois méthodes, l'évaporation de l'eau de mer pour recueillir le condensat d'eau douce, sa filtration, ou encore l'osmose inverse. Ces méthodes ne sont pas sans risques puisqu'elles laissent dans l'eau des composés organiques qui peuvent être nocifs pour l'homme [14]. L'optimisation des réservoirs d'eau du navire, par rapport à sa production d'eau, fait d'ailleurs l'objet d'étude scientifique [Kri16].

La distribution de l'eau à bord d'un navire impacte directement l'équipage ou les passagers par sa consommation, mais aussi indirectement par son utilisation quotidienne. Dans le secteur civil, Z. Sobol *et al.* estimaient en 1984 que 200 L d'eau par personne et par jour étaient nécessaires pour assurer les besoins de base de la vie quotidienne à bord (cuisine, toilette, lessive, utilisation des sanitaires, etc.) [Sob84]. Au regard des études scientifiques récentes qui corroborent ce même chiffre, il semble que ce quota soit toujours d'actualité [Edi11, MT20]. Dans le secteur militaire, ces standards sont davantage restreints, notamment dans les sous-marins. Par exemple, la consommation d'eau dans un SNA [15] de classe *Rubis* est limitée à 20 L par jour et par marin.

Dans le secteur civil comme militaire, le contrôle de la qualité de l'eau à bord, ainsi que sa bonne distribution, sont des problématiques majeures. L'altération de la qualité de l'eau peut engendrer des conséquences considérables sur la santé de l'équipage. Par exemple, un système de stockage et distribution de l'eau mal contrôlé peut constituer une voie de transmission de maladies infectieuses [JHC+96]. Une étude scientifique a mis en avant les sources infectieuses de plus de 100 épidémies survenues à bord d'un navire [RBC+04]. Un cinquième d'entre elles a été attribué à une source d'origine hydrique.

Outre son utilisation quotidienne pour assurer un certain niveau de conditions de vie à toute personne à bord, l'eau est aussi utilisée par différents systèmes auxiliaires en charge du bon fonctionnement du navire. Par exemple, sur certains navires de surface on distingue un système de ballast destiné à optimiser la navigation par le remplissage ou la vidange de réservoirs avec de l'eau. Ces processus de ballastage ou déballastage sont principalement effectués pour des conditions particulières de navigation comme l'entrée dans un chenal ou la traversée d'un canal, pendant le chargement ou le déchargement de la cargaison, ou lorsque

14. Potable water on ships : the top 5 most commonly asked questions. Martek Marine. Consulté le 05 mai 2021. `https://www.martek-marine.com/blog/potable-water-ships-top-5-commonly-asked-questions/`

15. Sous-marin Nucléaire d'Attaque

le navire se rend à l'accostage [16]. Dans le cas des sous-marins, les ballasts permettent de contrôler leur immersion via leurs remplissages ou leurs vidanges. La gestion de l'eau est également un enjeu majeur pour le maintien en bonne condition du système de propulsion du navire. Les systèmes de motorisation installés à bord sont conçus pour fonctionner sans interruption, et cela, avec un maximum d'efficacité. Afin de limiter et d'évacuer les pertes d'énergie thermique, un système de refroidissement est associé au système de motorisation. Le refroidissement est réalisé à partir d'échangeurs thermiques utilisant de l'eau en circuit fermé ou puisé dans la mer [17].

Les navires modernes embarquent des systèmes semi-automatiques de gestion de l'eau pour faciliter le contrôle et la surveillance des équipements et composants utilisés pour son stockage, sa distribution et son traitement. Le réseau de distribution d'eau à bord est composé d'équipements hydrauliques classiques comme des pompes, des vannes, des réservoirs, de systèmes de traitements des eaux usées et production d'eau potable. À l'identique des réseaux de distribution d'eau *intelligents*, ces équipements sont contrôlés par des *PLC* et surveillés par différents capteurs. L'ensemble du réseau est supervisé par un opérateur, depuis le poste de contrôle, à partir d'un système de contrôle et d'acquisition de données. En raison de ces caractéristiques, la gestion de l'eau à bord est assimilée à celle d'une infrastructure associée à une ville de taille réduite [Lee19].

Les vulnérabilités associées au réseau de distribution d'eau embarqué sont identiques à celles définies précédemment pour les réseaux de distribution d'eau *intelligents*. Néanmoins, les conséquences pouvant résulter de l'exploitation de ces vulnérabilités sont nettement plus importantes. La dégradation ou la mise en péril du système de gestion de l'eau à bord aurait un impact direct sur les personnes embarquées, et sur les fonctions propres du navire.

Pour ces raisons, nous avons fait le choix de confronter la méthode proposée à des jeux de données issues d'un réseau de distribution d'eau simulé. La simulation de celui-ci est réalisée à partir de deux outils différents, l'un utilisé pour la simulation hydraulique du réseau, et l'autre pour la simulation de sa couche numérique et des attaques associées.

16. A Guide To Ballast Tanks On Ships. Marine Insight. Consulté le 05 mai 2021. https://www.marineinsight.com/naval-architecture/a-guide-to-ballast-tanks-on-ships/

17. General Overview of Central Cooling System on Ships. Marine Insight. Consulté le 05 mai 2021. https://www.marineinsight.com/guidelines/general-overview-of-central-cooling-system-on-ships/

III.3.2 Simulation hydraulique du réseau de distribution d'eau

L'Agence de protection de l'environnement des États-Unis (*United States Environmental Protection Agency*), en charge de la protection de la nature et la santé des citoyens américains, est particulièrement concernée par l'étude de qualité de l'eau, sa distribution, ainsi que son traitement. De ce fait l'agence a développé EPANET [Ros00], un logiciel *open-source*[18] d'analyse des systèmes de distribution d'eau. Cette analyse comprend à la fois la modélisation du système, ainsi que la simulation de son comportement hydraulique et qualitatif. Tuyaux, nœuds, pompes, vannes, et réservoirs : chaque composant hydraulique et son comportement sont disponibles pour agrémenter la simulation du réseau. EPANET génère au travers de la simulation un certain nombre de variables comme le niveau d'eau dans les réservoirs, la pression à chaque nœud du réseau, ainsi que différentes variables associées à l'analyse de la qualité de l'eau, comme la concentration de substances chimiques dans les différentes portions du réseau.

De par ses caractéristiques et possibilités offertes à l'utilisateur, EPANET recouvre un immense spectre de domaines d'étude basé sur l'analyse de réseau de distribution d'eau. Une étude a utilisé les données générées par le logiciel pour obtenir un modèle de détection d'anomalie dans un réseau de distribution eau *intelligent*, à partir de l'estimation du comportement dynamique du système [AMR17]. D'autres études utilisent ce logiciel pour des problématiques environnementales liées à la distribution de l'eau. EPANET a par exemple permis la simulation d'un système d'irrigation, dans le cadre d'un développement de modèle pour synchroniser la disponibilité de l'énergie photovoltaïque avec l'énergie requise pour alimenter le réseau d'irrigation [MFC+18]. Un autre travail a utilisé ce logiciel pour simuler le réseau de distribution de la ville de Houston afin d'étudier la viabilité économique et environnementale de la réutilisation directe de l'eau [LLDO+20].

Un réseau de distribution d'eau simulé à partir d'EPANET, nommé *C-town*, a particulièrement été étudié dans la littérature. Ce réseau réel de taille moyenne fut introduit dans la littérature en 2010 lors du *Battle of the Water CalibrationNetworks*. Ce challenge regroupait des individus du monde universitaire, du secteur privé et des services publics, pour comparer différentes méthodes de calibration du réseau de distribution d'eau proposé afin d'améliorer ses performances. En tant que référence dans le domaine, ce réseau fut par la suite réutilisé pour d'autres travaux traitant de l'analyse et la gestion de fuites [SPB+16] ou de l'amélioration de la distribution de l'eau [DNGG+18].

18. Logiciel dont le code source est libre.

Comme présenté dans la figure III.12, ce réseau est constitué de 388 nœuds de consommation, 7 réservoirs (T1-T7), quatre vannes dont une actionnable (V1-V4), 11 pompes (PU1-PU11) regroupées en 5 stations de pompage, et un réservoir (R1). L'ensemble est relié par 429 liens.

Afin de personnaliser EPANET selon les besoins d'utilisation, le logiciel fournit un outil de programmation basé sur une *Dynamic Link Library (DLL)*[19] de plus de 50 fonctions. Celles-ci peuvent être incorporées dans différentes applications pour résoudre des problématiques spécifiques dans des domaines d'étude divers et variés. Elles permettent ainsi de modifier divers paramètres de conception du réseau, d'exécuter des simulations, de contrôler les systèmes de distribution, et surtout d'accéder aux résultats générés en parallèle de l'exécution. Cet outil de programmation est particulièrement utile pour le développement d'applications spécifiques associées à l'utilisation de réseau de distribution d'eau. Par exemple, cet outil de programmation a été utilisé dans des travaux de recherche afin de développer un logiciel de simulation pour optimiser le placement de capteur d'analyse de qualité de l'eau dans un réseau de distribution [EKP14]. Un autre outil de programmation exploite la LDL d'EPANET pour optimiser le fonctionnement des pompes dans un réseau de distribution d'eau en prenant compte différents paramètres [MSL16].

III.3.3 Simulation de la couche numérique du réseau de distribution d'eau

Bien qu'EPANET fournisse une représentation et une simulation détaillée des composants physiques principaux d'un réseau de distribution d'eau, il n'est pas conçu pour étudier les différentes interactions entre ces composants et les dispositifs numériques modernes de contrôle et de supervision. Parmi ces dispositifs on retrouve notamment : les compteurs d'eau *intelligent*, les capteurs connectés, les automates programmables, et les systèmes de contrôle et d'acquisition de données. Comme défini précédemment dans la section III.3.1, ces dispositifs présentent de nombreuses vulnérabilités en raison de leurs caractéristiques numériques. Ils doivent ainsi faire face à différentes menaces exploitant ces vulnérabilités pour perturber le fonctionnement du réseau de distribution d'eau. Ces menaces se caractérisent de plus en plus par des cyberattaques visant la couche numérique du réseau, et des attaques cyber-physiques visant les équipements du réseau qui interagissent avec le processus physique [HRG+20]. De l'arrêt total du réseau de distribution à la dégradation de la qualité de l'eau, les impacts

19. Bibliothèque logicielle dynamique

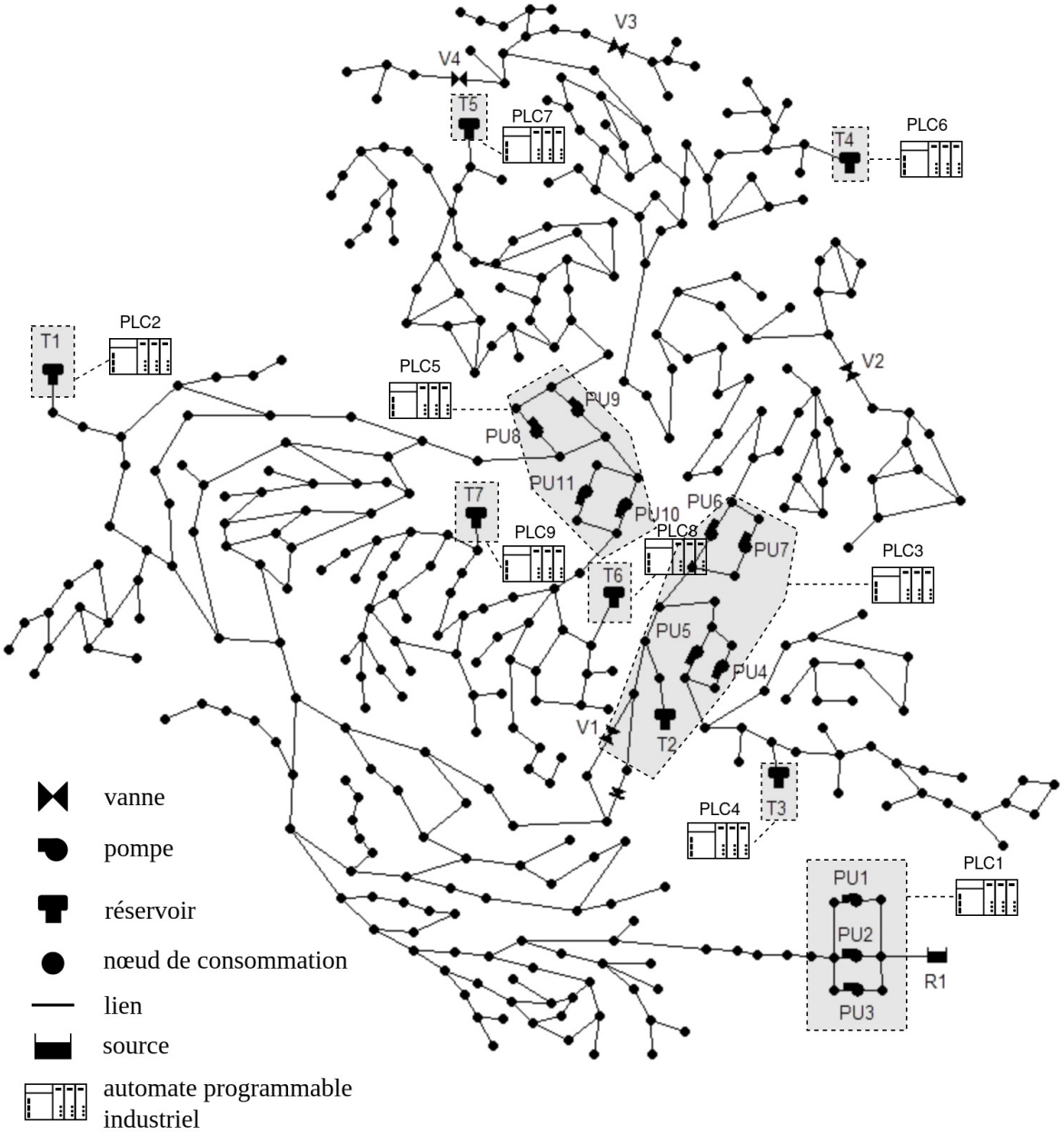


FIGURE III.12: Réseau de distribution d'eau *C-town* (parties hydraulique et numérique)

potentiels de ces attaques sont critiques. En conséquence, la caractérisation et la simulation des interactions entre le réseau hydraulique qui assure la distribution de l'eau, et le réseau numérique en charge de son contrôle et de sa surveillance, est une problématique majeure de recherche.

TABLE III.5: Composants du réseau de distribution d'eau *C-town*

Composants hydrauliques	**Nombre**	**Variables associées**
Nœuds de consommation	388	
Liens	429	
Réservoirs	7	l
Pompes	11	f, e
Vannes	4 (1 actionnable)	f, e
Dispositifs numériques		
PLC	9	
SCADA	1	

Un outil de programmation *open-source*, nommé epanetCPA, a été développé à partir de MATLAB® pour répondre à cette problématique [TGD+19]. Il exploite les capacités d'EPANET, au travers de sa DLL, pour modéliser et simuler une couche numérique en interaction avec le réseau de distribution d'eau afin de le contrôler et de le superviser. Cet outil transforme ainsi le réseau de distribution d'eau en réseau *intelligent*. La couche numérique comprend le système *SCADA* et les différents automates programmables, reliés à des capteurs et/ou actionneurs. Ces API génèrent des commandes de contrôle automatiques relatives à chaque actionneur, en adéquation avec les mesures de capteurs reçues, afin de contrôler le processus physique. Certains *PLC* sont amenés à communiquer entre eux pour fournir ces données de capteurs nécessaires à la génération des commandes de contrôle. De plus, chaque *PLC* envoie au système *SCADA* les données de capteur mesurées et les valeurs de variable d'état des actionneurs.

Chaque pompe PU et chaque vanne V est définie par 2 variables : une première caractérisant le débit volumique (f), et une deuxième déterminant l'état de marche de la pompe (e). Les réservoirs T sont quant à eux définis par une seule variable associée à leur niveau d'eau (l). La couche numérique est composée de 9 PLC et un SCADA. Ces dispositifs ne sont caractérisés par aucune variable. L'ensemble des composants hydrauliques et des dispositifs numériques sont présentés dans la Table III.5. Le stockage et la distribution de l'eau sont assurés par les 7 réservoirs dont le niveau déclenche l'activation ou l'arrêt des 11 pompes

et de la vanne actionnable. Chaque actionneur, i.e. les pompes et les vannes, est relié à l'un des 9 PLC qui contrôlent chacun d'entre eux à partir de commandes de contrôle locales. Les capteurs de niveau des 7 réservoirs sont de même connectés aux PLC pour transmettre les données mesurées et activer les actionneurs en proportion. Un système SCADA collecte les données relevées par les automates, ainsi que les valeurs des variables d'état des actionneurs, pour superviser et coordonner le processus en conséquence. L'ensemble des variables mesurables du réseau de distribution hydraulique *C-town* est détaillé dans la Table III.6.

TABLE III.6: Variables mesurables du réseau de distribution d'eau *C-town*

	Variable		
Composant	**Notation**	**Description**	**Unité**
Pompe	f	Débit volumique	gpm[1]
	e	Variable d'état (0/1)	n/a
Vanne	f	Débit volumique	gpm
	e	Variable d'état (0/1)	n/a
Réservoir	l	Niveau d'eau dans le réservoir	mètres

[1] : *gallon per minute*

TABLE III.7: Dépendances entre les composants du réseau de distribution d'eau *C-town*

PLC[1]	Capteur	Actionneurs
PLC1	—	PU1(T1), PU2(T1), PU3(—)
PLC2	T1	—
PLC3	T2	V1(T2), PU4(T3), PU5(T3), PU6(T4), PU7(T4)
PLC4	T3	—
PLC5	—	PU8(T5), PU9(—), PU10(T7), PU11(T7)
PLC6	T4	—
PLC7	T5	—
PLC8	T6	—
PLC9	T7	—

[1] : Une connexion d'automate à automate est établie lorsqu'un actionneur et son capteur de contrôle sont reliés à deux automates différents.

La Table III.7 présente le rôle de chacun des 9 automates, par rapport au capteur auquel il est relié ou l'actionneur hydraulique qu'il contrôle. Ces rôles sont spécifiques. La plupart des PLC qui contrôlent un actionneur ne sont pas connectés aux capteurs, et inversement.

Les données mesurées de capteur sont donc partagées entre différents automates pour générer des commandes de contrôle en adéquation avec l'état du processus physique. Dans la Table concernée, lorsqu'un actionneur agit sur le remplissage d'un réservoir, cela est représenté par le schéma de formulation suivant : « nom de l'actionneur (nom du réservoir) ». Si pour un actionneur donné, aucun réservoir n'est impacté par son activation ou son arrêt, cela est formulé de la sorte : « nom de l'actionneur(—) ».

III.3.4 Génération du graphe

Comme présenté dans la section III.4, un processus basé sur l'exploitation du driver Neo4j permet de générer le graphe 3-couches associé au réseau de distribution d'eau. Il est défini par deux sous-graphes des sous-systèmes (G_1) et variables (G_2) du CPS. La description du graphe généré et de ses composants est réalisée en trois parties :

1. La description du sous-graphe des sous-systèmes du CPS (G_1),
2. celle du sous-graphe des variables du CPS (G_2)
3. et le lien entre les deux.

Sous-graphe des sous-systèmes du CPS (G_1)

Dans le premier sous-graphe G_1 les composants du réseau hydraulique, à l'exception des nœuds de demandes, sont modélisés sous forme d'un ensemble $S_{physique}$ (Équation III.9) de $I = 19$ nœuds s_i appartenant à la couche physique du graphe :

$$S_{physique} = \{PU1, PU2, PU3, PU4, PU5, PU6, PU7, PU8, PU9, PU10, PU11, T1, T2, T3, T4, T5, T6, T7, V2\} \quad \text{(III.9)}$$

Les dispositifs numériques sont eux aussi modélisés à partir d'un ensemble $S_{numerique}$ (Équation III.10) de $I = 10$ nœuds s_i. Chaque nœud s_i appartenant à la couche numérique du graphe :

$$S_{numerique} = \{PLC1, PLC2, PLC3, PLC4, PLC5, PLC6, PLC7, PL8, PL9, SCADA\} \quad \text{(III.10)}$$

L'ensemble R de $L = 39$ relations de dépendances (Équation III.11), reliant ces nœuds entre eux, est défini à partir des informations de la Table III.7 ainsi que grâce aux connaissances de l'architecture du système :

$$R = \{7\times(T \rightarrow PLC), 9\times(PU \rightarrow T), 11\times(PLC \rightarrow PU), 4\times(PLC \rightarrow PLC), 8\times(PLC \rightarrow SCADA)\} \quad \text{(III.11)}$$

Sous-graphe des variables systèmes (G_2)

Le sous-graphe G_2 est quant à lui composé par les variables systèmes définies sous forme d'un ensemble V de $K = 31$ nœuds v_k appartenant à la troisième couche du modèle. Ces nœuds modélisent l'ensemble des variables associées aux composants hydrauliques du réseau de distribution d'eau.

$$V = \{f_{1-12}, e_{1-12}, l_{1-7}\} \quad \text{(III.12)}$$

Ces nœuds de variables système sont reliés entre eux à partir d'un ensemble C de $L = 29$ relations de corrélation. Ces relations sont définies à partir de la connaissance opérationnelle du réseau de distribution. Pour chaque pompe PU, son débit volumique f associé est structurellement corrélé à sa variable d'état e. Parallèlement, le niveau d'eau l de chaque réservoir T est opérationnellement corrélé au flux d'eau traversant les pompes en charge de son remplissage :

$$C = \{9 \times (f \rightarrow l), 11 \times (e \rightarrow l)\} \quad \text{(III.13)}$$

Liens entre les deux sous-graphes

Les deux sous-graphes G_1 et G_2 sont liés entre eux par un ensemble A de $U = 31$ relations d'association de nœud de variables systèmes v_k aux nœuds de sous-système s_i

(Équation III.14).

$$A = \{12 \times (f \rightarrow PU), 12 \times (s \rightarrow PU), 7 \times (l \rightarrow T)\} \tag{III.14}$$

Le graphe obtenu, composé des différents nœuds et relations, est présenté dans la Figure III.13, par soucis de clarté les couches ne sont pas représentées. Sont identifiables 9 portions du graphe, distinctes selon leur rôle opérationnel dans le réseau de distribution. Les portions 2, 3, 6 et 9 sont associées au maintien du niveau d'un réservoir à partir de deux pompes, contrairement à d'autres portions où une seule pompe/vanne est impliquée. En conséquence, ces portions sont donc plus intéressantes à étudier. Dans la suite de ces travaux, les études à partir du graphe de *C-town* généré ne traiteront que de ces portions. Un exemple de modélisation de la portion 9 du graphe est illustré dans la Figure III.14.

