الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR- ANNABA UNIVERSITY
UNIVERSITE BADJI MOKHTAR - ANNABA

جامعة باجي مختار-عنابة

Faculté : Sciences de l'ingéniorat **Année : 2021**
Département : Electronique

THÈSE

Présentée en vue de l'obtention du diplôme de Doctorat 3ème Cycle

Intitulé

Développement d'Outils de Surveillance pour la Gestion de la Cybersécurité des systèmes d'Automatismes et de Contrôle de Procédés SCADA

Option : Multimédia et Communication Numérique

Par : ZERDAZI Imene

DIRECTEUR DE THÈSE : FEZARI Mohamed Professeur Université de Annaba

DEVANT Le JURY

PRESIDENT :	**DOGHMANE Noureddine**	**Pr. Université de Annaba**
EXAMINATEURS :	**BAYART Mireille**	**Pr. Université de Lille**
	ELHILALI Yassin	**MCA. Université UPHF**
	BOUKARI Karima	**MCA. Université de Annaba**

Cette thèse a été preparée au

Laboratoire d'Automatique et Signaux Annaba (LASA) et Centre de Recherche en Informatique, Signal et Automatique de Lille (CRIStAL)

ملخص

تتيح أنظمة الحصول على البيانات والإشراف عليها (SCADA) الإدارة عن بعد للمنشآت التقنية المتناثرة من خلال ضمان التشغيل الآلي المحلي الكامل ، والتسجيل الدقيق لجميع الأحداث ، وإدارة الإنذار الفعال للموظفين المعنيين ، بما في ذلك التحكم الكامل عن بعد. اليوم يستخدم SCADA الإنترنت كحل للاتصال نظراً للمزايا التي يوفرها ، مثل:

التحكم في المرافق الصناعية في أي مكان وفي أي وقت بتكلفة متواضعة جدا مقارنة بخطوط التخصص. ومع ذلك ، كيف يمكن تأمين الاتفاقية الدولية لمكافحة الجريمة المنظمة ضد الهجمات التي يشنها المجرمون السيبرانيون الذين سيحاولون المساس بهذه النظم باستخدام نقاط ضعفهم وعيوب خطوط الاتصال ؟ ولحل هذه المشكلة ، بينت الكتابات أن التقنيات الأمنية لتكنولوجيات المعلومات والاتصالات ، المستخدمة وحدها ، ليست كافية ، لأنه سيتم تجاهل التهديدات التي يتعرض لها الجزء المادي. لهذا السبب نحتاج إلى نهج يسمح لنا بتأمين كل من الأجزاء الإلكترونية والمادية.

ومن أجل معالجة المشكلة الأمنية التي تعاني منها أنظمة SCADA ضد الهجمات السيبرانية ، نقترح في هذا العمل أسلوباً للكشف عن الهجمات عن طريق الخداع من قِبَل نماذج الرسم البياني للبوند وتوليد علاقات زائدة تحليلية. أولا ، سنبدأ بتحليل مختلف الهجمات وأوجه الضعف في SCADA على المستويين الإلكتروني والفيزيائي من أجل الحصول على فكرة عامة عن ناقلات الهجوم. ثم سنعرض الأساليب المختلفة المقترحة لسلامة هذه النظم ، مع بيان الحدود أيضا. ثم سنقترح نهجا جديدا لتحسين سلامة نظم الإشراف ، يجمع بين نهج نظرية المعلومات ومراقبة النظريات. جميع الحلول سيتم اختبارها عن طريق المحاكاة المطبقة على ربع الروبوت الذكي روبوكارت ، ثم على نظام الروبوت تورتلبوت.

الكلمات الرئيسية: SCADA ، الأمن ، الهجمات الإلكترونية ، الرسم البياني للسندات ، النمذجة.