Nous avons fait le choix de ne pas modéliser les nœuds de demande d'eau dans le graphe car ceux-ci sont considérés comme des composants passifs du réseau de distribution. En effet, EPANET simule leur consommation selon une courbe de demande définie en amont de la simulation. Celle-ci évolue au cours du temps de la simulation mais les différentes attaques injectées dans le réseau à partir d'epanetCPA ne modifient pas cette consommation. Il serait cependant envisageable d'étudier le taux de satisfaction de la demande pour certains nœuds, i.e. le rapport entre l'eau distribuée et l'eau demandée à un point de demande défini, pour évaluer l'impact des attaques sur les consommateurs.

III.3.5 Attaques simulées

Un système de distribution d'eau, comme tout système critique, doit à la fois satisfaire ses objectifs opérationnels inhérents à la distribution de l'eau, mais aussi ses obligations en matière de cybersécurité. Comme présenté dans la section I.3.1, un système cyber-physique doit respecter, par ordre d'importance, les critères fondamentaux de sécurité de l'information qui sont : la disponibilité, l'intégrité et la confidentialité. [RHM+16]. Les principaux types de cyberattaques visant les CPS ont été détaillés dans la section I.3.3. En addition des cyberattaques, un CPS peut aussi être impacté par des **attaques ou dysfonctionnements physiques**. La dégradation, volontaire ou non, de ses sous-systèmes physiques, sont à même d'induire des anomalies dans le système. EpanetCPA octroie à l'utilisateur d'injecter ces différentes attaques au sein de la simulation hydraulique pour analyser les effets et conséquences sur le réseau de distribution d'eau. On distingue dans l'outil 4 catégories

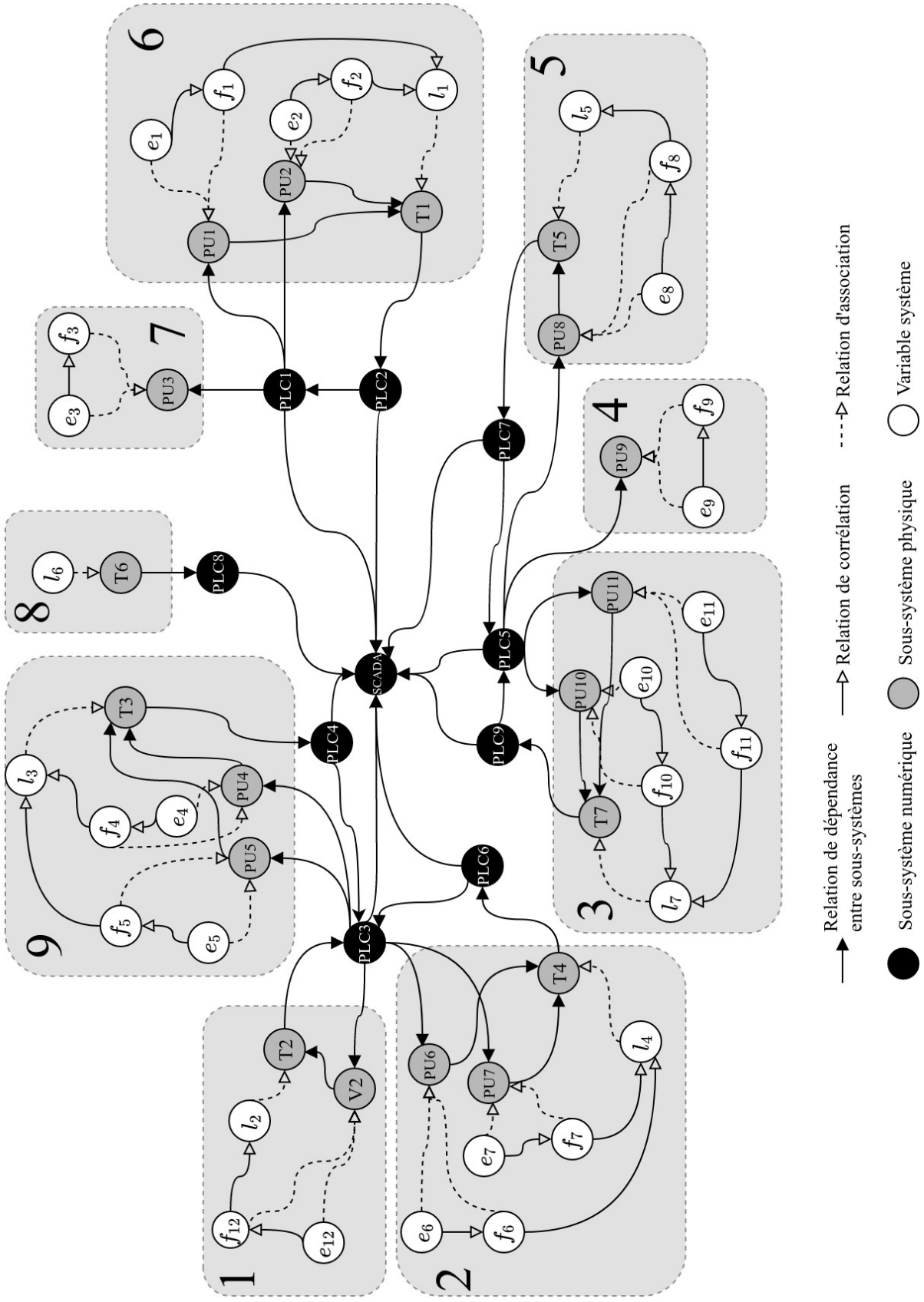


FIGURE III.13: Graphe de *C-town* généré

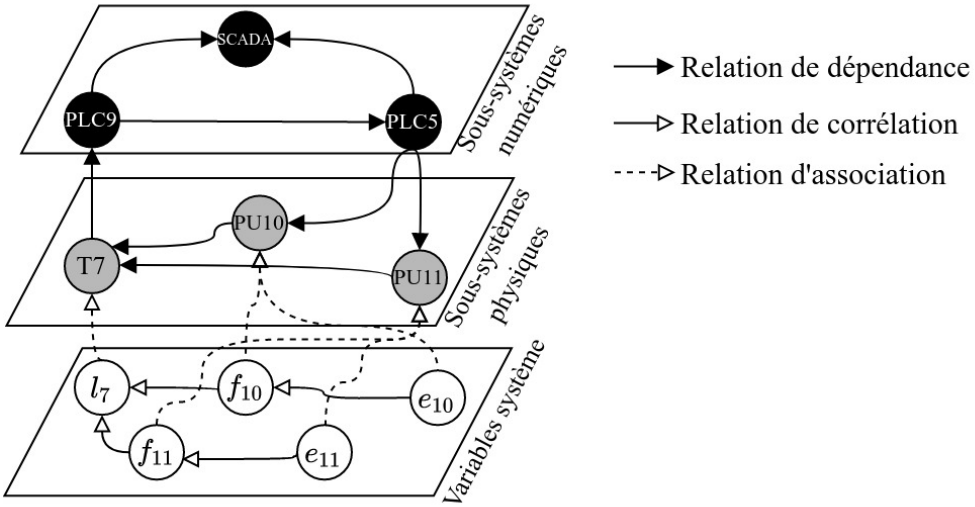


FIGURE III.14: Portion 9 du graphe de *C-town*

d'attaques impactant la couche physique ou numérique du système :

- Les attaques **physiques sur les capteurs**, pour modifier les valeurs mesurées en ajoutant un *offset*[20] ou en définissant une valeur constante.
- Les attaques **physiques sur les actionneurs**, pour modifier la valeur de leur variable d'état ou forcer leur mise en fonction ou leur arrêt.
- Les cyberattaques sur les liens de communications, pour altérer les échanges entre les différents sous-systèmes **numériques**. Il est ainsi possible d'altérer les échanges de valeurs mesurées en les substituant avec une valeur ou en ajoutant un offset. La disponibilité de la liaison peut être impactée par une attaque *DoS*, et ainsi empêcher les automates de recevoir les valeurs mesurées. L'intégrité de la liaison est aussi altérable à partir d'une attaque par rejeu pour tromper les automates et induire la génération de commandes de contrôle inadaptées.

Chacune des attaques injectées est caractérisée par des arguments spécifiques et des arguments communs à chaque attaque. Parmi ces arguments communs, on distingue notamment des conditions de déclenchement et d'arrêt de l'attaque. Deux types de conditions de déclenchement existent et sont aussi combinables entre elles :

- Une première condition basée sur le temps de simulation. Par exemple, l'attaque est déclenchée à $t_0 = 5h$ et s'arrête à $t_1 = 20h$.
- Une deuxième condition est définie par des valeurs de variables des actionneurs ou

20. décalage

des capteurs. Par exemple, l'attaque est injectée lors que la pompe PU10 est allumée ($e_{10} = true$) et s'arrête lorsque le niveau de réservoir T7 est supérieur à 2 m ($l_7 > 2$).

III.3.6 Scénarios d'expérimentation

L'objectif principal d'un système de distribution d'eau est de satisfaire la demande des utilisateurs du réseau tout en garantissant un certain niveau de qualité de l'eau distribuée. Les scénarios d'attaque créés dans le cadre de ces travaux visent ainsi à perturber ou arrêter le fonctionnement du réseau de distribution d'eau à partir de différentes cyberattaques afin d'évaluer leurs propagations au sein du système. Comme défini par epanetCPA, un scénario est composé de plusieurs éléments distinctifs :

— Une durée de simulation hydraulique. Elle est définie à partir d'EPANET.
— Une ou plusieurs cyberattaques selon une liste finie d'attaques proposées par epanetCPA.
— Une ou plusieurs conditions de déclenchement et d'arrêt des attaques.

Les scénarios d'attaques du réseau de distribution d'eau ont été définis de manière la plus réaliste possible pour être au plus proche des conditions opérationnelles réelles. En conséquence, les cyberattaques choisies pour chaque scénario correspondent aux menaces les plus représentatives pour ce type de système. Chaque scénario est défini par un type spécifique d'attaque initiée sur la couche physique ou numérique. Les attaques choisies impactent les deux critères de sécurité les plus critiques pour les CPS : la disponibilité et l'intégrité.

Un total de 5 scénarios a ainsi été créé : 1 scénario en fonctionnement nominal où le réseau ne subit aucune attaque, et 4 scénarios définis par une attaque distinctive impactant le réseau de distribution d'eau. Chacun de ces scénarios, et de ses composants associés, est détaillé dans la Table III.8. La durée de simulation de chaque scénario est fixée à 144 heures car cela est suffisant pour observer la propagation d'anomalies générées dans le réseau.

Dans le **premier scénario** une **cyberattaque** de type *DoS* cible l'automate. Celui-ci est en charge du recueil des valeurs mesurées du niveau de réservoir T1 pour ensuite les transmettre au PLC1, qui commande l'activation des pompes PU1 et PU2 en proportion. L'attaque *DoS* déclenchée à la $50^{\text{ème}}$ heures de la simulation ($t_{start} = 50h$), va impacter la **disponibilité** du canal de communication entre les deux automates en le saturant entièrement.

TABLE III.8: Descriptions des scénarios d'attaque

	Déclenchement de l'attaque			Description de l'attaque			
Scénario	Condition	Début	Fin	Type	Couche ciblée	Critère de sécurité impactée	Nº portion du graphe
1	Temps	50h	144h	*DoS*	**Couche numérique** : PLC2 en charge de l'envoi du niveau de réservoir l_1 au PLC1	Disponibilité	6
2	Temps	30h	144h	*Offset*	**Couche physique** : niveau de réservoir l_7	Intégrité	3
3	Niveau du réservoir n°3	$l_3 \leq 3$	144h	Injection de fausses données	**Couche physique** : arrêt des pompes PU4 et PU5	Disponibilité	9
4	Temps	50h	144h	Attaque par rejeu	**Couche numérique** : communication entre le PLC4 et le SCADA	Intégrité	9

En conséquence, l'automate PLC1 ne reçoit plus les valeurs du niveau du réservoir T1 et les opérations de pompages sont alors perturbées. Le contrôle des pompes par le PLC1 pourrait ne plus être en accord avec l'état réel du réservoir T1. L'attaque est arrêtée à la fin de la simulation, i.e. au bout de la 144ème heures de simulation ($t_{end} = 144h$).

Dans le **deuxième scénario** une attaque **physique** impactant le capteur de niveau de réservoir l_7 est injectée à $t_{start} = 30h$, et ce pour toute la durée de la simulation ($t_{end} = 144h$). Pour simuler un dysfonctionnement du capteur, un ***offset*** est ajouté sur les valeurs mesurées pour impacter leur*l'intégrité*. Les valeurs transmises au PLC5 et au SCADA, au travers du PLC9 qui recueille les données du capteur, ne sont plus en adéquation avec l'état réel du niveau de réservoir T7. Les pompes PU10 et PU11 pourraient être mises en service, ou arrêtées, à tort par le PLC5.

Dans le **troisième scénario** une attaque **physique** est simulée pour **forcer l'arrêt** des pompes PU4 et PU5 lorsque le niveau d'eau l_3 du réservoir T3 est inférieur ou égale à 3 m ($t_{start} = t_{l_3 \leq 3}$). La *disponibilité* des pompes est ainsi impactée, le réservoir T3 ne pourra plus être rempli grâce à l'activation des pompes par le PLC3. L'attaque s'achève avec la fin de la simulation ($t_{end} = 144h$).

Dans le **quatrième scénario** une **cyberattaque par rejeu** est perpétrée sur la liaison de communication **numérique** entre le PLC4 et le SCADA à $t_{start} = 50h$. Ce lien de communication est exclusivement utilisé pour le transfert des valeurs mesurées du niveau l_3 du réservoir T3 recueillies par le PLC4. L'attaque est composée de deux étapes : dans un premier temps l'attaquant espionne la communication pour enregistrer les valeurs de l_3 pendant un laps de temps $\Delta l = 5h$, puis il renvoie ces mêmes valeurs dans la liaison de communication en y ajoutant une composante aléatoire. L'attaque se termine avec la fin de la simulation ($t_{end} = 144h$).

III.3.7 Détection d'anomalie

La méthodologie de détection d'anomalie au sein du graphe est définie par 2 étapes :

1. La définition des métriques de détection d'anomalies.

2. Et leur intégration au sein du graphe.

Définition des métriques de détection d'anomalies

Divers composants interconnectés du réseau de distribution produisent des flux de données mesurables. Comme présenté précédemment, seules les pompes PU, les vannes V, et les réservoirs T, génèrent des données. Dans le cadre de cette étude, nous nous sommes donc exclusivement intéressés aux données produites par ces sous-systèmes physiques. Aucune donnée n'étant produite par les sous-systèmes numériques, ceux-ci ne sont pas pris en compte dans le processus de détection d'anomalies. Afin d'amorcer les différents processus d'évaluation de la propagation d'anomalies, il est indispensable dans un premier temps de détecter ces mêmes anomalies.

Dans ce cas d'étude, le choix des métriques d'analyse de la qualité est limité par les données issues de la simulation du réseau de distribution à partir des différents scénarios présentés. Seul un ensemble d'imperfections, de dimensions de la qualité peuvent être évaluées pour certains sous-systèmes physiques de *C-town*. Cette limitation d'étude des données produites par ces sous-systèmes est explicable par différents paramètres propres à la simulation :

— Seules des données issues de sous-systèmes physiques sont disponibles. Aucune donnée n'est issue de sous-systèmes numériques. La méthodologie de détection d'anomalies aurait pu être davantage aboutie si des données issues de la simulation des dispositifs numériques avaient été générées.
— Les données sont enregistrées à un intervalle de temps fixé par la simulation. En conséquence, aucune métrique d'analyse de la qualité en lien avec ce paramètre ne peut être prise en compte car il n'est pas affecté par les potentielles perturbations du réseau.
— Certaines caractéristiques propres aux sous-systèmes ne sont pas précisées ou ne sont pas simulées. Ce qui est, là aussi, un facteur limitant dans les possibilités de choix de métriques d'analyse de la qualité. Par exemple, certains paramètres propres à la confiance accordée aux différents capteurs de niveau ne sont pas connus, ou l'erreur inhérente à toute prise de mesure de capteur n'est pas simulée.

En considérant les différentes contraintes et limitations des données simulées, un ensemble de métriques a été identifié pour la détection d'anomalie au sein du réseau de distribution d'eau. Ces métriques sont issues des travaux de Pedro Merino Laso [Las17] dont la méthode d'évaluation de la qualité pour la détection d'anomalies a été présentée dans la section I.3.4.

Ces mesures d'analyse de la qualité sont regroupées en dimensions et présentées sous forme vectorielle. Comme présenté dans la section II.4.9, elles sont intégrées aux nœuds de variables système de la troisième couche du graphe généré. En raison des limitations associées à la simulation, nous nous sommes exclusivement intéressés à l'analyse de la qualité de l'information pour la détection d'anomalies au sein du réseau de distribution d'eau.

Nous avons ainsi évalué deux dimensions pour chaque pompe PU, une contextuelle et une extrinsèque :

— Dimension contextuelle : l'information est considérée comme **erronée**, et indiquée avec une valeur « $true$ », quand la valeur de son débit volumique n'est pas dans un état possible par rapport à la valeur de sa variable d'état. C'est-à-dire quand la pompe est allumée, sa variable d'état $e = 1$, et que son débit volumique f est égale à 0. Et inversement, si la pompe est éteinte ($e = 0$), son débit volumique f est supérieur à 0. Dans les cas contraires, cette dimension prend la valeur « $false$ ».

— Dimension extrinsèque : la **cohérence** de l'information est considérée comme « vraie », et indiquée avec une valeur « $true$ », quand la variable d'état de la pompe PU considérée respecte ses conditions de marche et d'arrêt en fonction du niveau l d'un réservoir T dont elle assure le remplissage. Si l'information n'est pas cohérente, elle est définie par une valeur « $false$ ».

Un exemple d'évaluation de la qualité de l'information d'une pompe PU est présenté ainsi :

$$\vec{IQV}_{PU(e)} = \left\{ \begin{array}{ll} \text{contextuelles} & \{cd_{err} = false\}, \\ \text{extrinsèques} & \{ed_{coh} = true\} \end{array} \right\} \tag{III.15}$$

Pour chaque réservoir T du réseau de distribution, une seule dimension contextuelle est étudiée. L'information du niveau de réservoir l est considérée **erronée** lorsque que sa valeur est égale à 0 ($l_T = 0$) ou supérieure au seuil maximal associé ($l_T > l_{max}$). La métrique associée est définie par une valeur « $true$ ». Dans le cas contraire, si les seuils de niveau sont respectés, elle sera indiquée avec une valeur « $false$ ». L'évaluation d'une unité d'information d'un réservoir T peut avoir un résultat d'évaluation comme le suivant :

$$\vec{IQV}_{T(l)} = \left\{ \begin{array}{ll} \text{extrinsèques} & \{ed_{coh} = true\} \end{array} \right\} \tag{III.16}$$

La méthodologie d'évaluation de la qualité de l'information est répétée pour chaque

pompe PU, et chaque réservoir T composant le réseau de distribution. Les règles opérationnelles qui régissent le contrôle des processus de remplissage des réservoirs sont définies par les seuils de niveau des réservoirs et les conditions de déclenchement des pompes et vannes. L'ensemble de ces règles est présenté dans la Table III.9.

TABLE III.9: Règles opérationnelles associées aux remplissages des réservoirs

	Seuil de niveau		**Conditions de déclenchement des pompes/vannes**	
Réservoir	**Minimum**	**Maximum**	**Marche**	**Arrêt**
T1	$l_{min} = 0\,\text{m}$	$l_{1_{max}} = 6.5\,\text{m}$	$e_{PU1} = 1$ si $l_{T1} < 4\,\text{m}$ $e_{PU2} = 1$ si $l_{T1} < 1\,\text{m}$	$e_{PU1} = 0$ si $l_{T7} > 6.3\,\text{m}$ $e_{PU2} = 0$ si $l_{T1} > 4.5\,\text{m}$
T2	$l_{min} = 0\,\text{m}$	$l_{2_{max}} = 5.9\,\text{m}$	$e_{V2} = 1$ si $l_{T2} < 0.5\,\text{m}$	$e_{V2} = 0$ si $l_{T2} > 5.5\,\text{m}$
T3	$l_{min} = 0\,\text{m}$	$l_{3_{max}} = 6.75\,\text{m}$	$e_{PU4} = 1$ si $l_{T3} < 3\,\text{m}$ $e_{PU5} = 1$ si $l_{T3} < 1\,\text{m}$	$e_{PU4} = 0$ si $l_{T3} > 5.3\,\text{m}$ $e_{PU5} = 0$ si $l_{T3} > 3.5\,\text{m}$
T4	$l_{min} = 0\,\text{m}$	$l_{4_{max}} = 4.7\,\text{m}$	$e_{PU6} = 1$ si $l_{T4} < 2\,\text{m}$ $e_{PU7} = 1$ si $l_{T4} < 3\,\text{m}$	$e_{PU6} = 0$ si $l_{T3} > 3.5\,\text{m}$ $e_{PU7} = 0$ si $l_{T4} > 4.5\,\text{m}$
T5	$l_{min} = 0\,\text{m}$	$l_{5_{max}} = 4.5\,\text{m}$	$e_{PU8} = 1$ si $l_{T5} < 1.5\,\text{m}$	$e_{PU8} = 0$ si $l_{T5} > 4.5\,\text{m}$
T6	$l_{min} = 0\,\text{m}$	$l_{6_{max}} = 5.5\,\text{m}$	Aucun actionneur impliqué	
T7	$l_{min} = 0\,\text{m}$	$l_{7_{max}} = 5\,\text{m}$	$e_{PU10} = 1$ si $l_{T7} < 2.5\,\text{m}$ $e_{PU11} = 1$ si $l_{T7} < 1\,\text{m}$	$e_{PU10} = 0$ si $l_{T7} > 4.8\,\text{m}$ $e_{PU11} = 0$ si $l_{T7} > 3\,\text{m}$

Intégration des métriques au sein du graphe

Une fois les mesures d'analyse de la qualité d'informations définies, celles-ci sont intégrées au sein de la troisième couche du graphe généré. Comme présenté dans la section II.4.9, cette intégration est réalisée par l'association des vecteurs d'évaluation de la qualité comme attribut des nœuds de variables système concernées.

Un exemple de cette intégration, au sein de la couche variable système de la portion nº 3 du graphe généré, est présenté dans la Figure III.15.

III.3.8 Pondération du graphe

Afin de fournir une pondération au graphe multicouche, il est nécessaire réaliser la méthode définie dans la section II.5.5. La méthode est basée sur l'évaluation du niveau de menace des sous-systèmes d'un CPS. Elle fournit pour chacun d'entre eux un poids représentatif

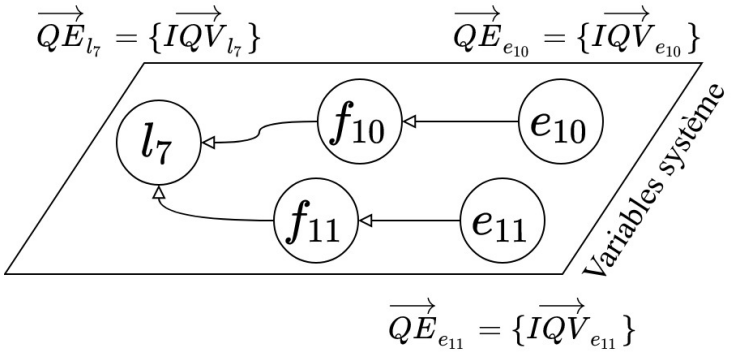


FIGURE III.15: Intégration de l'évaluation de la qualité dans le graphe généré

de leur appétence à propager une anomalie et à impacter les autres sous-systèmes avec lesquels ils interagissent.

L'emploi de la simulation entraîne des limitations inhérentes quant aux connaissances des composants hydrauliques et dispositifs numériques impliqués. Les informations à notre disposition concernant les éléments du réseau *C-town* nous obligent à prendre un certain nombre d'approximations pour réaliser la méthode d'évaluation. Celle-ci est uniformément réalisée pour chaque type de composant hydraulique et dispositif numérique, sans prendre en compte leur distinction opérationnelle dans les portions du réseau. Pour chaque sous-système, la cotation de chaque critère, ainsi que le niveau de menace qui en découle est défini dans la Table III.10.

À la fin du processus d'évaluation, on obtient le niveau de menace pour chaque nœud de sous-système composant le réseau de distribution d'eau. Ces niveaux de menaces sont directement intégrés au graphe sous forme d'attribut de pondération des relations entre sous-systèmes, partant du nœud considéré vers tous les autres. Un exemple de cette intégration est schématisé pour la portion du graphe n°3, impliquée dans le scénario n°2 (Figure III.16).

III.3.9 Résultats de l'évaluation de la propagation d'anomalies

D'après les 4 scénarios fonctionnels définis précédemment, différents résultats d'évaluation de la propagation des anomalies ont été obtenus. Ces évaluations, définies par deux processus distincts, ont été initiées par la détection de ces mêmes anomalies. Pour chaque scénario sont présentés les données du niveau de réservoir concerné et l'état de marche des pompes associées à son remplissage. Pour chaque scénario, les données du

TABLE III.10: Cotation des paramètres d'évaluation du niveau de menace des sous-systèmes du réseau de distribution d'eau

	Exposition				**Fiabilité cyber**				
	E_1		E_2		FC_1		FC_2		
Composant hydrauliques	$e_{1,1}$	$e_{1,2}$	$e_{2,1}$	$e_{2,2}$	$r_{1,1}$	$r_{1,2}$	$r_{2,1}$	$r_{2,2}$	**Niveau de menace**
Pompe	1/4	1/4	4/4	3/4	1/4	4/4	1/4	2/4	6.75
Vanne	1/4	1/4	4/4	3/4	1/4	4/4	1/4	2/4	6.75
Réservoir	1/4	1/4	4/4	3/4	1/4	4/4	1/4	3/4	6.25
Dispositifs numériques									
PLC	3/4	4/4	3/4	4/4	1/4	1/4	1/4	1/4	14
SCADA	4/4	4/4	4/4	4/4	1/4	1/4	1/4	1/4	16

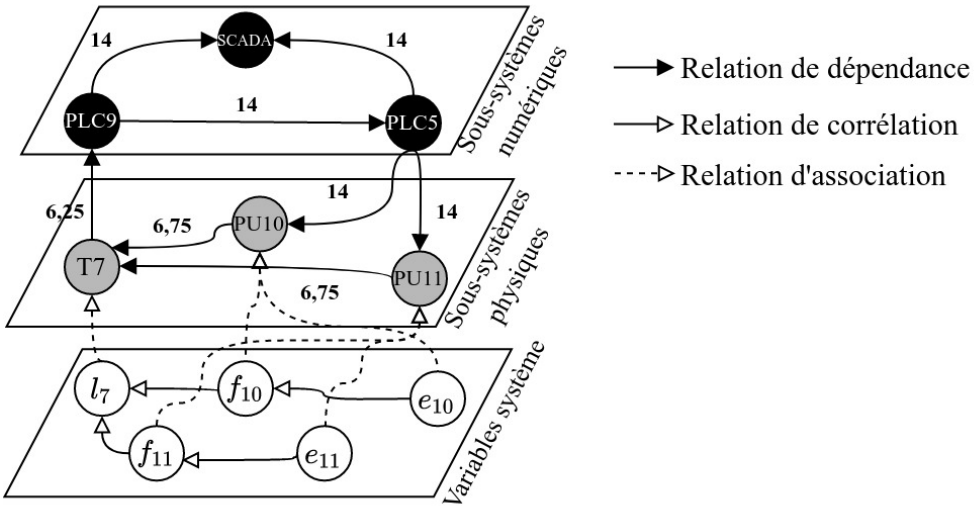


FIGURE III.16: Intégration du niveau de menace de propagation dans le graphe généré

niveau de réservoir concerné sont comparées avec celles issues du scénario en fonctionnement nominal dans les Figures III.17, III.18, III.19, et III.20. De même, les valeurs d'activation des pompes associées à chaque scénario sont comparées avec leurs valeurs nominales. Les graphiques obtenus sont présentés en Annexe C à partir des Figures C.4, C.5, C.6, et C.7

Dans le **premier scénario**, une attaque ***DoS*** à t = 50 h entraîne des changements d'état non conformes des pompes PU2 et PU1 par rapport au niveau de l_1 du réservoir

T1 (Figure C.4 en annexe C). Ceux-ci sont détectés par l'évaluation de la cohérence de l'information des pompes $ed_{coh}{=}false$ à $t = 57\,\text{h}$ et $t = 79.6\,\text{h}$. Ils constituent les premières étapes de propagation de l'anomalie. Chacune de ces détections initie les deux processus d'évaluation de la propagation. Comme présenté dans la Table III.11, les évaluations de la propagation sur les variables système caractérisent un impact possible sur le niveau l_1 du réservoir T1. Un débordement de T1 est ainsi détecté (étape de propagation 3) à partir de l'information erronée de son niveau ($l_1 \geq l_{1_{max}}$)à $t = 79,9h$. Le temps de vérification de l'impact de l'anomalie qui en résulte Δt est calculé comme suit : $\Delta t = t_2 - t_1 = 79.6 - 57 = 22.6\,\text{h}$ (Fig. III.17). Dans ce cas, l'estimation de l'impact de la propagation sur le réservoir T1 est confirmée 22.6 h plus tard. Différents chemins de propagation, avec des scores d'impact associés, sont calculés à chaque détection d'anomalie à partir du deuxième processus d'évaluation de la propagation. Les résultats obtenus sont présentés dans la Table III.12.

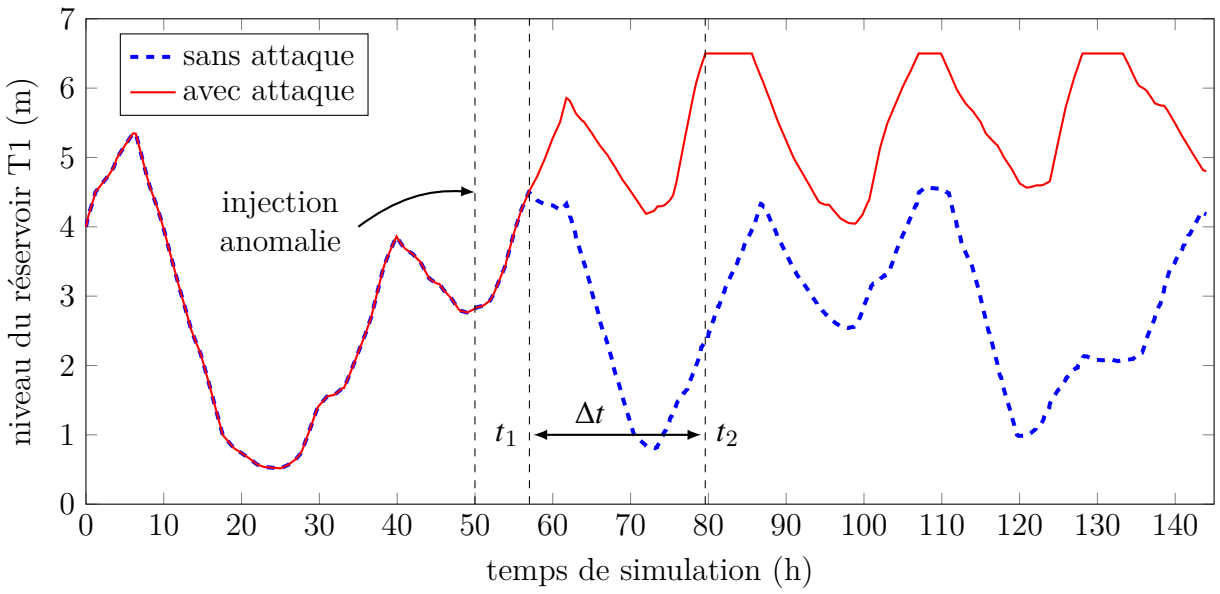


FIGURE III.17: Scénario 1, niveau du réservoir T1

Pour le **deuxième scénario**, un attaquant affecte l'intégrité du niveau l_7 du réservoir T7 en y ajoutant un ***offset*** constant de +2. Cette altération provoque des changements d'états non conformes des pompes PU10 et PU11 (Fig. C.5), contrôlées par le PLC5 en fonction des valeurs du niveau de réservoir transmises par le PLC9. Comme indiqué dans la Figure III.18, dès l'injection de l'anomalie celle-ci est détectée par l'évaluation de l'information erronée cd_{err} du réservoir T7 à $t = 30\,\text{h}$. À cause de *l'offset*, le niveau transmis est supérieur au niveau maximal acceptable ($l_7 \geq l_{7_{max}}$) tel que défini dans les règles de contrôles du système.

Dans le cadre du premier processus d'évaluation de la propagation, cette anomalie n'affecte aucune autre variable système (Tab. III.11). Différents chemins de propagation, et leurs *PIS*, sont néanmoins calculés (Tab. III.12) à partir du deuxième processus d'évaluation.

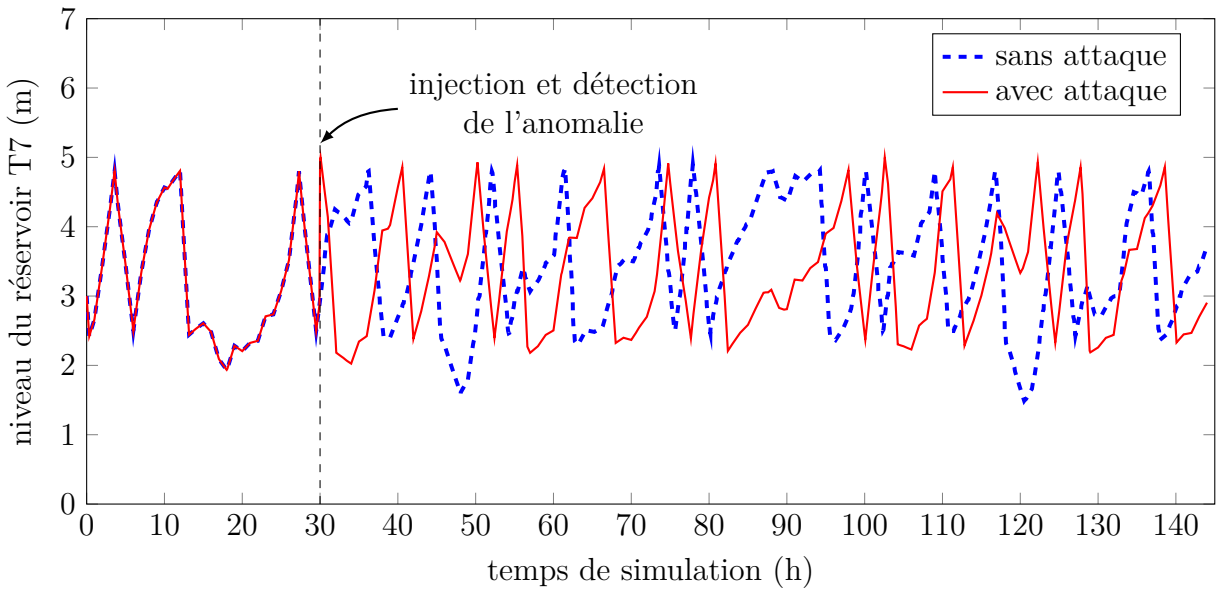


FIGURE III.18: Scénario 2, niveau du réservoir T7

Dans le **troisième scénario**, **une injection de fausses données** force un changement d'état non conforme des pompes PU4 et PU5 (Fig. C.6 en annexe C) lorsque le niveau l_3 du réservoir T3 est inférieur ou égale à 3 (Fig. III.19). Leur intégrité est ainsi affectée par cet état contraint qui diffère des besoins de contrôle du processus de remplissage du réservoir T3 auquel elles sont associées. Cette anomalie est détectée deux fois par l'évaluation de la cohérence de l'information des pompes PU4 et PU5 ($ed_{coh}{=}false$), respectivement à $t = 3.9\,\text{h}$ et $t = 11.3\,\text{h}$. Ces deux détections amorcent les processus d'évaluation de la propagation. Les premiers processus identifient un impact potentiel de l'anomalie sur le niveau l_3 du réservoir T3. Ultérieurement, un niveau de réservoir faible est détecté ($l_3 = 0$) à partir de l'évaluation de l'information $cd_{err}{=}true$ à $t = 13.7\,\text{h}$. L'impact potentiel sur l_3 calculé à $t_1 = 3.9\,\text{h}$ est confirmé à $t_2 = 13.7\,\text{h}$, soit $\Delta t = t_2 - t_1 = 9.8\,\text{h}$ après. L'ensemble des chemins de propagation, et les *PIS* associés, issus du deuxième processus d'évaluation de la propagation, sont présentés dans la Table III.12.

Le **quatrième scénario** est quant à lui composé d'une **attaque par rejeu**. À partir de $t = 50\,\text{h}$, les valeurs mesurées du niveau l_3 du réservoir T3 sont répétées dans la liaison de communication entre le PLC4 et le SCADA pendant les cinq premières heures jusqu'à la fin de la simulation. Le niveau du réservoir T3 au cours du scénario est présenté dans la

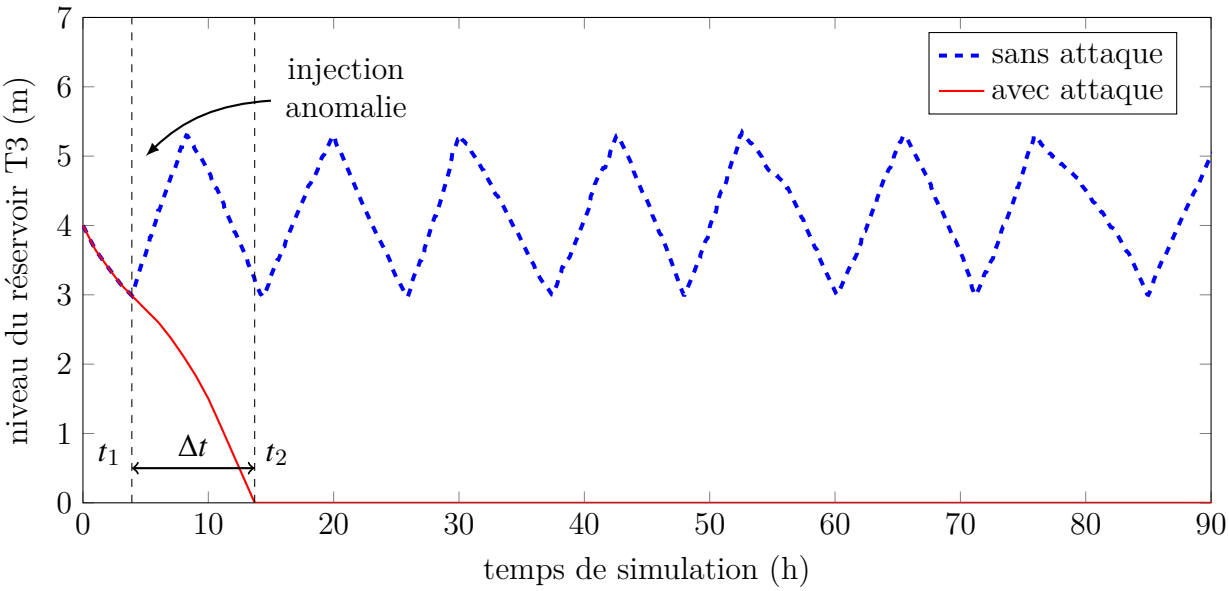


FIGURE III.19: Scénario 3, niveau du réservoir T3

Figure III.20. Les valeurs d'activations des pompes PU4 et PU5 lors du scénario d'attaque restent identiques à celles obtenues à partir du scénario en fonctionnement normal (Fig. C.7 en annexe C). Aucune anomalie n'est détectée, tant au niveau des métriques d'analyse de la qualité des données du réservoir, que celles associées pompes. Durant toute la durée de la simulation les états des pompes PU4 et PU5 sont cohérents par rapport au niveau l_3, qui lui reste compris dans sa plage de valeurs possibles ($l_{min} \leq l_3 \geq l_{3_{max}}$). En conséquence, aucune évaluation de la propagation d'anomalies n'est calculée pour ce scénario.

III.4 Outil informatique développé pour l'interaction avec le graphe

La méthode de génération du graphe multicouche est principalement basée sur un processus d'interaction entre un programme informatique, développé dans le cadre de nos travaux [PMLP21b], et un logiciel de gestion du graphe : **Neo4j**. Ce processus s'appuie sur un driver *API (Application Programming Interface)* développé par une solution de gestion de graphe : Neo4j. En amont de l'utilisation de cette solution, nous avons effectué un état de l'art des différents outils de gestion de graphes existants.

TABLE III.11: Résultats du premier processus d'évaluation de l'impact de la propagation pour chaque scénario

	Étape 1 de propagation de l'anomalie		Étape 2 de propagation de l'anomalie		Étape 3 de propagation de l'anomalie		AVIT
Scénario	Détection	PSV	Détection	PSV	Détection	PSV	Δt
1	ed_{coh} = false t = 57 h	$e_2 \rightarrow f_2 \rightarrow l_1$	ed_{coh} = false t = 79 h	$e_1 \rightarrow f_1 \rightarrow l_1$	cd_{err} = true t = 79.6 h	l_1	22.6 h
2	cd_{err} = true t = 30 h	l_7	n/a n/a	n/a	n/a n/a	n/a	n/a
3	ed_{coh} = false t = 3.9 h	$e_4 \rightarrow f_4 \rightarrow l_3$	ed_{coh} = false t = 11.3 h	$e_5 \rightarrow f_5 \rightarrow l_3$	cd_{err} = true t = 13.7 h	l_3	9.8 h

PSV : Propagation dans les variables systèmes (*Propagation on System Variables*)
AVIT : Temps de vérification d'impact de l'anomalie (*Anomaly Verification Impact Time*)

TABLE III.12: Résultats du deuxième processus d'évaluation de l'impact de la propagation pour chaque scénario

	Étape 1 de propagation de l'anomalie		Étape 2 de propagation de l'anomalie		Étape 3 de propagation de l'anomalie	
Scénario	Chemins de propagation	*PIS*	Chemin de propagation	*PIS*	Chemin de propagation	*PIS*
1	PU2-T1-PLC2-SCADA	27	PU1-T1-PLC2-SCADA	27	T1-PLC2-SCADA	20.25
	PU2-T1-PLC2-PLC1-SCADA	41	PU1-T1-PLC2-PLC1-SCADA	41	T1-PLC2-PLC1-SCADA	34.25
	PU2-T1-PLC2-PLC1-PU1-T1	47.75	**PU1-T1-PLC2-PLC1-PU2-T1**	47.75	**T1-PLC2-PLC1-PU1-T1**	41
	PU2-T1-PLC2-PLC1-PU2	41	PU1-T1-PLC2-PLC1-PU1	41	**T1-PLC2-PLC1-PU2-T1**	41
2	T7-PLC9-SCADA	20.25	n/a	n/a	n/a	n/a
	T7-PLC9-PLC5-SCADA	34.25				
	T7-PLC9-PLC5-PU10-T7	41				
	T7-PLC9-PLC5-PU11-T7	41				
3	PU4-T3-PLC4-SCADA	27	PU5-T3-PLC4-SCADA	27	T3-PLC4-SCADA	20.25
	PU4-T3-PLC4-PLC3-SCADA	41	PU5-T3-PLC4-PLC3-SCADA	41	T3-PLC4-PLC3-SCADA	34.25
	PU4-T3-PLC4-PLC3-PU5-T3	47.75	**PU5-T3-PLC4-PLC3-PU4-T3**	47.75	**T3-PLC4-PLC3-PU4-T3**	41
	PU4-T3-PLC4-PLC3-PU4	41	PU5-T3-PLC4-PLC3-PU5	41	**T3-PLC4-PLC3-PU5-T3**	41

PIS : Score d'impact de la propagation (*Propagation Impact Score*)
Les chemins en gras sont associés aux scores d'impact de propagation les plus significatifs pour chaque étape de chaque scénario.

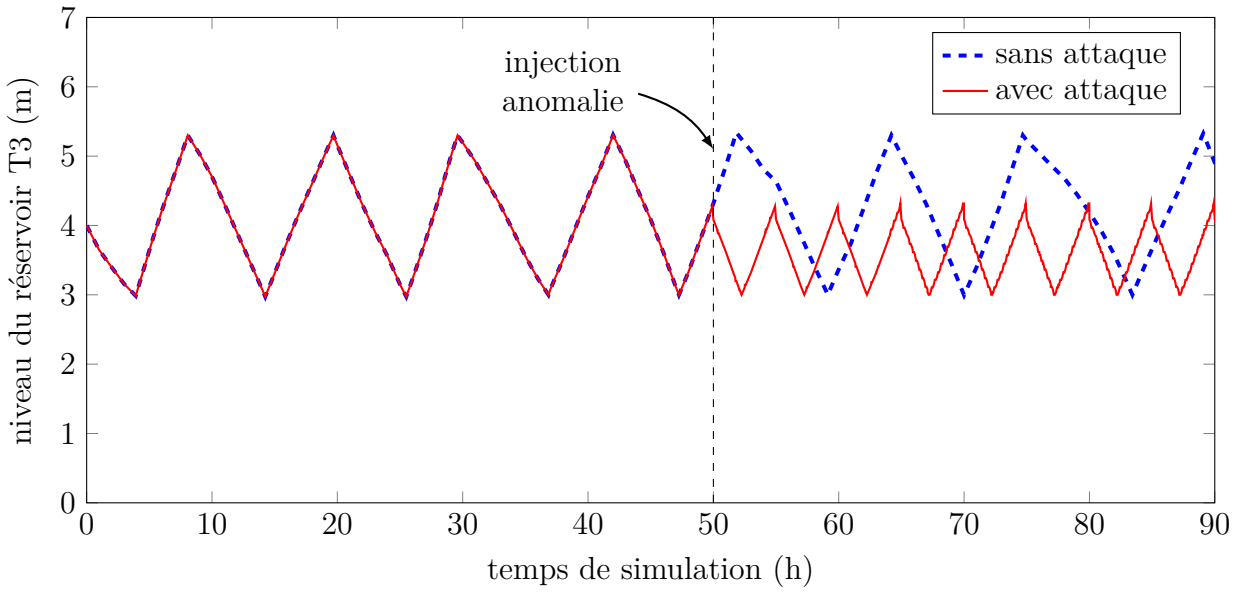


FIGURE III.20: Scénario 4, niveau du réservoir T3

III.4.1 Outils de gestion de graphes existants

La valorisation des données issues de graphes (*graph-based data*) nécessite l'emploi d'outils spécifiques. Ils permettent généralement de créer et générer le graphe, mais aussi d'explorer sa topologie pour en extraire diverses métriques d'analyses. Une multitude d'outils a déjà été développée et proposée pour cela. Ils se distinguent notamment par leur type de licence d'exploitation. Parmi ceux-ci on dénote notamment : *GraphBuilder*, *Titan*, *Apache Giraph*, *Naiad*, *GraphX*, *Gephi*, *Neo4j*, et bien d'autres encore [CFV21].