Résumé

Les systèmes de supervision et d'acquisition des données (SCADA) permettent une gestion à distance d'installations techniques dispersées en assurant une complète automatisation locale, un enregistrement précis de tous les événements, une gestion d'alarme efficace vers le personnel concerné et notamment un contrôle intégral à distance. Les SCADA d'aujourd'hui utilisent le réseau internet comme une solution de communication vu les avantages qu'il offre, tels que : contrôler les installations industrielles n'importe où et à n'importe quel moment avec un coût très modeste comparé aux lignes spécialisées. Cependant, comment sécuriser les SCADA face aux attaques lancées par les Cyber-malfaiteurs qui tenteraient de compromettre ces systèmes en utilisant leurs vulnérabilités et les failles des lignes de communications ? Pour résoudre ce problème, la littérature a montré que, utilisées seules, les techniques de sécurité pour les tech- nologies de l'information et de communication n'étaient pas suffisantes, car les menaces sur la partie physique seraient ignorées. C'est pourquoi nous avons besoin d'une approche qui nous permette de sécuriser tant la partie cyber que la partie physique.

Afin de répondre à la problématique de sécurité des systèmes SCADA contre les cyberattaques, nous proposons dans ce travail une méthode de détection d'attaques par tromperie par la modé- lisation Bond Graph et la génération des relations de redondance analytique (RRA). D'abord, nous commencerons par une analyse des différentes attaques et vulnérabilités des SCADA sur les niveaux cyber et physique afin d'avoir une idée générale des vecteurs d'attaques. Ensuite nous présenterons les différentes méthodes proposées pour la sécurité de ces systèmes, en en montrant également les limites. Puis nous proposerons une nouvelle approche pour améliorer la sécurité des systèmes de supervision, qui combine l'approche de la théorie de l'information et celle du contrôle de la théorie. Toutes les solutions seront testées par simulations appliquées sur un quart de robot intelligent RobuCar, puis sur le système de robotsTurtlebot.

Mots-clés : SCADA, sécurité, cyberattaques, bond graph, modélisation.

Abstract

Supervisory Control and Data Acquisition (SCADA) systems allow to remotely monitor distri- buted technical installations by ensuring a complete local automation, an accurate recording for all events, an efficient alarm management to the staff concerned and, in particular a complete remote control. Today SCADA system uses the internet as a communication solution because it offers advantages such as, controlling industrial installations anywhere and at any time at a very modest cost compared to the dedicated lines. However, how can SCADA systems be secured against attacks launched by cyber criminals seeking to compromise these systems, using the communication line flows and vulnerabilities of these systems ? To answer this question many works have opted for the security of the cyber part of SCADA systems. However, the literature has shown that using only the cyber techniques to deal with the security of a cyber-physical system such as SCADA it's not enough because the malicious physical actions, that might threa- ten the performance of the systems will be ignored. For this reason, a new method is needed to secure both layers (cyber and physical) at the same time.

In order to respond to the problem of SCADA security systems against cyber attacks, we propose in this work a method of detection of deception attacks by Bond Graph modeling and the generation of analytical redundancy relations (ARR). First, we will start with an analysis of the different attacks and vulnerabilities of industrial SCADA supervision systems on the cyber and physical levels in order to get a general idea of the attack vectors. Then we will present the different methods proposed for SCADA security, and we will present their limits as well. Afterwards, we will propose a new approach to improve the safety of supervision systems, which combines the information theory approach and the control theory approach. We will present a method of modeling and detecting deception attacks using the Bond Graph (BG) tool. All solutions are validated by simulations applicated on intelligent robot RobuCar.

Key-words : SCADA, sécurité, attaques, bond graph, modélisation

Remerciements

Cette thèse est l'aboutissement de plusieurs années et n'aurait jamais pu voir le jour sans le soutien et l'aide de nombreuses personnes qui m'ont accompagnée tout au long de cette épopée ! Je tiens donc ici à les remercier et à leur témoigner ma reconnaissance.

Je tiens tout d'abord à remercier mon directeur de thèse, Mohamed Fezari, d'avoir suivi mon travail durant ces années et ma co-directrice, Mireille Bayart, d'avoir accepté de m'inclure, durant un an, dans son groupe de travail (CI2S) du laboratoire CRIStAL et de m'avoir donné l'opportunité de vivre une expérience enrichissante lors de mon travail de thèse.