De par leurs propriétés inhérentes, et notamment pour leur licence *open-source*, nous avons plus particulièrement étudié les logiciels **Gephi** et **Neo4j**. Une comparaison de leurs caractéristiques, vis-à-vis de l'emploi que nous souhaitons en faire dans la suite de ces travaux, est présentée dans la Figure III.13

Le logiciel Gephi a été développé pour l'analyse de données à partir de graphe [BHJ09]. Il octroie à l'utilisateur une interaction avec la représentation du graphe ainsi que sa structure propre. Gephi propose les métriques les plus courantes pour l'analyse de graphe, et plus particulièrement de réseaux, comme le score de centralité, la détection de communauté au encore le chemin le plus court entre deux sommets. Il permet aussi une interaction avec les données du graphe au travers de filtres dynamiques visuels pour par exemple créer de nouveaux graphes à partir des résultats obtenus. Les atouts principaux de Gephi résident

néanmoins dans ses propriétés de la visualisation de graphe. Cela peut être à la fois employé pour la personnalisation de la représentation du graphe, pour mettre en avant diverses informations, mais aussi pour la visualisation de graphe dynamique qui évolue au cours du temps.

Neo4j est quant à lui une solution *NoSQL*[21] développée pour la gestion de bases de données sous forme de graphe [Mil13]. Contrairement aux bases de données traditionnelles qui organisent les données en lignes, colonnes et tableaux, Neo4j se caractérise par une structure flexible définie par des relations entre les données stockées. Le traitement et l'analyse de ces données s'effectuent à partir de requêtes conçues dans un langage informatique propre à Neo4j, le langage *Cypher*. Cet outil se distingue par une véritable suite logicielle qui recouvre toutes les applications possibles à partir de graphe. Une librairie est notamment proposée pour utiliser directement et simplement divers algorithmes basés sur la théorie des graphes [HN19]. De l'intégration à la visualisation, en passant par les différents outils d'analyse, l'ensemble du processus d'interaction avec le graphe est pris en compte. Un des atouts majeurs de cet outil réside dans les nombreuses API fournies pour intégrer Neo4j dans diverses applications et ainsi tirer profit de ses propriétés.

III.4.2 Procédures d'interaction avec le graphe

Comme présenté dans la Figure III.21, l'outil informatique développé se caractérise par deux types principaux de procédures d'interaction. Nous allons détailler plus précisément ces procédures dans cette section.

Première procédure d'interaction

Une première procédure d'interaction permet de générer le graphe sous Neo4j. Chaque élément de celui-ci doit être caractérisé dans le programme informatique en respectant le modèle défini dans la section II.4.3. On distingue dans cette définition les différents sous-systèmes s_i du CPS, ses variables v_k, ainsi que les différentes relations r_j et c_l associées. Dans cet exemple, chacune des relations est représentée comme un lien (symbolisé par « $\rightarrow$ ») entre deux nœuds. Un algorithme du programme informatique, exploitant le driver API de Neo4j, permet de transformer cette définition du système en graphe 3-couches visualisable et exploitable sur Neo4j. Le graphe est généré en adéquation avec les éléments structurels

21. Système de bases de données non relationnelles.

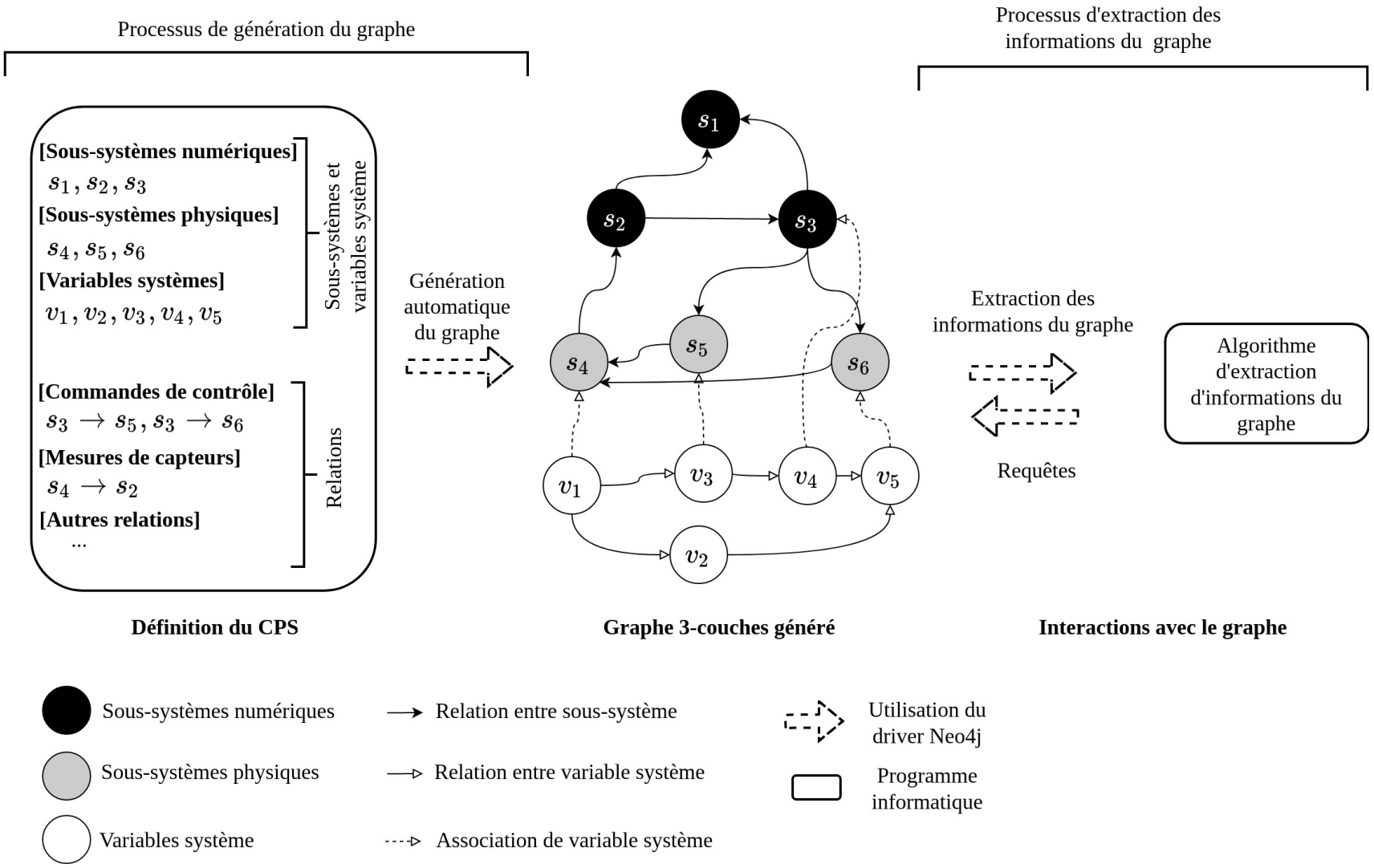


FIGURE III.21: Procédures d'interaction avec le graphe

TABLE III.13: Comparaison des logiciels étudiés pour l'utilisation de graphe

Attributs	Gephi	Neo4j
Interaction	Interface visuelle	Langage de requêtes propre à l'outil (Cypher)
Personnalisation du graphe	Algorithmes d'agencement, personnalisation des couleurs et tailles des éléments du graphe	Modifications possibles des couleurs, tailles et icônes des éléments du graphe
Analyse du graphe	Filtres dynamiques intégrés sans script	Langage de requêtes propre à l'outil (Cypher)
Algorithmes de graphe	Non	Librairie spécifique (*Graph Data Science library*)
Métriques proposées	Métriques courantes pour l'analyse de réseaux	Métriques courantes et algorithmes complexes pour tirer profit du graphe
Intégration	Interface de programmation	Interface de programmation, multiples drivers (.Net, Java, JavaScript, Go, et Python) et connecteurs à d'autres applications
Documentation	Bien documenté, forum d'utilisateur peu actif	Très bien documenté, forum d'utilisateurs très actif
Composants supplémentaires	Plugins[1] disponible	Plugins et applications disponibles

[1] : *Module d'extension*

définis précédemment.

Deuxième procédure d'interaction

Une deuxième procédure d'interaction octroie l'extraction de données et informations du graphe. Cela est aussi réalisé à partir d'un algorithme contenu dans le programme informatique développé exploitant le driver Neo4j. Sont alors extractibles différentes caractéristiques courantes du graphe, ainsi que diverses métriques obtenues avec des algorithmes plus ou moins complexes de la théorie des graphes. Ces algorithmes sont directement mis à disposition

dans Neo4j [HN19] ce qui facilite grandement leurs emplois. Nous distinguons principalement deux types d'utilisation des informations extraites pour l'analyse du graphe. Premièrement, des métriques et informations courantes sont extraites pour l'identification des nœuds et relations critiques. Deuxièmement, des métriques et informations sont utilisées au sein d'algorithmes plus poussées pour l'analyse profonde du graphe. Dans notre cas, ces informations sont extraites et utilisées pour l'analyse et l'évaluation de la propagation d'anomalies dans un modèle de graphe 3-couches. Deux exemples d'application de ces différents processus de génération et d'interaction ont été présentés dans les sections précédentes à partir de deux cas d'études.

III.5 Comparaison et positionnement par rapport à d'autres méthodes

Cette section positionne les travaux réalisés dans les domaines explorés. Tout d'abord, la méthodologie pour la modélisation structurelle d'un CPS sera comparée avec d'autres méthodes de modélisation présentées dans la section I.4.2 de l'état de l'art. Puis nous détaillerons le positionnement de nos travaux pour l'évaluation de la propagation d'anomalies dans les systèmes, en comparaison avec les méthodes existantes.

III.5.1 Comparaison avec d'autres modèles de représentation de système cyber-physique

Le modèle de représentation de CPS proposé à partir de nos travaux est distinguable en deux parties distinctes. Nous distinguons dans un premier temps la représentation structurelle des éléments principaux (physiques et numériques) qui composent le système, ainsi que les dépendances correspondantes. Deuxièmement, le modèle proposé permet la représentation des variables système, associées à ces éléments, et leurs dépendances. Il est donc plus pertinent de dissocier ces deux parties du modèle proposé pour les comparer à des travaux existants dans des domaines de recherches identiques.

Représentation des éléments du système

Parmi l'ensemble des travaux présentés dans la section I.4.2 traitant de la représentation structurelle des CPS et de leurs dépendances, un modèle est particulièrement adapté pour le comparer à celui que nous proposons. Le modèle fourni par Koosha Marashi *et al.* octroie la représentation des éléments du CPS et des intra dépendances qui le composent [MSH16]. De nombreuses caractéristiques diffèrent pour ces deux modèles et sont présentées dans la Table III.14.

TABLE III.14: Comparaison avec un autre modèle pour la représentation des éléments d'un CPS

	Modèles	
Caractéristiques	[MSH16]	Cette thèse
Type de graphe	Multicouche, orienté et pondéré	Multicouche, orienté et pondéré
Nombre et types de couches	2 types de couches : -Cyber -Physique	3 types de couches : -Numérique -Physique -Variables
Nœuds	2 types : -Cyber -Physique	3 types : -Numérique -Physique -Variable
Relations	4 types : -Physique→Cyber -Cyber→Physique -Physique→Physique -Cyber→Cyber	3 types : -Sous-système→Sous-système -Variable→Variable -Variable→Sous-système
Définition de la pondération	Degré d'influence (subjectif)	Évaluation des risques (objectif)
Intégration de méthode de détection	Non	Oui
Cas d'études	CPS de distribution d'électricité	CPS maritimes

Ce modèle, basé sur un graphe orienté et pondéré, est composé de 2 couches principales (cyber et physique). De même, les sous-systèmes du CPS sont représentés sous forme de

nœuds (cyber ou physique) et les dépendances sont définies à partir de 4 types principaux pour caractériser l'influence d'un sous-système sur un autre. Le modèle de représentation de CPS que nous proposons dans ces travaux de thèse est lui aussi fondé sur un graphe orienté et pondéré. À la différence que celui-ci est composé de 3 couches. Les caractéristiques des deux premières couches (numérique et physique) sont similaires à celles du modèle comparé. La troisième couche intégrée dans notre représentation permet une caractérisation et une analyse des dépendances entre les variables du CPS étudié. De plus, elle rend possible l'intégration de métriques issues de diverses méthodes de détection. Trois types de nœuds sont distinguables dans le modèle proposé : deux associés aux sous-systèmes du CPS (numérique ou physique), et un troisième pour les variables du système. Ces nœuds sont liés entre eux à partir de 2 types de dépendances : entre sous-systèmes et entre variables. À cela s'ajoutent les différentes relations d'associations entre variables et sous-systèmes.

Ces deux modèles se différencient principalement par la méthode de pondération du graphe utilisée. Koosha Marashi *et al.* définissent la pondération des arêtes du graphe à partir d'une variable de « degré d'influence », comprise dans l'intervalle $[0, 1]$, et traduisant quantitativement l'influence d'un sous-système sur un autre. Ce poids est fixé de manière **subjective** à partir des connaissances d'un expert, de retour d'expériences ou de simulations, ou encore grâce à diverses informations extérieures. *À contrario*, la méthode de pondération proposée dans ces travaux de thèse s'appuie sur une évaluation quantitative de la criticité des sous-systèmes à partir d'une évaluation multicritère du niveau de menace. Bien que celle-ci doit être réalisée par un expert du domaine, cette méthode se caractérise par son **objectivité**. Plus la criticité d'un sous-système est élevée, plus les dépendances qui en résultent le sont également.

Enfin, les deux modèles se distinguent par leurs cas d'études d'application. Koosha Marashi *et al.* ont uniquement étudié des CPS liés à la distribution de l'électricité [MSH17]. Tandis que pour illustrer le modèle proposé, nous l'avons confronté à deux cas d'études de CPS maritimes critiques [PLP20], [PMLP21a].

Représentation des variables d'un CPS

Un modèle de représentation des variables d'un CPS sous forme de graphe est particulièrement adapté pour la comparaison avec celui que nous proposons dans ces travaux de thèse. John H Castellanos *et al.* ont utilisé un graphe orienté non pondéré pour représenter les différentes dépendances entre les variables d'un système cyber-physique [COZ18]. Un

Data Flow Graph (DFG)[22] est automatiquement généré à partir du programme embarqué d'un PLC contenant diverses variables du système. Les différences entre les caractéristiques de ce modèle, et celui proposé dans cette thèse sont présentées dans la Table III.15.

TABLE III.15: Comparaison avec une autre modèle pour la représentation des variables d'un CPS

	Modèles	
Caractéristiques	[COZ18]	Cette thèse
Type de graphe	Orienté, non-pondéré	Orienté, non-pondéré
Nœuds	Variable	Variable
Relations	2 types : -lien fort -lien faible	2 types : -structurelle -opérationnelle
Utilisation de Neo4j	Oui	Oui

Ce graphe est composé d'un ensemble de nœuds représentant les différentes variables employées dans le système. Les arêtes entre ces nœuds illustrent des dépendances explicites ou implicites entre les variables. Ces dépendances sont respectivement qualifiées de « lien fort » et « lien faible ». Dans le modèle proposé à partir de ces travaux de thèse, les variables du CPS et leurs dépendances sont elles aussi représentées sous forme de graphe orienté non pondéré. Tout comme dans le modèle comparé, les variables sont définies sous forme de nœuds et deux types de dépendances les lient entre elles.

Dans le modèle proposé par John H Castellanos *et al.* les sous-systèmes auxquels sont associées les variables ne sont pas représentés. Ce qui signifie que l'analyse de l'impact de la propagation d'une anomalie sur le système ne se fera qu'au travers de ses variables. Or un CPS est composé d'une multitude de sous-systèmes qui ne sont pas forcément associés à une variable. De ce fait la modélisation du CPS proposée dans cette thèse combine la représentation des sous-systèmes, des variables, et des diverses dépendances pour fournir un outil d'analyse le plus complet possible.

22. Graphe de flux de données

III.5.2 Comparaison de l'approche par rapport aux autres méthodes d'évaluation de la propagation d'anomalies

L'approche proposée dans ces travaux de thèse permet d'évaluer quantitativement des chemins potentiels de propagation d'anomalies en se basant sur un modèle spécifique de représentation de graphe. Georgios Kavallieratos *et al.* ont formulé une méthode similaire pour analyser les différents chemins de propagation d'une attaque visant une boucle système d'un C-ES composé de différents CPS [KK20]. Les caractéristiques de cette méthode sont comparées avec celle que nous proposons dans la Table III.16.

TABLE III.16: Comparaison avec un autre méthode d'évaluation de la propagation d'anomalies

	Modèles	
Caractéristiques	[KK20]	Cette thèse
Perspective du système étudié	Externe	Externe et interne
Type de graphe	Orienté	Multicouche, orienté et pondéré
Intégration de la méthode de détection	Non	Oui
Pondération du graphe	Méthode d'évaluation des risques DREAD[1]	Évaluation du niveau de menace (section II.5.5)
Nombre de critères	4 critères (3 niveaux d'évaluation)	2 critères, chacun composé de 2 paramètres (4 niveaux d'évaluation)
Algorithme de graphe utilisé	*DFS*	*DFS*
Évaluation quantitative des chemins	*Attack Path Importance*	*PIS*
Cas d'études maritimes	CPSs pour la navigation	CPS de propulsion CPS de gestion de l'eau

[1] : *Damage, Reproducibility, Exploitability, Affected users, and Discoverability*

La méthode proposée par Georgios Kavallieratos *et al.* repose sur un modèle de graphe orienté permettant de représenter les dépendances **externes** entre différents CPS. Celle-ci présente de nombreuses différences par rapport au modèle de graphe que nous proposons

dans ces travaux. Celui-ci octroyant la représentation des dépendances **internes** d'un CPS en y intégrant diverses métriques de détection d'anomalies.

Ces deux méthodes bénéficient de pondération de graphe différente, basées sur l'évaluation de la criticité des éléments du système. Georgios Kavallieratos *et al.* se basent sur la méthode *DREAD*, à partir de 4 critères composés de 3 niveaux d'évaluation. Concernant la méthode développée et utilisée dans ces travaux, celle-ci présente davantage de critères et de niveaux d'évaluation. Nous l'avons détaillée dans la section II.5.5.

Aussi, les deux méthodes calculent les divers chemins de propagation à partir de l'algorithme de *DFS*. Ces chemins sont aussi évalués quantitativement dans chacune d'entre elles. À partir d'une métrique *Attack Path Importance* pour la méthode de Georgios Kavallieratos *et al.*, et grâce au *PIS* dans celle que nous proposons.

Enfin, il est important de souligner que c'est deux méthodes sont illustrées à partir de cas d'études maritimes. Ce qui est particulièrement intéressant pour leur comparaison.

III.6 Conclusion

Deux cas d'étude de CPS critiques ont été étudiés : un prototype de CPS maritime, et un réseau de distribution d'eau *intelligent*. Cela nous a permis de confronter les différentes approches proposées dans le Chapitre II.

Pour chaque cas d'étude, nous avons modélisé et généré le graphe associé au système étudié, ainsi que choisi et intégré les différentes métriques d'évaluation de la qualité pour la détection d'anomalies. Plusieurs scénarios d'expérimentations composées d'attaques réalistes ont été identifiées et testées. Dans le premier cas d'étude, les résultats obtenus ont permis de mettre en avant l'apport de la modélisation sous forme de graphe quant à la modélisation des CPS et de ses dépendances. Ces premiers résultats positifs ont confortés le choix d'orientation de notre approche, tout en soulignant les parties à examiner et développer davantage. Dans le deuxième cas d'étude, nous avons évalué la propagation d'anomalie au travers de différents processus unitaires et globaux. Les résultats obtenus ont conduit à la validation de la méthode d'évaluation de la propagation d'anomalies proposée dans le cadre de cette thèse.

Nous avons pu observer comment la combinaison d'une méthodologie de modélisation à différents processus d'évaluation des risques de propagation conduisent à l'obtention d'une méthode d'évaluation de propagation d'anomalies adaptée aux CPS maritimes.

Chapitre IV

Conclusion générale et perspectives

Sommaire

IV.1 Problématique

Le secteur maritime représente actuellement une valeur économique, stratégique, et politique immense dont la criticité ne cesse, et ne cessera de s'accroître. Du transport de fret à la projection de forces militaires, en passant par la pose de câbles sous-marins, différents types de navires sont employés dans la réalisation des missions associées à ce secteur d'activité. Ils se distinguent par l'utilisation de divers systèmes maritimes hétérogènes permettant d'assurer l'ensemble de leurs fonctions, plus ou moins vitales. De par les contraintes inhérentes au domaine d'application, ces systèmes se caractérisent par un fort niveau de dépendance. La défaillance de l'un d'entre eux peut ainsi potentiellement impacter l'ensemble du navire à partir d'une défaillance en cascade. En conséquence, la problématique des dépendances associée aux systèmes maritimes doit être particulièrement considérée, et ce à partir de différentes perspectives, pour répondre à l'ensemble des besoins associés.

Certains systèmes d'information maritimes sont des cas particuliers de CPS. Ils se distinguent par leur dualité entre le monde physique et numérique et sont notamment employés

pour assurer des fonctions vitales du navire. De par leurs doubles surfaces d'attaque, les CPS sont particulièrement vulnérables à différents types d'attaque. En raison du fort niveau de dépendances de ces systèmes, les anomalies injectées peuvent alors se propager dans le navire et engendrer des conséquences critiques. C'est pourquoi une modélisation des dépendances, intra et inter CPS, est primordiale. De plus, l'analyse quantitative des différents chemins potentiels de propagation est nécessaire pour les comparer, évaluer leur criticité, et analyser l'effet des possibles solutions mises en oeuvre pour limiter l'impact de la propagation des anomalies.

Nous avons initialement identifié trois questions de recherche, et une question de développement, relatives à la problématique de cette thèse : la notion de dépendance dans un navire (QR1), la modélisation structurelle d'un CPS et ses dépendances associées (QR2), l'évaluation de la propagation d'anomalie dans un CPS (QR3), et l'automatisation des solutions proposées au travers d'un outil informatique pour répondre aux questions précédentes (QD1).

IV.2 Travaux réalisés

Ces travaux de thèses ont été le résultat de recherches mises en oeuvre pour répondre de manière appropriée à la problématique de propagation d'anomalies dans les **systèmes cyber-physiques maritimes** comme conséquence induite de leur caractéristique de fort niveau de **dépendance**. De ce fait, il était primordial de définir dans son ensemble ce domaine d'activité, et plus particulièrement les spécificités et contraintes des systèmes associées aux navires, pour mieux comprendre la problématique de dépendance.

Pour répondre à cette problématique, en accord avec la question de recherche QR1, nous avons dans un premier temps défini le cadre de recherche en caractérisant la notion de dépendance au sein d'un navire. Cela a permis d'identifier différentes couches de dépendances entre les systèmes maritimes, notamment par rapport à la notion de perspective interne et externe d'un système. La représentation générique des dépendances entre systèmes maritimes a permis de mieux appréhender et caractériser les dépendances des CPS d'un navire.

Par la suite, nous avons répondu à la QR2 en proposant une méthode de modélisation des CPS basée sur la théorie des graphes. Le modèle de graphe orienté multicouche développé fournit une solution adaptée quant à la visualisation et la formulation mathématique du problème de dépendance au sein des CPS. De surcroît, le modèle de graphe proposé se

caractérise par sa généricité. Ce qui en fait une solution de modélisation viable pour d'autres domaines d'application traitant du problème de dépendance dans les CPS.

Pour répondre à la QR3, nous avons proposé une méthode d'évaluation quantitative des chemins de propagation dans un CPS. La méthode proposée se distingue par deux différents processus d'évaluation des chemins de propagation en adéquation avec le modèle de graphe généré à partir de la QR2. Ces deux processus se basent notamment sur un algorithme de parcours de graphe.

Afin de favoriser la mise en oeuvre des solutions proposées pour les questions de recherche QR2 et QR3, nous avons développé un outil informatique basé sur le logiciel de gestion de graphe Neo4j (QD1). Cet outil facilite le processus d'interaction avec le graphe généré à partir de deux types de procédures distinctes. Le premier type de procédure permet de simplifier la création du graphe défini à partir des caractéristiques du CPS étudié. Tandis que le deuxième type permet d'extraire diverses métriques du graphe pour les intégrer au sein d'une analyse externe.

Enfin, la méthode proposée a été confrontée à deux cas d'études maritimes différents. Le premier cas d'étude de prototype de CPS du *Naval Cyber Range* a permis d'illustrer la cohérence du modèle de graphe proposé pour la représentation des dépendances dans un CPS, ainsi que les possibilités d'analyse topologique qui en résultent. Le deuxième cas d'étude de réseau de distribution d'eau *C-town* nous a permis de confirmer la cohérence du modèle de graphe, tout en illustrant les possibilités offertes pour l'évaluation des chemins de propagation d'anomalies. L'implémentation de la méthode proposée à des CPS caractérisés par des fonctions totalement différentes, bien que relatives au maritime, souligne la généricité de celle-ci.

À partir de l'ensemble de résultats présentés, nous considérons que la méthodologie proposée fournit une approche appropriée pour l'évaluation de la propagation d'anomalies dans les CPS. La structure de l'approche fait que chaque élément la constituant peut être particularisé, ou traité indépendamment, selon les besoins de l'application souhaitée. Le travail réalisé représente ainsi une première étape pour la résolution de la problématique des dépendances dans les systèmes maritimes, et plus généralement dans les navires.

IV.3 Discussion

Les solutions énoncées répondent aux problèmes associés aux questions de recherche initialement définies, néanmoins, elles sont associées à divers verrous scientifiques toujours existants et comportent un certain nombre de limitations. Dans cette section, nous présentons un certain nombre de ces limitations à partir d'une discussion de l'ensemble des résultats obtenus, tant au niveau de la méthodologie proposée que son application aux cas d'étude.

Le modèle de **graphe orienté multicouche** développé pour répondre à la problématique de cette thèse se caractérise par sa généricité. Il est particulièrement adapté pour représenter des CPS utilisés pour le contrôle de processus industriels. Or comme il a été détaillé dans la solution pour la QR1, un navire est défini par un nombre important de systèmes hétérogènes, tant par leur nature que par leur fonction. Les CPS ne représentent donc pas l'intégralité des systèmes employés à bord. Le modèle de graphe proposé n'est pas forcément adapté à tous les systèmes maritimes, notamment ceux en lien avec l'*Information Technology*. En conséquence il serait nécessaire d'adapter le modèle aux besoins et spécificités de ce type de système employés à bord.

La définition des caractéristiques du modèle de graphe, en adéquation avec la QR2, est elle aussi discutable. La définition des sommets du graphe du CPS étudié, ainsi que ses arêtes, nécessite une bonne connaissance architecturale de celui-ci. Cette définition est primordiale pour les diverses analyses qui vont résulter de ce même graphe. Or cette connaissance n'est pas, ou pas assez, explicitée. Nous en avons fait notamment l'expérience dans notre recherche de *dataset* où les dépendances entre sous-systèmes étaient rarement caractérisées. À l'échelle globale d'un navire, cette limitation est d'autant plus exacerbée. Tout au long de son cycle de vie, l'architecture réseau d'un navire est en constante évolution sans que les modifications soient forcément explicitées à partir d'une cartographie et archivées dans une solution documentée. Cela est notamment dû à la complexité intrinsèque de l'architecture, mais surtout, aux interventions d'une multitude de sous-traitants lors des phases de maintien en condition opérationnelle.

La solution fournie pour répondre à la QR3 s'appuie majoritairement sur un algorithme de parcours du graphe qui fournit les chemins de propagations, composés des sous-systèmes traversés, ainsi que le score d'impact total obtenu à partir de la pondération des arêtes parcourues. La méthode de pondération du graphe est donc partie prenante dans l'évaluation résultante, et donc dans la solution proposée. À partir de l'étude de l'état de l'art traitant des dépendances associées aux CPS, il a été constaté que deux méthodes principales de

pondération étaient utilisées. Un premier type de méthode évalue la criticité topologique de chaque sommet du graphe pour la reporter sur les arêtes sortantes de ces mêmes sommets. Tandis que le deuxième type de méthode s'appuie sur une évaluation définie par une connaissance externe (expertise, retour d'expérience, simulation, etc.). Plutôt que de développer une méthode de pondération propre aux dépendances d'un CPS, nous avons fait le choix de définir cette pondération à partir d'une évaluation du niveau de menaces des sous-systèmes le composant et de la reporter sur les dépendances résultantes. Bien que cela soit discutable, nous avons fait le parti pris de se placer du point de vue du sous-système pour évaluer son importance en fonction de ses connexions, mais aussi de ses caractéristiques inhérentes et son rôle opérationnel. Cette méthodologie s'appuie sur la cotation de métriques issues de critères adaptées aux caractéristiques des CPS. Comme toute composante d'une évaluation des risques, la réalisation de celle-ci nécessite une connaissance certaine du système étudié pour fournir une analyse représentative. Aussi, la pertinence de l'algorithme de *DFS*, utilisé pour obtenir les chemins potentiels de propagation, est discutable quant à son utilisation pour des graphes de taille plus importante. Les temps de calcul associés au parcours du graphe pourraient ne pas être adaptés aux besoins de réponse en temps réel des CPS.

Concernant l'outil informatique développé en adéquation avec la QD1, il permet de faciliter l'implémentation des solutions aux QR2 et QR3 mais présente certaines limitations dans son utilisation. Premièrement, une connaissance minimale du langage Cypher (langage spécifique à Neo4j) est requise pour personnaliser l'utilisation de l'outil dans une application spécifique. Deuxièmement, la définition du système étudié dans l'outil peut s'avérer complexe lorsque celui-ci se distingue par un grand nombre de sous-systèmes et dépendances associées. Il en résulte alors un graphe dont la visualisation n'est pas au plus optimisée. Afin de répondre à l'ensemble de ces problèmes, il serait nécessaire d'intégrer d'autres modules complémentaires pour faciliter davantage la caractérisation du système, ainsi qu'améliorer sa représentation dans l'outil. Cela pourrait être réalisé au sein d'une solution informatique générique et standardisée.

L'approche proposée a été validée grâce à deux *datasets* représentant des CPS employés dans le domaine d'application maritime. Chacun des cas d'étude a seulement été confronté à une quantité réduite de scénarios d'expérimentations (4 pour chacun d'eux) dans un environnement contrôlé, pour le premier, et simulé pour le second. De plus, chacun des scénarios réalisés ne comprenait qu'une seule anomalie. Ce qui facilite grandement sa détection, et l'ensemble des analyses de propagation qui en résultent. Concernant le premier cas d'étude, le nombre de sous-systèmes et de variables du prototype de CPS n'a pas permis de confron-

ter notre méthodologie à une génération et une étude de graphe de taille importante. Cette limitation est commune au deuxième cas d'étude de réseau de distribution d'eau *intelligent*. Même si le graphe global obtenu totalise 60 noeuds et 68 arêtes, cela est encore trop peu pour l'associer aux problématiques des graphes de grande taille. Concernant les résultats d'évaluation de la propagation d'anomalie, nous avons pu constater que les scores d'impacts obtenus pour chaque chemin étaient plutôt proportionnels au nombre de sous-systèmes parcourus. Cela pourrait s'expliquer en partie par la méthode de pondération. En effet, celle-ci se base sur une échelle de cotation de critères spécifiques aux CPS. Cette échelle de cotation, ainsi que la mise en équation des valeurs qui en résultent, devrait être améliorée pour fournir une évaluation quantitative plus significative. Une autre possibilité serait que la connaissance du système étudié n'est pas suffisante pour définir les métriques de cotations et ainsi obtenir une pondération réaliste. Les travaux de Georgios Kavallieratos, traitant de l'évaluation quantitative des chemins de propagation inter CPS, ont permis de mettre en avant cette même observation dans les scores de chemins obtenus [KK20]. Ce qui corrobore l'importance d'une définition de pondération de graphe adaptée et représentative. Notamment lorsque diverses analyses résultent de celle-ci.

Divers verrous scientifiques, associés aux travaux réalisés, sont encore à considérer. Cela implique notamment l'intégration de la contextualisation des anomalies détectées pour affiner l'estimation de l'impact de leur propagation. Aussi, afin de répondre à la problématique de la détection et d'évaluation de la propagation en temps réel, il est nécessaire de reconsidérer divers aspects de la méthodologie proposée pour les adapter aux contraintes d'analyses inhérentes. Cela concerne le modèle de graphe, sa pondération, les moyens mis en place pour la détection d'anomalies, ainsi que les solutions algorithmiques d'étude de la propagation. Enfin, l'ensemble de la méthodologie formulée se base sur l'expertise de l'utilisateur et sa connaissance des systèmes étudiés. Cet aspect des travaux exprimés dans cette thèse peut ainsi engendrer des variabilités dans les évaluations de propagation obtenues.

IV.4 Perspectives

Grâce à la diversité des problèmes étudiés, ainsi qu'aux travaux réalisés dans cette thèse, les perspectives résultantes de ce travail sont multiples et variées. Comme cela a été détaillé dans les sections précédentes, l'approche proposée pour l'évaluation de la propagation d'anomalies dans les CPS maritimes a engendré la formulation et la considération de diverses autres problématiques ayant un impact majeur sur le sujet d'étude initial. Par conséquent, il

apparaît comme une évidence que le modèle proposé, ainsi que l'ensemble des problématiques identifiées, doit être davantage approfondi.

Les travaux réalisés pour répondre à la QR1 ont fait émerger les besoins de représentation et analyses des différentes couches de dépendances entre les éléments d'un navire. Dans cette thèse, nous avons proposé une modélisation des dépendances des CPS. Ce qui ne représente qu'une partie de la solution nécessaire. D'autres modèles devraient être développés pour couvrir la totalité des besoins associés à cette problématique. L'ensemble de ces modèles pourraient être unifiés à partir d'un méta modèle de représentation des dépendances dans un navire. En complément, il serait nécessaire de considérer d'autres types de dépendances que celles entre systèmes. Par rapport aux conséquences critiques qu'elles induisent, les dépendances liées aux opérateurs humains seraient par exemple primordiales à traiter [PSHB20]. En adéquation avec l'évolution du secteur maritime et des systèmes employés, il semble également nécessaire d'accentuer l'identification et la modélisation des dépendances d'un navire donné avec d'autres systèmes externes. Cela devrait être réalisé de manière adaptative en accord avec les missions du navire. Le secteur maritime civil est notamment concerné avec la démocratisation de systèmes autonomes. Le secteur maritime militaire est tout autant concerné avec l'utilisation de véhicules sans pilote, mais aussi de par l'emploi accru de la Veille Coopérative Navale. Cette nouvelle stratégie opérationnelle, basée sur l'échange d'informations, accentue les capacités de connaissance de la situation tactique au sein d'une force navale.

Les éléments de réponse proposés pour la QR2 se caractérisent par leur généricité. Le modèle de graphe orienté multicouche pourrait être amélioré en définissant des types de relations additionnelles, de même que des noeuds, pour être adapté à d'autres cas d'application que l'étude de la problématique des dépendances dans un CPS maritime. Cela se traduirait par l'ajout de couches supplémentaires dans le modèle proposé. Par exemple, une couche supplémentaire représentant les divers processus métier pourrait être intégrée. Ces différents processus, représentés sous forme de noeuds, seraient associés à des missions spécifiques du navire. Les relations entre ceux-ci seraient alors représentatives des différentes dépendances existantes. Cela améliorerait notamment la représentativité de l'information à l'opérateur concerné. Des éléments de réponses à cette perspective ont déjà été formulés dans des travaux de Gabriel Jakobson où un graphe multicouche est proposé pour modéliser les dépendances entre éléments d'un CPS et ses missions [Jak11]. Comme nous l'avons défini dans le paragraphe précédent, l'ajout d'une couche spécifique à l'humain serait tout aussi important. Un opérateur intervenant sur le CPS pourrait être modélisé sous forme de noeud

spécifique, et son lien de dépendance vis à vis du système sous forme de relation. Ces quelques perspectives corroborent l'aspect polyvalent du modèle de graphe multicouche proposé dans ces travaux de thèse.

L'approche développée, en adéquation avec les besoins associés à la QR3, fait elle aussi émerger diverses perspectives de travaux futurs potentiels. La méthodologie de pondération du sous-graphe des sous-systèmes du CPS pourrait être améliorée en y intégrant une évaluation topologique de ses éléments. Des métriques issues de la méthode d'évaluation fournie par Aida Akbarzadeh *et al.* pourraient par exemple être utilisées [AK20]. Cette méthode s'appuie sur la théorie des graphes pour évaluer les composants critiques d'un CPS. En complément des métriques statiques, des métriques d'évaluation dynamique, telles que l'évaluation de la *confiance* [Las17], pourraient être intégrées pour fournir une pondération en temps réel. Il faudrait alors formuler une équation adaptée pour combiner les scores obtenus des diverses évaluations. Le graphe obtenu serait alors qualifié de *graphe dynamique*, avec toutes les caractéristiques et contraintes qui en incombent. Diverses méthodes de pondération devraient être développées pour chaque couche spécifique du modèle. Par exemple, les relations de dépendances entre les noeuds de variables système pourraient être pondérées à partir de coefficients de corrélation. Aussi, les algorithmes de graphe utilisés pour obtenir les potentiels chemins de propagation devraient considérer les types des relations parcourus pour adapter l'évaluation de la propagation. Enfin, il serait primordial de pouvoir anticiper l'évolution et l'impact de la propagation d'anomalie dans le temps. Pour cela, diverses méthodes d'apprentissage automatique pourraient être formulées pour fournir des indicateurs de propagation pertinents à l'opérateur concerné. L'évaluation dynamique de la propagation d'anomalies qui en résulterait serait alors plus complète et représentative vis-à-vis des besoins majeurs liés à cette problématique.

Une perspective majeure de nos travaux est directement associée à la génération du graphe multicouche, dont les besoins ont été formulés à partir de la QD1. Bien que celle-ci soit facilitée par l'outil informatique développé, elle pourrait être encore plus automatisée. Pour cela, différentes méthodes sont envisagées. Des données et des informations, collectées en différents points de l'architecture réseau du système étudié, pourraient être traitées et utilisées dans un script spécifique pour définir et créer les noeuds et les relations du graphe grâce à l'outil déjà existant. Par exemple, cela pourrait être réalisé en analysant les trames de communications entre différents éléments du système. Une autre possibilité serait d'implémenter une méthode déjà existante pour la génération de graphe de variables système à partir de l'analyse des programmes embarqués dans les automates programmables

[COZ18]. Concernant l'outil informatique en lui-même, celui-ci devrait être mis à disposition de la communauté scientifique à partir d'une licence *open-source*. Une documentation détaillée l'accompagnerait pour faciliter son utilisation dans diverses applications.

Comme nous l'avons défini dans les paragraphes précédents, de nombreuses perspectives des travaux proposés sont associées à la représentation des informations aux opérateurs pour faciliter la prise de décision. Ces informations, issues de différentes analyses liées à la problématique des dépendances dans un navire, pourraient être intégrées au sein de la *Maritime Cyber Situational Awareness* pour faciliter la cybersurveillance des systèmes maritimes [JBKS19]. Par exemple, l'évaluation dynamique de la propagation d'anomalie s'inscrirait dans une logique d'évaluation dynamique des risques (*Dynamic Risk Assessment*) pour favoriser la prise de décision. Aussi, dans ses travaux de thèse, Olivier Jacq a souligné l'importance de la représentation des éléments d'un système d'information maritime pour l'identification des composants critiques, et l'analyse des potentiels impacts qui en résultent [Jac21b]. Un graphe semblerait être la solution la plus adaptée pour faciliter la représentation de ces informations dans un contexte de visualisation et compréhension des flux de données importants. C'est ce même formalisme mathématique qui a été utilisé par Gustavo Gonzalez-Granadillo *et al.* pour évaluer dynamiquement les risques associés à un CPS en charge de la distribution d'électricité [GGDM+18].

Enfin, l'approche proposée a été validée pour deux cas particuliers de système cyber-physique à partir de différents scénarios. Même si ceux-ci ont été formulés pour des cas d'études associés à des situations réelles et significatives, ils sont réalisés dans un environnement expérimental totalement contrôlé. Une perspective essentielle pour des travaux futurs serait d'implémenter l'approche proposée dans un nombre plus important et varié de systèmes. Différentes boucles interdépendantes du *Naval Cyber Range* représenteraient par exemple un cas d'étude pertinent et représentatif.

Liste de publications

IV.5 Articles de conférence

Les travaux de thèses présentés dans ce manuscrit ont été capitalisés à partir de 4 articles soumis et présentés dans 3 conférences internationales certifiées IEEE :

— N. Pelissero, P. Merino Laso et J. Puentes, *Naval cyber-physical anomaly propagation analysis based on a quality assessed graph*, 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). [**PLP20**]

— N. Pelissero, P. Merino Laso et J. Puentes, *Impact assessment of anomaly propagation in a naval water distribution cyber-physical system*, 2021 IEEE International Conference on Cyber Security and Resilience (CSR). [**PMLP21a**]

— N. Pelissero, P. Merino Laso, O. Jacq et J. Puentes, *Towards modeling of naval systems interdependencies for cybersecurity*, Global Oceans 2021. [**PMLJP21**]

— N. Pelissero, P. Merino Laso et J. Puentes, *Model graph generation for naval cyber-physical systems*, Global Oceans 2021. [**PMLP21b**]

La correspondance entre les éléments de réponses apportés par ces articles, et les questions de recherche énoncées dans ce manuscrit, est illustré dans la Table IV.1 .

Table IV.1: Matrice articles scientifiques / questions de recherche

	QR1	**QR2**	**QR3**	**QD1**
[PLP20]			■	
[PMLP21a]		■	■	
[PMLJP21]	■			
[PMLP21b]				■

Bibliographie

[AG20] Vincenzo Arrichiello and Paola Gualeni. Systems engineering and digital twin : a vision for the future of cruise ships design, production and operations. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, 14(1) :115–122, 2020.

[Age18a] Agence nationale de la sécurité et des systèmes d'information (ANSSI). Guide des bonnes pratiques de sécurité informatique à bord des navires. Technical report, ANSSI, 2018.

[Age18b] Agence nationale de la sécurité et des systèmes d'information (ANSSI). La méthode ebios risk manager - le guide (version 1.1). Technical report, ANSSI, 2018.

[AIS18] Rasim Alguliyev, Yadigar Imamverdiyev, and Lyudmila Sukhostat. Cyber-physical systems and their security issues. *Computers in Industry*, 100 :212–223, 2018.

[AK20] Aida Akbarzadeh and Sokratis Katsikas. Identifying critical components in large scale cyber physical systems. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pages 230–236, 2020.

[AK21] Aida Akbarzadeh and Sokratis Katsikas. Identifying and analyzing dependencies in and among complex cyber physical systems. *Sensors*, 21(5) :1685, 2021.

[Alw21] A Alwan. *Data Quality Management in Large-Scale Cyber-Physical Systems*. PhD thesis, University of East London, 2021.

[AMMN+16] Hamad Al-Mohannadi, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen, and Jules Disso. Cyber-attack modeling analysis techniques : An overview. In *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)*, pages 69–76. IEEE, 2016.

[AMR17] Chuadhry Mujeeb Ahmed, Carlos Murguia, and Justin Ruths. Model-based attack detection scheme for smart water distribution networks. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, page 101–113, New York, NY, USA, 2017. Association for Computing Machinery.

[ANS19] ANSSI (Agence nationale de la sécurité et des systèmes d'information). Fiches méthodes ebios rm (version 1.1). Technical report, ANSSI, 2019.

[AS14] Hosny Abbas and Samir Shaheen. Future scada challenges and the promising solution : the agent-based scada. *International Journal of Critical Infrastructures*, 10 :307 – 333, 01 2014.

[AWK02] Paul Ammann, Duminda Wijesekera, and Saket Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 217–224, 2002.

[BBC+14] Stefano Boccaletti, Ginestra Bianconi, Regino Criado, Charo I Del Genio, Jesús Gómez-Gardenes, Miguel Romance, Irene Sendina-Nadal, Zhen Wang, and Massimiliano Zanin. The structure and dynamics of multilayer networks. *Physics Reports*, 544(1) :1–122, 2014.

[BGS+21] Luke C. Brownlow, Conner J. Goodrum, Michael J. Sypniewski, James A. Coller, and David J. Singer. A multilayer network approach to vulnerability assessment for early-stage naval ship design programs. *Ocean Engineering*, 225 :108731, apr 2021.

[BHJ09] Mathieu Bastian, Sebastien Heymann, and Mathieu Jacomy. Gephi : an open source software for exploring and manipulating networks. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 3, 2009.

[BIM18] BIMCO. The guidelines on cyber security onboard ships - version 3. Technical report, 2018.

[BIM20] BIMCO. The guidelines on cyber security onboard ships - version 4. Technical report, 2020.

[Bir17] David Birkett. Water critical infrastructure security and its dependencies. *Contemporary Voices : St Andrews Journal of International Relations*, 8(2), 2017.

[BJL+21] Clet Boudehenn, Olivier Jacq, Maxence Lannuzel, Jean-Christophe Cexus, and Abdel Boudraa. 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.

[BLGA17] Anatolij Bezemskij, George Loukas, Diane Gan, and Richard J Anthony. Detecting cyber-physical threats in an autonomous robotic vehicle using bayesian networks. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 98–103. IEEE, 2017.

[BLLL17] Zhaohong Bie, Yanling Lin, Gengfeng Li, and Furong Li. Battling the extreme : A study on the power system resilience. *Proceedings of the IEEE*, 105(7) :1253–1266, 2017.

[BSH+18] Dorian Brefort, Colin Shields, Agnieta Habben Jansen, Etienne Duchateau, Rachel Pawling, Koen Droste, Ted Jasper, Michael Sypniewski, Conner Goodrum, Mark A. Parsons, Mustafa Yasin Kara, Mark Roth, David J. Singer, David Andrews, Hans Hopman, Alan Brown, and Austin A. Kana. An architectural framework for distributed naval ship systems. *Ocean Engineering*, 147 :375–385, 2018.

[BTBV19] Victor Bolbot, Gerasimos Theotokatos, Evangelos Boulougouris, and Dracos Vassalos. Safety related cyber-attacks identification and assessment for autonomous inland ships. In *International Seminar on Safety and Security of Autonomous Vessels (ISSAV)*, 2019.

[BTBV20] Victor Bolbot, Gerasimos Theotokatos, Evangelos Boulougouris, and Dracos Vassalos. A novel cyber-risk assessment method for ship systems. *Safety Science*, 131 :104908, 2020.

[BV18] BV. Rules on cyber security for the classification of marine units, 2018.

[BW03] David Bailey and Edwin Wright. 1 - background to scada. In David Bailey and Edwin Wright, editors, *Practical SCADA for Industry*, pages 1–10. Newnes, Oxford, 2003.

[CAB00] Robert CABANE. *Théorie des graphes*. Ed. Techniques Ingénieur, 2000.

[CBCS15] Martine Collard, Laurent Brisson, Philippe Collard, and Erick Stattner. Rumor spreading modeling : Profusion versus scarcity. In *2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 1547–1554. IEEE, 2015.

[CBK09] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection : A survey. *ACM computing surveys (CSUR)*, 41(3) :1–58, 2009.

[CFV21] Miguel E Coimbra, Alexandre P Francisco, and Luís Veiga. An analysis of the graph processing landscape. *Journal of big Data*, 8(1) :1–41, 2021.

[Che17] Hong Chen. Applications of cyber-physical system : a literature review. *Journal of Industrial Integration and Management*, 2(03) :1750012, 2017.

[Com20] European Commission. Eu transport in figures. statistical pocketbook 2020. Technical report, European Union, 2020.

[COZ18] John H Castellanos, Martín Ochoa, and Jianying Zhou. Finding dependencies between cyber-physical domains for security testing of industrial control systems. In *Proceedings of the 34th Annual Computer Security Applications Conference*, pages 582–594, 2018.

[Dac94] Marc Dacier. *Towards quantitative evaluation of computer security*. PhD thesis, PhD thesis, Institut National Polytechnique de Toulouse, 1994.

[dam16] Direction des affaires maritimes. Cyber sécurité - Évaluer et protéger le navire. Technical report, Direction Générale des Infrastructures, des Transports et de la Mer (DGITM), 2016.

[dam17] Direction des affaires maritimes. Cyber sécurité - renforcer la protection des systèmes industriels à bord des navires. Technical report, Direction Générale des Infrastructures, des Transports et de la Mer (DGITM), 2017.

[DC15] Hui Dong and Lirong Cui. System reliability under cascading failure models. *IEEE Transactions on Reliability*, 65(2) :929–940, 2015.

[Den12] Dorothy Denning. Stuxnet : What has changed ? *Future Internet*, 4 :672–687, 12 2012.

[DHX+18] Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, and Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275 :1674 – 1683, 2018.

[DNGG+18] Armando Di Nardo, Carlo Giudicianni, Roberto Greco, Manuel Herrera, and Giovanni F Santonastaso. Applications of graph spectral techniques to water distribution network management. *Water*, 10(1) :45, 2018.

[DR14] Joël De Rosnay. *Le macroscope. Vers une vision globale.* Média Diffusion, 2014.

[DSDB16] Alessandro D'Innocenzo, Francesco Smarra, and Maria Domenica Di Benedetto. Resilient stabilization of multi-hop control networks subject to malicious attacks. *Automatica*, 71 :1–9, 2016.

[dT15] Forum International des Transports. The impact of mega-ships. (10), 2015.

[DWHW16] Derui Ding, Zidong Wang, Qing-Long Han, and Guoliang Wei. Security control for discrete-time stochastic nonlinear systems subject to deception attacks. *IEEE Transactions on Systems, Man, and Cybernetics : Systems*, 48(5) :779–789, 2016.

[Edi11] Fourth Edition. Guidelines for drinking-water quality. *WHO chronicle*, 38(4) :104–108, 2011.

[EHC+20] André Listou Ellefsen, Peihua Han, Xu Cheng, Finn Tore Holmeset, Vilmar Æsøy, and Houxiang Zhang. Online fault detection in autonomous ferries : Using fault-type independent spectral anomaly detection. *IEEE Transactions on Instrumentation and Measurement*, 69(10) :8216–8225, 2020.

[EKP14] D.G. Eliades, M. Kyriakou, and M.M. Polycarpou. Sensor placement in water distribution systems using the s-place toolkit. *Procedia Engineering*, 70 :602–611, 2014. 12th International Conference on Computing and Control for the Water Industry, CCWI2013.

[EKT16] Oliver Eigner, Philipp Kreimel, and Paul Tavolato. Detection of man-in-the-middle attacks on industrial control networks. In *2016 International Conference on Software Security and Assurance (ICSSA)*, pages 64–69, 2016.

[EPKP15] Georgios Ellinas, Christos Panayiotou, Elias Kyriakides, and Marios Polycarpou. Critical infrastructure systems : Basic principles of monitoring, control, and security. In *Intelligent monitoring, control, and security of critical infrastructure systems*, pages 1–30. Springer, 2015.

[Eul53] Leonhard Euler. Leonhard euler and the königsberg bridges. *Scientific American*, 189(1) :66–72, 1953.

[Eur08] Conseil Européen. Directive 2008/114/ce. *Journal officiel européen L 345*, 2008.

[Eve11] Shimon Even. *Graph algorithms*. Cambridge University Press, 2011.

[For17] Joint Task Force. Security and privacy controls for information systems and organizations. Technical report, National Institute of Standards and Technology, 2017.

[fS15] International Organization for Standardization. Iso/iec/ieee international standard - systems and software engineering – system life cycle processes. *ISO/IEC/IEEE 15288 First edition 2015-05-15*, pages 1–118, 2015.

[Gar15] R Garderes. Glossaire interarmées de terminologie opérationnelle, 2015.

[GCRP19] Mouzhi Ge, Stanislav Chren, Bruno Rossi, and Tomas Pitner. Data quality management framework for smart grid systems. In *International Conference on Business Information Systems*, pages 299–310. Springer, 2019.

[GGDKGA17] Gustavo Gonzalez-Granadillo, Elena Doynikova, Igor Kotenko, and Joaquin Garcia-Alfaro. Attack graph-based countermeasure selection using a stateful return on investment metric. In *International Symposium on Foundations and Practice of Security*, pages 293–302. Springer, 2017.

[GGDM+18] Gustavo Gonzalez-Granadillo, Samuel Dubus, Alexander Motzek, Joaquin Garcia-Alfaro, Ender Alvarez, Matteo Merialdo, Serge Papillon, and Hervé Debar. Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems*, 83 :535–552, 2018.

[GMV+12] Giovanna Bagnasco Gianni, Matilde Marzullo, Stefano Valtolina, Barbara Rita Barricelli, Susanna Bortolotto, Piero Favino, Andrea Garzulino, and Raffaella Simonelli. An ecosystem of tools and methods for archeological research. In *2012 18th International Conference on Virtual Systems and Multimedia*, pages 133–140. IEEE, 2012.

[GPGV14] Volkan Gunes, Steffen Peter, Tony Givargis, and Frank Vahid. A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems*, 8 :4242–4268, 12 2014.

[GSS18] Conner J. Goodrum, Colin P.F. Shields, and David J. Singer. Understanding cascading failures through a vulnerability analysis of interdependent ship-centric distributed systems using networks. *Ocean Engineering*, 150 :36–47, 2018.

[HAJ+20] Niamat Ullah Ibne HOSSAIN, Safae El Amrani, Raed Jaradat, Mohammad Marufuzzaman, Randy Buchanan, Christina Rinaudo, and Michael Hamilton. Modeling and assessing interdependencies between critical infrastructures using bayesian network : A case study of inland waterway port and surrounding supply chain network. *Reliability Engineering & System Safety*, 198 :106898, 2020.

[HG15] Ove Hoegh-Guldberg. Reviving the ocean economy : the case for action. 2015.

[HK20] Bruce Hartpence and Andres Kwasinski. Combating tcp port scan attacks using sequential neural networks. In *2020 International Conference on Computing, Networking and Communications (ICNC)*, pages 256–260, 2020.

[HL08] Lih-Hsing Hsu and Cheng-Kuan Lin. *Graph theory and interconnection networks*. CRC press, 2008.

[HN19] A.E. Hodler and M. Needham. *Graph Algorithms : Practical Examples in Apache Spark and Neo4j*. O'Reilly Media, 2019.

[Hop00] Adrian A. Hopgood. *Intelligent Systems for Engineers and Scientists*. CRC Press, oct 2000.

[HRG+20] Amin Hassanzadeh, Amin Rasekh, Stefano Galelli, Mohsen Aghashahi, Riccardo Taormina, Avi Ostfeld, and M Katherine Banks. A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, 146(5) :03120003, 2020.

[Int17] International Maritime Organization (IMO). Guidelines on maritime cyber risk management. Msc-fal.1/circ.3. international maritime organization., 2017.

[ISA] ISA. Ansi/isa-95.

[Jac21a] Olivier Jacq. Advanced database of maritime cyber incidents released for litterature. `https://gitlab.com/m-cert/admiral`, 2021.

[Jac21b] Olivier Jacq. *Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la Cyber Situational Awareness du monde maritime*. PhD thesis, IMT Atlantique, 01 2021.

[Jak11] Gabriel Jakobson. Mission cyber security situation assessment using impact dependency graphs. In *14th international conference on information fusion*, pages 1–8. IEEE, 2011.

[JBB+18] Olivier Jacq, Xavier Boudvin, David Brosset, Yvon Kermarrec, and Jacques Simonin. Detecting and hunting cyberthreats in a maritime environment : Specification and experimentation of a maritime cybersecurity operations centre. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–8. IEEE, 2018.

[JBKS19] Olivier Jacq, David Brosset, Yvon Kermarrec, and Jacques Simonin. Cyber attacks real time detection : towards a cyber situational awareness for naval systems. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–2, 2019.

[JHC+96] Daniel B Jernigan, Jo Hofmann, Martin S Cetron, JP Nuorti, BS Fields, RF Benson, RF Breiman, HB Lipman, RJ Carter, CA Genese, et al. Outbreak of legionnaires' disease among cruise ship passengers exposed to a contaminated whirlpool spa. *The Lancet*, 347(9000) :494–499, 1996.

[JHZ13] Jonas Johansson, Henrik Hassel, and Enrico Zio. Reliability and vulnerability analyses of critical infrastructures : Comparing two approaches in the context of power systems. *Reliability Engineering & System Safety*, 120 :27–38, 2013.

[JNO05] Sushil Jajodia, Steven Noel, and Brian O'berry. Topological analysis of network attack vulnerability. In *Managing cyber threats*, pages 247–266. Springer, 2005.

[JT19] Kevin Jones and Kimberly Tam. Macra : A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18, 01 2019.

[JTP16] Kevin D Jones, Kimberly Tam, and Maria Papadaki. Threats and impacts in maritime cyber security. 2016.

[Kam18] Mehran Kamrava. *Troubled Waters : Insecurity in the Persian Gulf*. Cornell University Press, 2018.

[Kar11] Stamatis Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, pages 4490–4494, 2011.

[KBJ17] Lutz Kretschmann, Hans-Christoph Burmeister, and Carlos Jahn. Analyzing the economic benefit of unmanned autonomous ships : An exploratory cost-comparison between an autonomous and a conventional bulk carrier. *Research in transportation business & management*, 25 :76–86, 2017.

[KDGE18] Khaled Karray, Jean-Luc Danger, Sylvain Guilley, and M Abdelaziz Elaabid. Attack tree construction and its application to the connected vehicle. In *Cyber-Physical Systems Security*, pages 175–190. Springer, 2018.

[KDK20] Georgios Kavallieratos, Vasiliki Diamantopoulou, and Sokratis K Katsikas. Shipping 4.0 : Security requirements for the cyber-enabled ship. *IEEE Transactions on Industrial Informatics*, 16(10) :6617–6625, 2020.

[KK12] Kyoung-Dae Kim and Panganamala R Kumar. Cyber–physical systems : A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue) :1287–1308, 2012.

[KK20] Georgios Kavallieratos and Sokratis Katsikas. Attack path analysis for cyber physical systems. In Sokratis Katsikas, Frédéric Cuppens, Nora Cuppens, Costas Lambrinoudakis, Christos Kalloniatis, John Mylopoulos, Annie Antón, Stefanos Gritzalis, Weizhi Meng, and Steven Furnell, editors, *Computer Security*, pages 19–33, Cham, 2020. Springer International Publishing.

[KKG18] Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. Cyber-attacks against the autonomous ship. In *Computer Security*, pages 20–36. Springer, 2018.

[KKG20] Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. Modelling shipping 4.0 : A reference architecture for the cyber-enabled ship. In Ngoc Thanh Nguyen, Kietikul Jearanaitanakij, Ali Selamat, Bogdan Trawiński, and Suphamit Chittayasothorn, editors, *Intelligent Information and Database Systems*, pages 202–217, Cham, 2020. Springer International Publishing.

[KLYM19] Samir Khan, Chun Fui Liew, Takehisa Yairi, and Richard McWilliam. Unsupervised anomaly detection in unmanned aerial vehicles. *Applied Soft Computing*, 83 :105650, 2019.

[KM27] William Ogilvy Kermack and Anderson G McKendrick. A contribution to the mathematical theory of epidemics. *Proceedings of the royal society of london. Series A, Containing papers of a mathematical and physical character*, 115(772) :700–721, 1927.

[Kni02] John C Knight. Safety critical systems : challenges and directions. In *Proceedings of the 24th international conference on software engineering*, pages 547–550, 2002.

[Koz92] Dexter C. Kozen. *Depth-First and Breadth-First Search*, pages 19–24. Springer New York, New York, NY, 1992.

[Kri16] Srećko Krile. Fresh water supply from different sources in the shipping. *Procedia Engineering*, 149 :190–196, 2016. International Conference on Manufacturing Engineering and Materials, ICMEM 2016, 6-10 June 2016, Nový Smokovec, Slovakia.

[KUG12] G.H. Kjølle, I.B. Utne, and O. Gjerde. Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety*, 105 :80–89, 2012. ESREL 2010.

[Las17] Pedro Merino Laso. *Détection de dysfonctionements et d'actes malveillants basée sur des modèles de qualité de données multi-capteurs*. PhD thesis, Ecole nationale supérieure Mines-Télécom Atlantique, 2017.

[LBP16] Pedro Merino Laso, David Brosset, and John Puentes. Monitoring approach of cyber-physical systems by quality measures. In *International Conference on Sensor Systems and Software*, pages 105–117. Springer, 2016.

[LCLP20] Seulbi Lee, Minji Choi, Hyun-Soo Lee, and Moonseo Park. Bayesian network-based seismic damage estimation for power and potable water supply systems. *Reliability Engineering & System Safety*, 197 :106796, may 2020.

[LDB20] Harjinder Singh Lallie, Kurt Debattista, and Jay Bal. A review of attack graph and attack tree visual syntax in cyber security. *Computer Science Review*, 35 :100219, 2020.

[Lee61] Chin Yang Lee. An algorithm for path connections and its applications. *IRE transactions on electronic computers*, (3) :346–365, 1961.

[Lee19] Susanne Lee. Managing water quality on board passenger vessels to ensure passenger and crew safety. *Perspectives in Public Health*, 139(2) :70–74, mar 2019.

[Les76] Jacques Lesourne. *Les systèmes du destin*. Dalloz Economie, 1976.

[Lev17] Oskar Levander. Autonomous ships on the high seas. *IEEE spectrum*, 54(2) :26–31, 2017.

[LHS15] Ana Laugé, Josune Hernantes, and Jose M Sarriegi. Critical infrastructure dependencies : A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection*, 8 :16–23, 2015.

[Lit03] Richard G Little. Toward more robust infrastructure : observations on improving the resilience and reliability of critical systems. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, pages 9–pp. IEEE, 2003.

[LLDO+20] Lu Liu, Evan Lopez, Leonardo Dueñas-Osorio, Lauren Stadler, Yuefeng Xie, Pedro Alvarez, and Qilin Li. The importance of system configuration for distributed direct potable water reuse. *Nature Sustainability*, 3, 07 2020.

[LLW12] James Ladyman, James Lambert, and Karoline Wiesner. What is a complex system ? *European Journal for Philosophy of Science*, 3(1) :33–67, jun 2012.

[LPO19] Miguel López, Alberto Peinado, and Andrés Ortiz. An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks. *Computer Networks*, 165 :106945, 2019.

[LS17] Edward Ashford Lee and Sanjit A Seshia. *Introduction to embedded systems : A cyber-physical systems approach*. Mit Press, 2017.

[LWXP19] Shuyun Luo, Yuzhou Wen, Weiqiang Xu, and Deepak Puthal. Adaptive task offloading auction for industrial cps in mobile edge computing. *IEEE Access*, 7 :169055–169065, 2019.

[LXC+21] Yuan Luo, Ya Xiao, Long Cheng, Guojun Peng, and Danfeng Yao. Deep learning-based anomaly detection in cyber-physical systems : Progress and opportunities. *ACM Computing Surveys (CSUR)*, 54(5) :1–36, 2021.

[MBGJ] Emmanuel Miconnet, Olivier Bettan, Daniel Gidoin, and Eric Jouenne. Un exemple d'usage des graphes d'attaques pour l'évaluation dynamique des risques en cyber-sécurité.

[MBZ+20] Leonardo M. Millefiori, Paolo Braca, Dimitris Zissis, Giannis Spiliopoulos, Stefano Marano, Peter K. Willett, and Sandro Carniel. Covid-19 impact on global maritime mobility. September 2020.

[MC14] Robert Mitchell and Ray Chen. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *IEEE Transactions on Dependable and Secure Computing*, 12(1) :16–30, 2014.

[MD18] Haralambos Mouratidis and Vasiliki Diamantopoulou. A security analysis method for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(9) :4093–4100, 2018.

[mf12] Cluster maritime français. Le livre bleu de la marétique. 2012.

[MFC+18] A. Mérida García, I. Fernández García, E. Camacho Poyato, P. Montesinos Barrios, and J.A. Rodríguez Díaz. Coupling irrigation scheduling with solar energy production in a smart irrigation management system. *Journal of Cleaner Production*, 175 :670–682, 2018.

[Mil13] Justin J Miller. Graph database applications and concepts with neo4j. In *Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA*, 2013.

[MS10] Yilin Mo and Bruno Sinopoli. False data injection attacks in control systems. In *Preprints of the 1st workshop on Secure Control Systems*, pages 1–6, 2010.

[MSC21] Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships. Technical report, International Maritime Organization, 2021.

[MSH16] Koosha Marashi, Sahra Sedigh Sarvestani, and Ali R Hurson. Quantification and analysis of interdependency in cyber-physical systems. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*, pages 149–154. IEEE, 2016.

[MSH17] Koosha Marashi, Sahra Sedigh Sarvestani, and Ali R Hurson. Consideration of cyber-physical interdependencies in reliability modeling of smart grids. *IEEE Transactions on Sustainable Computing*, 3(2) :73–83, 2017.

[MSL16] Angela Marchi, Angus Simpson, and Martin Lambert. Optimization of pump operation using rule-based controls in epanet2 : New ettar toolkit and correction of energy computation. *Journal of Water Resources Planning and Management*, 142 :04016012, 02 2016.

[MT20] Rosanda Mulić and Iris Jerončić Tomić. Supplying ships with safe drinking-water. *International Maritime Health*, 71(2) :123–128, 2020.

[MTU18] Yusuke Mishina, Kazuo Takaragi, and Katsuyuki Umezawa. A method of threat analysis for cyber-physical system using vulnerability databases. In *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–7. IEEE, 2018.

[MV16] Dietmar PF Möller and Hamid Vakilzadian. Cyber-physical systems in smart transportation. In *2016 IEEE international conference on electro information technology (EIT)*, pages 0776–0781. IEEE, 2016.

[Nat21] Marine Nationale. Dossier d'information 2021. *Cols bleus*, 2021.

[NDP17] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri. An introduction to information security. Technical report, jun 2017.

[NKHA13] Behnam Neyshabur, Ahmadreza Khadem, Somaye Hashemifar, and Seyed Shahriar Arab. NETAL : a new graph-based method for global alignment of protein–protein interaction networks. *Bioinformatics*, 29(13) :1654–1662, 05 2013.

[NZ19] Baoyu Ni and Lingdong Zeng. Ship design process. In *Encyclopedia of Ocean Engineering*, pages 1–8. Springer Singapore, 2019.

[OGA+05] Xinming Ou, Sudhakar Govindavajhala, Andrew W Appel, et al. Mulval : A logic-based network security analyzer. In *USENIX security symposium*, volume 8, pages 113–128. Baltimore, MD, 2005.

[oTD20] United Nations Conference on Trade and Development. Review of maritime transport 2020. Technical report, United Nations, 2020.

[PBH11] Roni Parshani, Sergey V. Buldyrev, and Shlomo Havlin. Critical effect of dependency groups on the function of networks. *Proceedings of the National Academy of Sciences*, 108(3) :1007–1010, 2011.

[PDK+18] Giota Paparistodimou, Alex Duffy, Philip Knight, Ian Whitfield, Malcolm Robb, and Caroline Voong. Network-based metrics for assessment of naval distributed system architectures. 2018.

[PLP20] Nicolas Pelissero, Pedro Merino Laso, and John Puentes. Naval cyber-physical anomaly propagation analysis based on a quality assessed graph. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–8. IEEE, 2020.

[PMLJP21] Nicolas Pelissero, Pedro Merino Laso, Olivier Jacq, and John Puentes. Towards modeling of naval systems interdependencies for cybersecurity. In *Global Oceans 2021*, 2021.

[PMLP21a] Nicolas Pelissero, Pedro Merino Laso, and John Puentes. Impact assessment of anomaly propagation in naval water distribution cyber-physical system. In *2021 IEEE International Conference on Cyber Security and Resilience (IEEE CSR)*, pages 1–8. IEEE, 2021. (accepted).

[PMLP21b] Nicolas Pelissero, Pedro Merino Laso, and John Puentes. Model graph generation for naval cyber-physical systems. In *Global Oceans 2021*, 2021.

[PPM18] Nikolaos Polatidis, Michalis Pavlidis, and Haralambos Mouratidis. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 56 :74–82, 2018.

[Pre03] US President. Homeland security presidential directive 7 : Critical infrastructure identification, prioritization, and protection. *Weekly Compilation of Presidential Documents*, 39 :1816–1822, 2003.

[PS98] Cynthia Phillips and Laura Painton Swiler. A graph-based system for network-vulnerability analysis. In *Proceedings of the 1998 workshop on New security paradigms*, pages 71–79, 1998.

[PSHB20] Paul Perrotin, Salah Sadou, David Hairion, and Antoine Beugnard. Detecting human vulnerably in socio-technical systems : a naval case study. In *Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems : Companion Proceedings*, pages 1–8, 2020.

[PTT+20] Evangelos Pournaras, Riccardo Taormina, Manish Thapa, Stefano Galelli, Venkata Palleti, and Robert Kooij. Cascading failures in interconnected power-to-water networks. *SIGMETRICS Perform. Eval. Rev.*, 47(4) :16–20, April 2020.

[Pub04] FIPS Pub. Standards for security categorization of federal information and information systems. *NIST FIPS*, 199, 2004.

[PVB+15] Frederic Petit, Duane Verner, David Brannegan, William Buehring, David Dickinson, Karen Guziel, Rebecca Haffenden, Julia Phillips, and James Peerenboom. Analysis of critical infrastructure dependencies and interdependencies. Technical report, Argonne National Lab.(ANL), Argonne, IL (United States), 2015.

[QMSC20] Gabriela Quitana, Maria Molinos-Senante, and Alondra Chamorro. Resilience of critical infrastructure to natural hazards : A review focused on drinking water systems. *International Journal of Disaster Risk Reduction*, 48 :101575, 2020.

[QYL20] Xiaogang Qi, Guizhen Yang, and Lifang Liu. Robustness analysis of the networks in cascading failures with controllable parameters. *Physica A : Statistical Mechanics and its Applications*, 539 :122870, feb 2020.

[QZQ+18] Zhaoyang Qu, Yu Zhang, Nan Qu, Lei Wang, Yang Li, and Yunchang Dong. Method for quantitative estimation of the risk propagation threshold in electric power cps based on seepage probability. *IEEE Access*, 6 :68813–68823, 2018.

[R+18] Ronald S Ross et al. Risk management framework for information systems and organizations : A system life cycle approach for security and privacy. 2018.

[RAMH18] Daniel Ramotsoela, Adnan Abu-Mahfouz, and Gerhard Hancke. A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. *Sensors*, 18(8) :2491, 2018.

[RBC+04] Roisin M Rooney, Jamie K Bartram, Elaine H Cramer, Stacey Mantha, Gordon Nichols, Rohini Suraj, and Ewen CD Todd. A review of outbreaks of waterborne disease associated with ships : evidence for risk management. *Public health reports*, 119(4) :435–442, 2004.

[RCL11] OJ Rodseth, Morten Jagd Christensen, and K Lee. Design challenges and decisions for a new ship data network. *ISIS*, pages 15–16, 2011.

[RCM+17] Alexandre Valério Rodrigues, Rodolfo Santos Carapau, Mario Monteiro Marques, Victor Lobo, and Fernando Coito. Unmanned systems interoperability in military maritime operations : Mavlink to stanag 4586 bridge. In *OCEANS 2017 - Aberdeen*, pages 1–5, 2017.

[Reb14] George Rebovich. Mitre systems engineering guide. *The MITRE Corporation, http ://www. mitre. org/publications/systems-engineering-guide/systemsengineering-guide. accessed*, 2, 2014.

[RHM+16] Amin Rasekh, Amin Hassanzadeh, Shaan Mulchandani, Shimon Modi, and M. Banks. Smart water networks and cyber security. *Journal of Water Resources Planning and Management*, 142 :01816004, 02 2016.

[RKR+20] Hossein Mohammadi Rouzbahani, Hadis Karimipour, Abolfazl Rahimnejad, Ali Dehghantanha, and Gautam Srivastava. Anomaly detection in cyber-physical systems using machine learning. In *Handbook of Big Data Privacy*, chapter Chapter 10. Springer Nature, 2020.

[Ros00] Lewis Rossman. *Epanet 2 users manual*, volume 38. 01 2000.

[RPK01] S.M. Rinaldi, J.P. Peerenboom, and T.K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6) :11–25, 2001.

[RT14] Ørnulf Jan Rødseth and Åsmund Tjora. A system architecture for an unmanned ship. In *Proceedings of the 13th international conference on computer and IT applications in the maritime industries (COMPIT)*. Verlag Schriftenreihe Schiffbau, 2014 Redworth, UK, 2014.

[RWZ+18] Wendi Ren, Jiajing Wu, Xi Zhang, Rong Lai, and Liang Chen. A stochastic model of cascading failure dynamics in communication networks. *IEEE Transactions on Circuits and Systems II : Express Briefs*, 65(5) :632–636, may 2018.

[SARX19] Zafar Saeed, Rabeeh Ayaz Abbasi, Muhammad Imran Razzak, and Guandong Xu. Event detection in twitter stream using weighted dynamic heartbeat graph approach [application notes]. *IEEE Computational Intelligence Magazine*, 14(3) :29–38, 2019.

[Sch13] William D Schindel. 4.3. 2 systems of innovation ii : The emergence of purpose. In *INCOSE International Symposium*, volume 23, pages 1006–1020. Wiley Online Library, 2013.

[SCYY16] Guo-lin Shao, Xing-shu Chen, Xue-yuan Yin, and Xiao-ming Ye. A fuzzy detection approach toward different speed port scan attacks based on dempster–shafer evidence theory. *Security and Communication Networks*, 9(15) :2627–2640, 2016.

[SDF18] Bastien Sultan, Fabien Dagnat, and Caroline Fontaine. A methodology to assess vulnerabilities and countermeasures impact on the missions of a naval system. In Sokratis K. Katsikas, Frédéric Cuppens, Nora Cuppens, Costas Lambrinoudakis, Christos Kalloniatis, John Mylopoulos, Annie Antón, and Stefanos Gritzalis, editors, *Computer Security*, pages 63–76, Cham, 2018. Springer International Publishing.

[SJ18] Ajeet Singh and Anurag Jain. Study of cyber attacks on cyber-physical system. *SSRN Electronic Journal*, 2018.

[SJB21] Rahul Saxena, Mahipal Jadeja, and Vikrant Bhateja. Propagation analysis of covid-19 : An sir model-based investigation of the pandemic. *Arabian Journal for Science and Engineering*, pages 1–13, 2021.

[SKO+20] Gulshan Shrivastava, Prabhat Kumar, Rudra Pratap Ojha, Pramod Kumar Srivastava, Senthilkumar Mohan, and Gautam Srivastava. Defensive modeling of fake news through online social networks. *IEEE Transactions on Computational Social Systems*, 7(5) :1159–1167, 2020.

[SLX16] Chih-Che Sun, Chen-Ching Liu, and Jing Xie. Cyber-physical system security of a power grid : State-of-the-art. *Electronics*, 5(3) :40, 2016.

[SMM+19] Hillary Sillitto, James Martin, Dorothy McKinney, Regina Griego, Dov Dori, Daniel Krob, Patrick Godfrey, Eileen Arnold, and Scott Jackson. Systems engineering and system definitions. In *INCOSE*, 2019.

[Sob84] Z. Sobol. *The Ship's Water Supply*, pages 128–134. Springer Berlin Heidelberg, Berlin, Heidelberg, 1984.

[SPB+16] Juan Saldarriaga, Diego Páez, Jessica Bohórquez, Nicolás Páez, Juan Pablo París, Daniela Rincón, Camilo Salcedo, and Daniel Vallejo. Rehabilitation and leakage reduction on c-town using hydraulic criteria. *Journal of Water Resources Planning and Management*, 142(5) :C4015013, 2016.

[SSCD18] Agostino Sturaro, Simone Silvestri, Mauro Conti, and Sajal K Das. A realistic model for failure propagation in interdependent cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, 7(2) :817–831, 2018.

[SSCO08] Karen A Scarfone, Murugiah P Souppaya, Amanda Cody, and Angela D Orebaugh. Sp 800-115. technical guide to information security testing and assessment, 2008.

[Sta16] John Stark. *Product Lifecycle Management*, pages 1–35. Springer International Publishing, Cham, 2016.

[STB17] Kashif Saleem, Zhiyuan Tan, and William Buchanan. Security for cyber-physical systems in healthcare. In *Health 4.0 : How Virtualization and Big Data are Revolutionizing Healthcare*, pages 233–251. Springer, 2017.

[Sun19] Kai Sun. *WAMS-Based Controlled System Separation to Mitigate Cascading Failures in Smart Grid*, pages 185–195. Springer International Publishing, Cham, 2019.

[SYM+16] T. Shah, A. Yavari, K. Mitra, S. Saguna, P. P. Jayaraman, F. Rabhi, and R. Ranjan. Remote health care cyber-physical system : quality of service (qos) challenges and opportunities. *IET Cyber-Physical Systems : Theory Applications*, 1(1) :40–48, 2016.

[SZ15] Kewei Sha and Sherali Zeadally. Data quality challenges in cyber-physical systems. *J. Data and Information Quality*, 6(2-3) :8 :1–8 :4, June 2015.

[TFN+19] James R. Thompson, Damon Frezza, Burhan Necioglu, Michael L. Cohen, Kenneth Hoffman, and Kristine Rosfjord. Interdependent critical infrastructure model (ICIM) : An agent-based model of power and water infrastructure. *International Journal of Critical Infrastructure Protection*, 24 :144–165, mar 2019.

[TGD+19] R. Taormina, S. Galelli, H.C. Douglas, N.O. Tippenhauer, E. Salomons, and A. Ostfeld. A toolbox for assessing the impacts of cyber-physical attacks on water distribution systems. *Environmental Modelling & Software*, 112 :46 – 51, 2019.

[URN+19] Mathias Uslar, Sebastian Rohjans, Christian Neureiter, Filip Pröstl Andrén, Jorge Velasquez, Cornelius Steinbrink, Venizelos Efthymiou, Gianluigi Migliavacca, Seppo Horsmanheimo, Helfried Brunner, et al. Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain : A european perspective. *Energies*, 12(2) :258, 2019.

[VEM+15] Maria Vrakopoulou, Peyman Mohajerin Esfahani, Kostas Margellos, John Lygeros, and Göran Andersson. *Cyber-Attacks in the Automatic Generation Control*, pages 303–328. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[VIS96] Dennis Volpano, Cynthia Irvine, and Geoffrey Smith. A sound type system for secure flow analysis. *Journal of computer security*, 4(2-3) :167–187, 1996.

[vL90] Jan van Leeuwen. Graph algorithms. In *Algorithms and complexity*, pages 525–631. Elsevier, 1990.

[VPQVS16] C Vissers, Luís Ferreira Pires, Dick AC Quartel, and Marten Van Sinderen. *Architectural Design*. Springer, 2016.

[VS20] Thierry Vanelslander and Christa Sys. *Maritime Supply Chains*. Elsevier, 2020.

[WCZ+21] Yipeng Wu, Zhilong Chen, Xudong Zhao, Huadong Gong, Xiaochao Su, and Yicun Chen. Propagation model of cascading failure based on discrete dynamical system. *Reliability Engineering & System Safety*, 209 :107424, may 2021.

[WHN16] Benjamin Weinert, A. Hahn, and Oliver Norkus. A domain-specific architecture framework for the maritime domain. In *GI-Jahrestagung*, 2016.

[WW18] Lihui Wang and Xi Vincent Wang. *Latest Advancement in CPS and IoT Applications*, pages 33–61. Springer International Publishing, Cham, 2018.

[WWFR+21] S. Wurtzer, P. Waldman, A. Ferrier-Rembert, G. Frenois-Veyrat, J.M. Mouchel, M. Boni, Y. Maday, V. Marechal, and L. Moulin. Several forms of sars-cov-2 rna can be detected in wastewaters : Implication for wastewater-based epidemiology and risk assessment. *Water Research*, 198 :117183, 2021.

[WWH+19] Tao Wang, Xiaoguang Wei, Tao Huang, Jun Wang, Luis Valencia-Cabrera, Zhennan Fan, and Mario J Pérez-Jiménez. Cascading failures analysis considering extreme virus propagation of cyber-physical systems in smart grids. *Complexity*, 2019, 2019.

[WXZ+14] Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu. Srid : State relation based intrusion detection for false data injection attacks in scada. In Mirosław Kutyłowski and Jaideep Vaidya, editors,

Computer Security - ESORICS 2014, pages 401–418, Cham, 2014. Springer International Publishing.

[XBM21] Eduardo Xamena, Nélida Beatriz Brignole, and Ana Gabriela Maguitman. Structural analysis of relevance propagation models. *Knowledge-Based Systems*, page 107563, 2021.

[XCW+19] Yunpeng Xiao, Diqiang Chen, Shihong Wei, Qian Li, Haohan Wang, and Ming Xu. Rumor propagation dynamic model based on evolutionary game and anti-rumor. *Nonlinear Dynamics*, 95(1) :523–539, 2019.

[Yan20] Zejun Yang. *Resilience enhancement for interdependent critical infrastructures*. PhD thesis, University of British Columbia, 2020.

[YCM20] Zejun Yang, Ying Chen, and Jose Marti. Modelling cascading failure of a cps for topological resilience enhancement. *IET Smart Grid*, 3(2) :207–215, 2020.

[YŞYT20] Devran Yazir, Bekir Şahin, Tsz Leung Yip, and Po-Hsing Tseng. Effects of covid-19 on maritime industry : a review. *International maritime health*, 71(4) :253–264, 2020.

[Yu96] Eric Siu-Kwong Yu. *Modelling Strategic Relationships for Process Reengineering*. PhD thesis, CAN, 1996.

[YZG19] Dan Ye, Tian-Yu Zhang, and Ge Guo. Stochastic coding detection scheme in cyber-physical systems against replay attack. *Information Sciences*, 481 :432–444, 2019.

[YZY+17] Jun Yang, Chunjie Zhou, Shuanghua Yang, Haizhou Xu, and Bowen Hu. Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, 65(5) :4257–4267, 2017.

[ZDX+19] Boyu Zhu, Song Deng, Yunan Xu, Xinya Yuan, and Zi Zhang. Information security risk propagation model based on the seir infectious disease model for smart grid. *Information*, 10(10) :323, 2019.

[ZJJZ13] Yanli Zhang, Hongzhang Jin, Nuo Jia, and Aili Zou. Cascading failure evalution of ship fire-fighting system. In *2013 IEEE International Conference on Mechatronics and Automation*. IEEE, aug 2013.

[ZLDS+18] Yuriy Zacchia Lun, Alessandro D'Innocenzo, Francesco Smarra, Ivano Malavolta, and Maria Benedetto. State of the art of cyber-physical systems security : an automatic control perspective. *Journal of Systems and Software*, 149, 12 2018.

[ZPM21] Ewelina Ziajka-Poznańska and Jakub Montewka. Costs and benefits of autonomous shipping—a literature review. *Applied Sciences*, 11(10) :4553, 2021.

[ZR19] Remus Zăgan and Gabriel Raicu. Understanding of the cyber risk on board ship and ship stability. *Annals of "Dunarea de Jos" University of Galati. Fascicle XI Shipbuilding*, 42 :81–90, Nov. 2019.

[ZWC+19] Jianping Zeng, Shuang Wu, Yanyu Chen, Rui Zeng, and Chengrong Wu. Survey of attack graph analysis methods from the perspective of data and knowledge processing. *Security and Communication Networks*, 2019, 2019.

[ZY18] Yingrui Zhang and Osman Yağan. Modeling and analysis of cascading failures in interdependent cyber-physical systems. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 4731–4738. IEEE, 2018.

Annexes

Annexe

A *Information Technology* et *Operational Technology*

Les différences les plus significatives entre l'*Information Technology* et l'*Operational Technology* sont présentées dans la Table A.1.

TABLE A.1: Différences principales entre les systèmes IT et OT [BIM18]

Catégorie	**Système *IT***	**Système *OT***
Importance des critères de sécurité	►Confidentialité, Intégrité, et Disponibilité	►Disponibilité, Intégrité, et Confidentialité
Exigences de performances	►Non temps réel ►La réponse doit être cohérente ►Interaction d'urgence moins critique ►Pour la sécurité, un contrôle d'accès strictement limité peut être mis en œuvre dans la mesure nécessaire	►Temps réel ►Temps de réponse critique ►La réponse à l'interaction humaine et à toute autre interaction d'urgence est critique ►La réponse à l'interaction humaine et à toute autre interaction d'urgence est critique
Exigences de disponibilité	►Redémarrage acceptable ► Des pertes de disponibilité peuvent être tolérées en fonction des besoins opérationnels du système	►En raison des exigences de disponibilité des processus industriels, le redémarrage n'est pas accepté ►Une redondance des systèmes peut être nécessaire pour répondre aux exigences de disponibilité
Exigences de maîtrise des risques	►Gérer les données ►La confidentialité et l'intégrité des données sont primordiales ►La tolérance aux pannes peut être moins importante ►Les impacts potentiels peuvent entraîner des retards dans les domaines suivants : -autorisation du navire, -chargement/déchargement, -opérations commerciales	►Contrôler les opérations physiques ►La sécurité est primordiale, suivie par la protection du processus ►La tolérance aux pannes est essentielle, même un temps d'arrêt momentané n'est pas acceptable ►Les impacts potentiels sont : -la non-conformité ainsi, -les dommages causés au personnel à bord, -à l'environnement, -aux équipements et/ou à la cargaison

(suite de la table en page suivante)

Catégorie	Système *IT*	Système *OT*
Fonctionnement des systèmes	►Les systèmes sont conçus pour être utilisés avec des systèmes d'exploitation classiques ►Les mises à jour sont effectuées grâce à l'utilisation d'outils de déploiement automatisé	►Des systèmes d'exploitation disparates, et potentiellement propriétaires, souvent sans capacité native de sécurité ►Les modifications des logiciels doivent être effectuées avec précaution (généralement effectuées par les concepteurs), en raison des algorithmes de contrôle spécialisés et de matériel et logiciels modifiés
Contraintes en ressources	►Les systèmes sont spécifiés avec suffisamment de ressources pour supporter l'ajout d'applications tierces telles que des solutions de sécurité	►Les systèmes sont conçus spécifiquement pour le processus physique auquel ils sont associés et pourraient ne pas disposer de suffisamment de mémoire, et de ressources informatiques, pour supporter l'ajout de capacités de sécurité

Annexe B

Définitions liées à la notion de cybersécurité

L'ensemble de ces notions sont associées à celle de la cybersécurité.

Definition B.1. *La cyberprotection est l'ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles [Gar15].*

Definition B.2. *La cyberdéfense est l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels [Gar15].*

Definition B.3. *La résilience se définit comme la capacité d'une organisation à faire face à des évènements (incidents ou agression), à leur résister et à se rétablir. Appliquée au cyberespace, elle est appelée cyber résilience et définie comme la capacité d'un système d'information à résister à une panne et à revenir à son état initial après l'incident [Gar15].*

Annexe C

Signaux issus des capteurs

Dans cette annexe sont présentés les différents signaux complémentaires obtenus à partir des scénarios du premier et deuxième cas d'étude, dont les résultats sont respectivement explicités dans la section III.2.8 et la section III.3.9.

C.1 Premier cas d'étude

C.1.1 Deuxième scénario : PLC stop

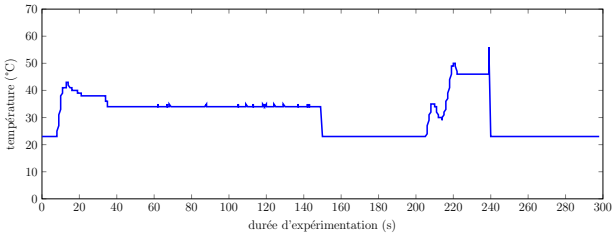
La Figure C.1 présente les valeurs des variables t_m, l_{ft}, et l_{ot} au cours du deuxième scénario.

C.1.2 Troisième scénario : *MiTM* sur la vitesse de rotation s_p

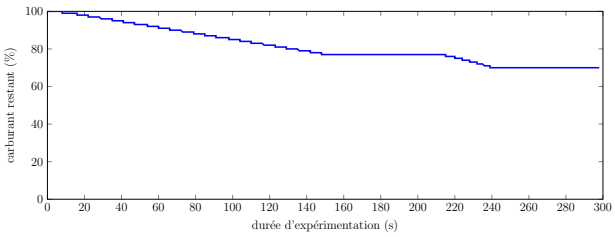
La Figure C.2 présente les valeurs des variables o_v, t_m, l_{ft}, et l_{ot} au cours du troisième scénario.

C.1.3 Quatrième scénario : *MiTM* sur l'ouverture de vanne o_v

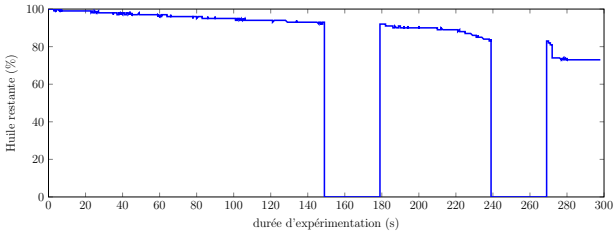
La Figure C.3 présente les valeurs des variables s_p, t_m, l_{ft}, et l_{ot} au cours du troisième scénario.



(a) Température t_m du moteur

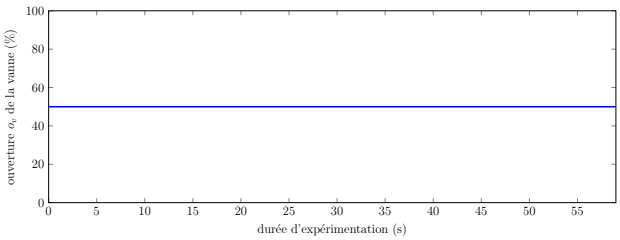


(b) Niveau l_{ft} de carburant

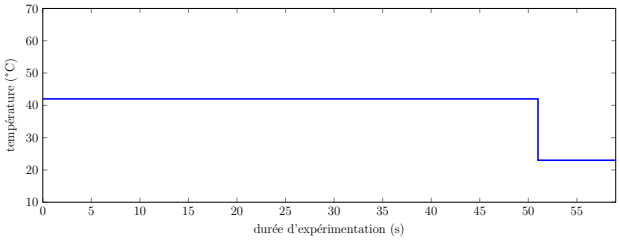


(c) Niveau l_{ot} d'huile

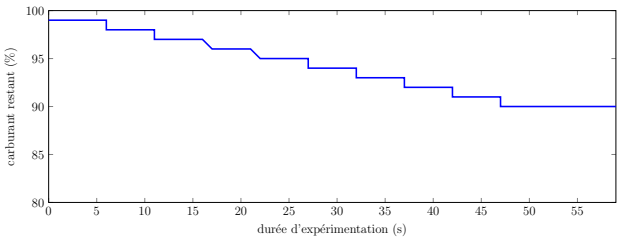
FIGURE C.1: Résultats du scénario *PLC stop*



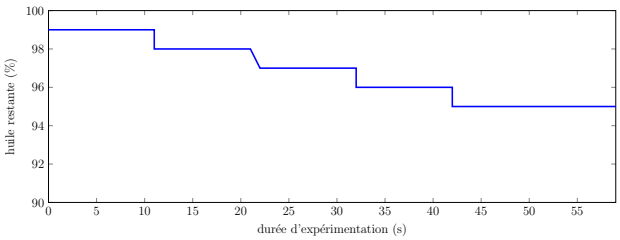
(a) Ouverture o_v de la vanne



(b) Température t_m du moteur

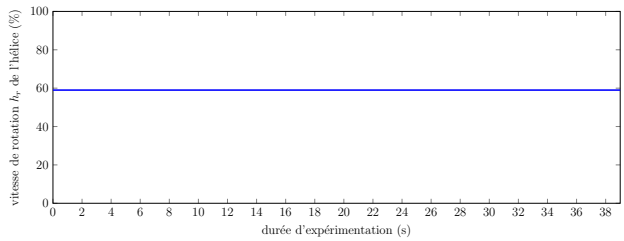


(c) Niveau l_{ft} de carburant

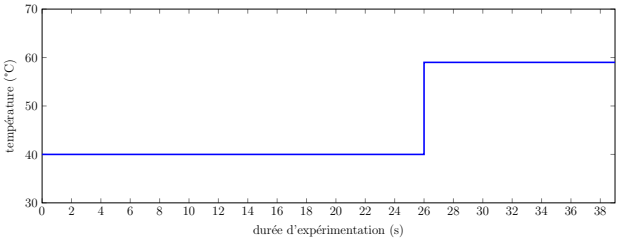


(d) Niveau l_{ot} d'huile

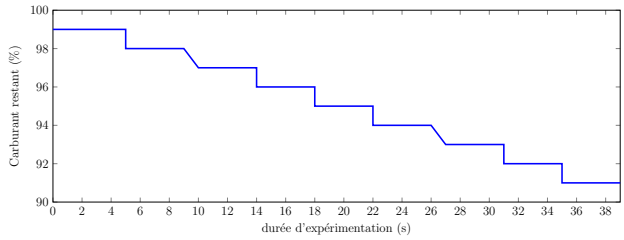
FIGURE C.2: Résultats du scénario *MiTM* sur la vitesse de rotation s_p



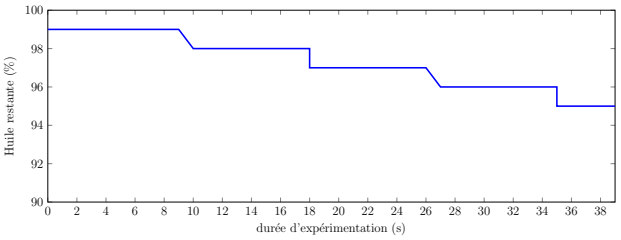
(a) Vitesse de rotation h_r de l'hélice



(b) Température t_m du moteur



(c) Niveau l_{ft} de carburant



(d) Niveau l_{ot} d'huile

FIGURE C.3: Résultats du scénario *MiTM* sur l'ouverture de vanne o_v

C.2 Deuxième cas d'étude

C.2.1 Premier scénario : attaque *DoS*

La Figure C.4 présente les valeurs d'activation des pompes PU1 et PU2 au cours du premier scénario.

C.2.2 Deuxième scénario

La Figure C.5 présente les valeurs d'activation des pompes PU10 et PU11 au cours du second scénario.

C.2.3 Troisième scénario

La Figure C.6 présente les valeurs d'activation des pompes PU4 et PU5 au cours du troisième scénario.

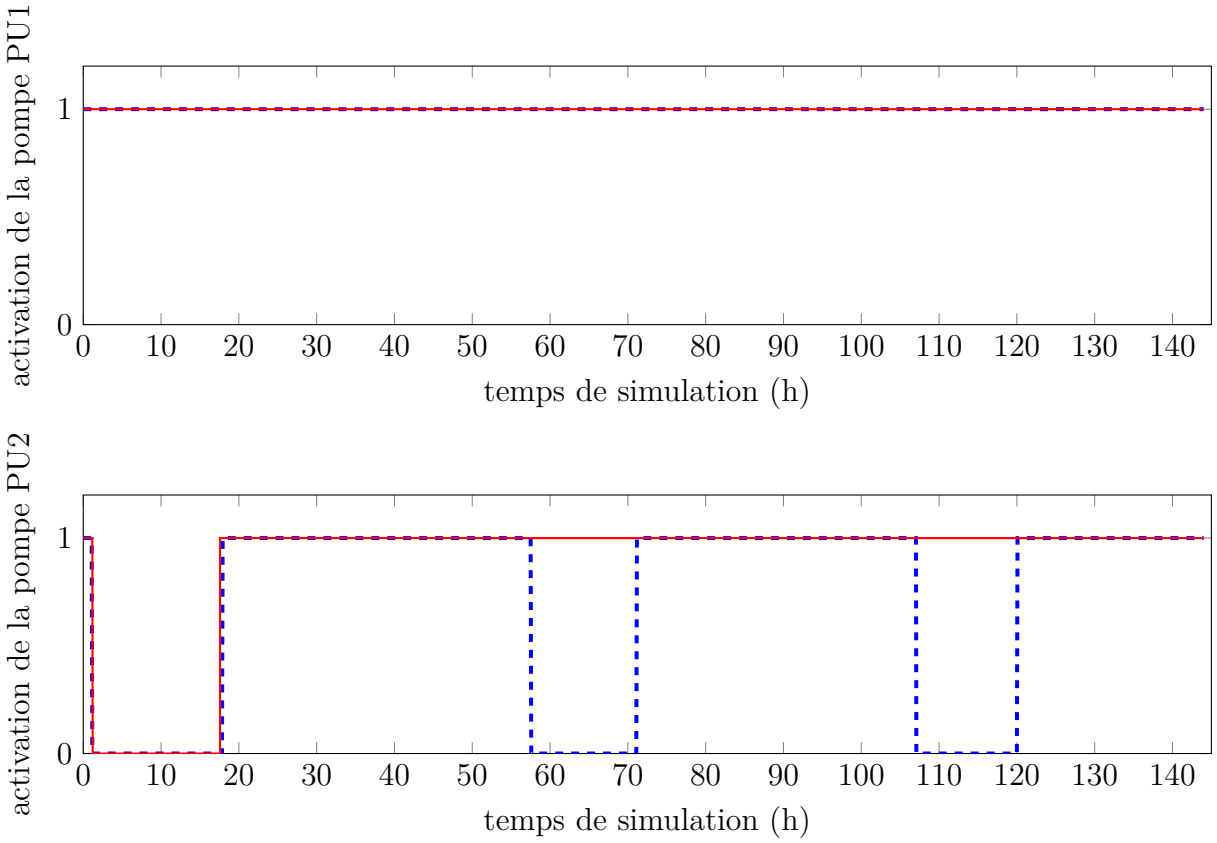


FIGURE C.4: Résultats du scénario 1

C.2.4 Quatrième scénario

La Figure C.7 présente les valeurs d'activation des pompes PU4 et PU5 au cours du quatrième scénario.

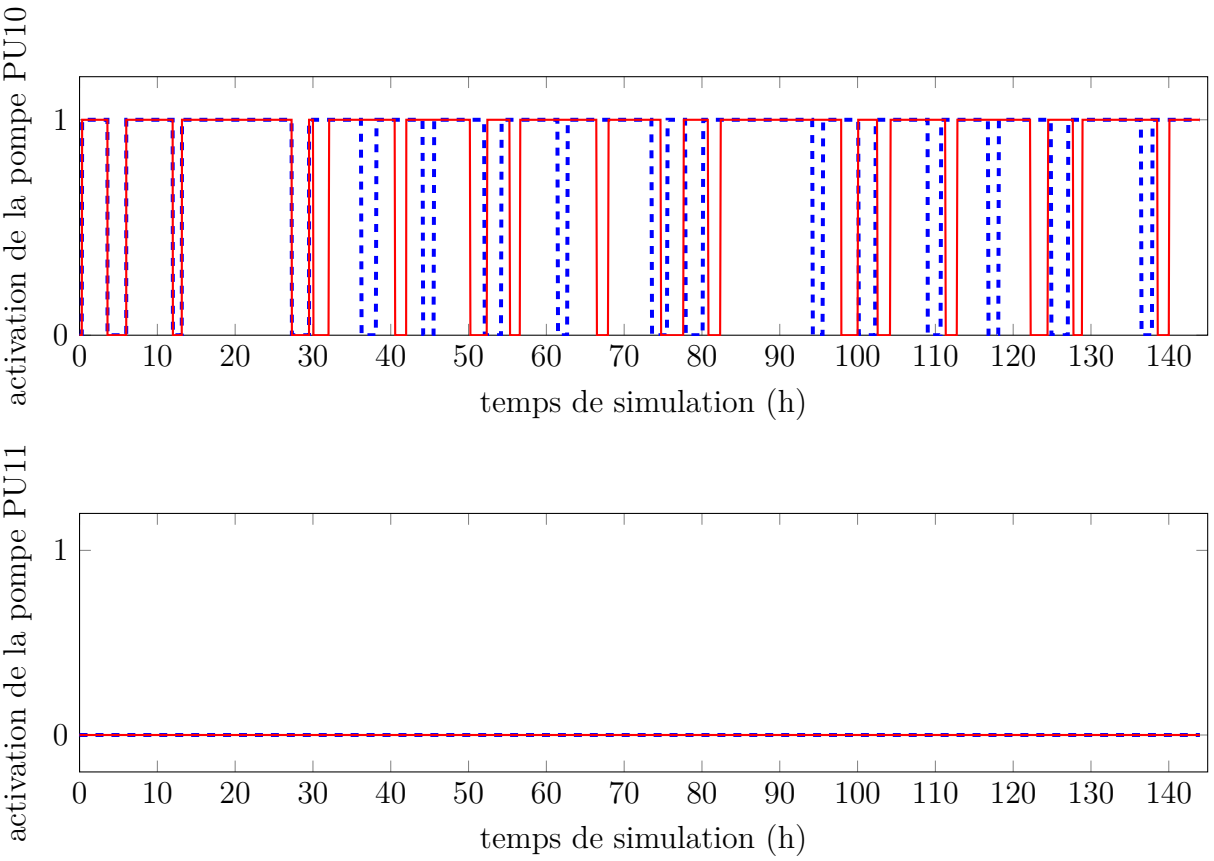


FIGURE C.5: Résultats du scénario 2

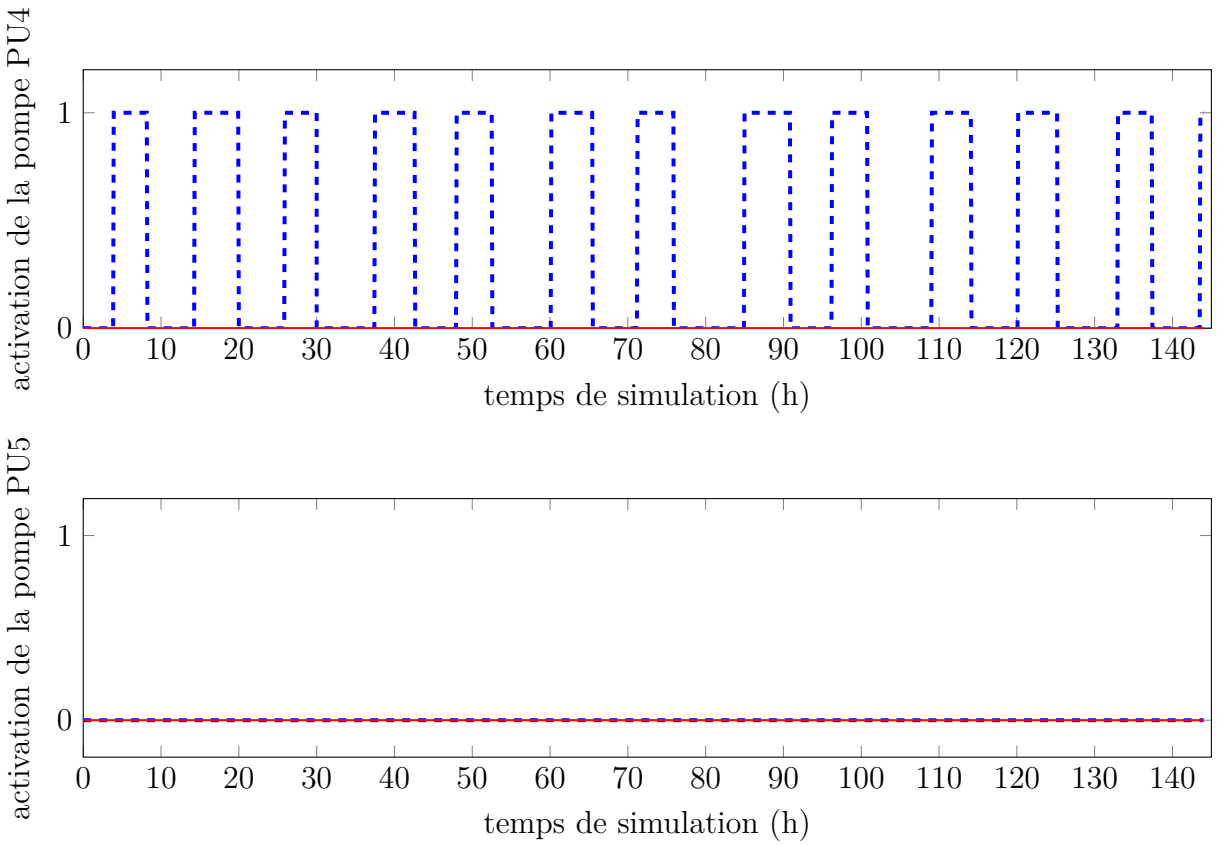


FIGURE C.6: Résultats du scénario 3

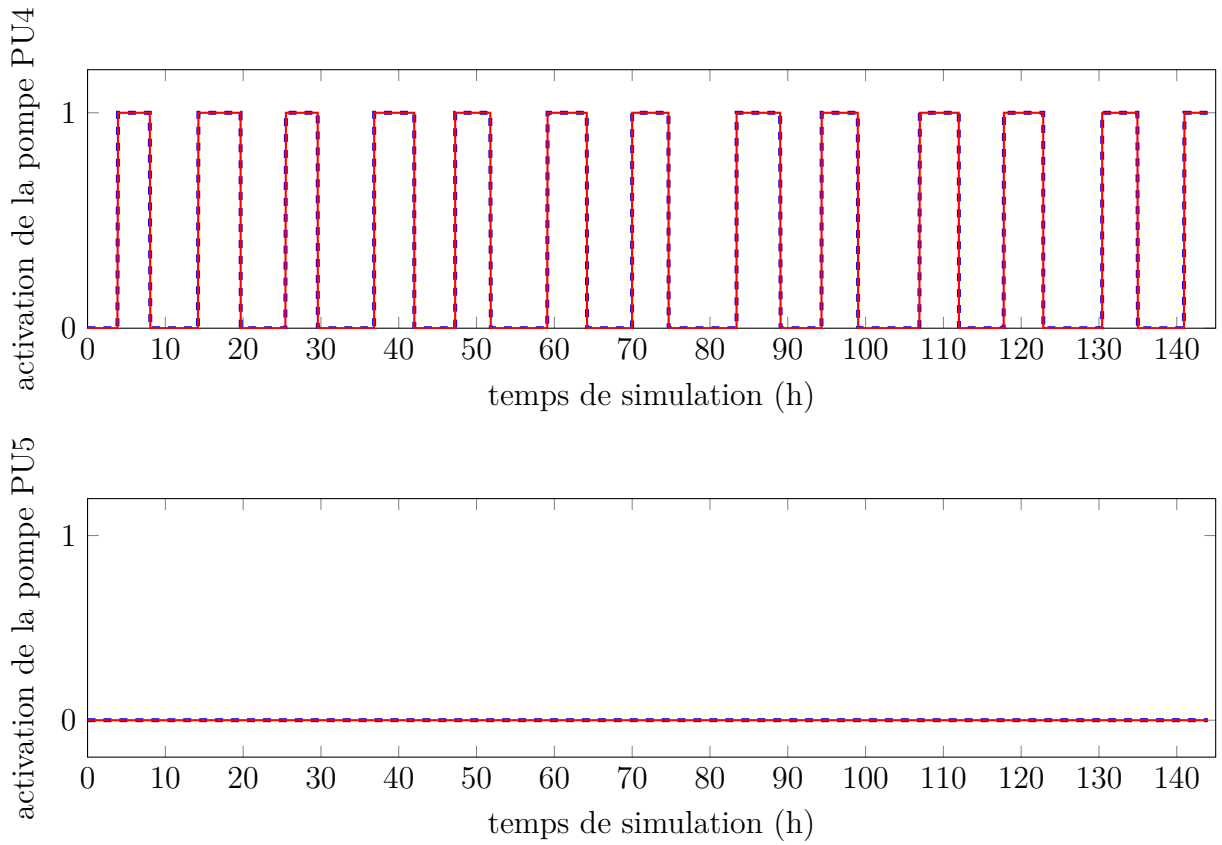


FIGURE C.7: Résultats du scénario 4

Annexe D Acronymes

AIS : *Automatic Identification System.*

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

API : Automate Programmable Industriel.

API : *Application Programming Interface.*

BFS : *Breadth First Search.*

C-ES : *Cyber-Enabled Ship.*

CPS : *Cyber-Physical System.*

DCS : *Distributed Control System.*

DDoS : *Distributed Denial of Service.*

DFS : *Deep First Search.*

DLL : *Dynamic Link Library.*

DoS : *Denial of Service.*

DQV : *Data Quality Vector.*

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité.

ECDIS : *Electronic Chart Display Information System.*

GITO : Glossaire Interarmées de Terminologie Opérationnelle.

GMDSS : *Global Maritime Distress and Safety System.*

IA : Intelligence artificielle.

IC : Infrastructure Critique.

ICS : *Industrial Control Systems.*

IHM : Interface Homme-Machine.

IMO : *International Maritime Organisation.*

INCOSE *International Council On Systems Engineering.*

IoT : *Internet of Things.*

IP : *Internet Protocol.*

IQV : *Information Quality Vector.*

ISM : *International Safety Management.*

MCO : Maintien en Conditions Opérationnelles.

NIS : *Network and Information System Security.*

nmap : *Network Mapper.*

NSA : *National Security Agency*

OMI : Organisation Maritime Internationale.

OIV : Opérateurs d'Importance Vitale.

OSE : Opérateurs de Services Essentiels.

PIB : Produit Intérieur Brut.

PLC : *Programmable Logic Controller.*

RM : *Risk Manager.*

SCADA : *Supervisory Control and Data Acquisition.*

SoS : *System of Systems.*

SQL : *Structured Query Language.*

SI : Système d'Information.

SIR : *Susceptible, Infected, Recovered.*

SVM : *Support Vector Machine.*

TEU : *Twenty-foot Equivalent Unit.*

UE : Union Européenne.

UV : *Unmanned Vehicle.*

DOCTORAT BRETAGNE LOIRE / MATHSTIC

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

Titre : Modèle d'analyse et d'évaluation de la propagation d'anomalies dans les systèmes cyber-physiques maritimes

Mot clés : Systèmes cyber-physiques ; cybersécurité maritime ; théorie des graphes ; analyse de risques ; propagation d'anomalies

Résumé : L'émergence de la 4ème révolution industrielle a fortement démocratisé l'utilisation de systèmes cyber-physiques (*Cyber Physical System (CPS)*) dans le secteur maritime. À bord, ils se caractérisent par divers composants interdépendants qui assurent le contrôle d'opérations physiques critiques à partir de commandes numériques. Une anomalie visant l'un de ces systèmes peut profiter de cette caractéristique pour se propager dans l'ensemble du navire, et engendrer des conséquences irréversibles. Premièrement, nous avons considéré la problématique des dépendances à l'échelle globale du navire pour caractériser l'importance de celles associées aux CPS. Ensuite, un modèle innovant de graphe 3-couches (numérique, physique, et variables système) a été formulé pour fournir une analyse structurelle du CPS. Diverses métriques de détection d'anomalies, basées sur l'analyse de la qualité, y sont intégrées pour amorcer les processus d'évaluation de la propagation dans un CPS maritime. Cette solution a été éprouvée sur deux CPS maritimes responsables de fonctions critiques : la propulsion et la distribution de l'eau. De nombreuses perspectives émergent de ces travaux pour fournir une réponse globale à la problématique d'évaluation de la propagation d'anomalies dans un navire.

Title: Model for analysis and evaluation of anomaly propagation in maritime cyber-physical systems

Keywords: Cyber-physical systems; maritime cybersecurity; graph theory; risk analysis; anomaly propagation

Abstract: The emergence of the 4th industrial revolution has democratized the use of cyber-physical systems (CPS) in the maritime sector. On board, they are characterized by various interdependent components that control critical physical operations through digital commands. An anomaly targeting one of these systems can benefit from this characteristic to easily propagate in the whole ship, and generate irreversible consequences. Firstly, we have considered the problem of dependencies at the global scale of the ship to characterize the importance of the dependencies associated with CPS. Then, an innovative 3-layer graph model (numerical, physical, and system variables) has been formulated to allow the CPS structural analysis. Various anomaly detection metrics, based on quality analysis, are integrated to initiate propagation assessment processes in a maritime CPS. This solution has been tested on two maritime CPS responsible for critical functions: propulsion and water distribution. Many perspectives emerge from this work to provide a global answer to ship anomalies propagation problems.