Je remercie également les membres de jury qui m'ont fait l'honneur d'évaluer et de valider mes travaux. Notamment Yassine El Hilali et Boukari Karima pour avoir accepté d'être les rapporteurs de ce travail : leurs conseils et remarques ont permis d'améliorer la version finale de ce document.

Je remercie le responsable du laboratoire LASA, Pr. Doghmane Nouredine, et le chef de département d'Electronique, Dr. Redjati Abdelghani, pour avoir mis à ma disposition tous les moyens nécessaires pour mener à bien ce travail.

Je remercie particulièrement Pr. Taibi Mohamed. C'est grâce à lui que j'ai pu intégrer le laboratoire IEMN-DAOE pendant mon master, ce qui m'a offert l'opportunité d'intégrer le laboratoire CRIStAL par la suite.

Je remercie aussi mes collègues dans notre groupe au laboratoire CRIStAL pour la bonne ambiance de travail, les conseils, l'aide et le soutien moral. J'ai passé d'agréables moments en votre compagnie.

Je remercie chaleureusement les membres de ma famille pour leurs encouragements. En particulier, je remercie mes parents pour leur soutien indéfectible, leurs conseils pertinents et surtout leur patience infinie. Je remercie également mon frère et ma sœur.

Merci à vous tous, ce travail n'aurait pas pu être mené à terme sans votre participation.

Table des figures

Liste des tableaux

Liste des Acronymes

ACRONYME	Description de l'Acronyme
API	Automate Programmable industriel
BG	Bond Graph
CIA	Confidentiality, Integrity, Availability
CRIStAL	Centre de Recherche en Informatique, Signal et Automatique de Lille DCS Distributed Control System
DDoS	Distributed Denial of Service
DNP	Distributed Network Protocol
FDI	Fault Detection and Isolation
FSM	Fault Signature Matrix
GSM	Global System for Mobile Communication
HMI	Human Machine Interface
IEEE	Institute of Electrical and Electronics Engineers IDS Intrusion Detection System
IoT	Internet of Things
IT	Information Technology
LAN	Local Area Network
MBR	Master Boot Record
MTU	Master Terminal Unit
MS-SQL	Microsoft SQL Server
NCS	Networked control System
OT	Operational Technology
PC	Personal Computer
PLC	Programmable Logic Controller
ROS	Robot Operating System
RRA	Relation de Redondance Analytique
RTU	Remote Terminal Unit
SCI	Système de Contrôle Industriel
SCADA	Supervisory Control and Data Acquisition TCP/IP Transmission Control Protocol/Internet Protocol TIC Technologie de l'Information et de Communication
TNT	Télévision Numérique Terrestre
UDP	User Datagram Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
2D	2 Dimensions
3D	3 Dimensions

Table des matières

Table des matières

CHAPITRE 1

Introduction

Contents

Dans ce chapitre, nous présentons le contexte de cette thèse, puis la motivation et le cadre de nos études. Ensuite, nous présentons nos principales contributions et nous concluons par la structure de ce document.

1.1 Contexte et motivation de la thèse

Dans les environnements industriels, les systèmes de contrôle et d'acquisition de données (SCADA) sont utilisés pour la surveillance et la gestion d'installations complexes telles que les centrales électriques, les raffineries, les chemins de fer, etc. Ces systèmes s'appuient sur des capteurs déployés sur une grande surface pour recueillir en temps réel des informations sur le processus industriel. Ces informations sont envoyées à un contrô- leur qui les traite et renvoie des commandes à des dispositifs de terrain tels que des actionneurs ou des vannes.

La sécurité est une question importante dans les systèmes SCADA. En effet, la perturbation de ces systèmes peut causer des dégâts aux infrastructures critiques telles que la distribution d'électricité, la distribution de pétrole et de gaz naturel, le traitement de l'eau et des eaux usées et les systèmes de transport. Cela peut avoir un impact sérieux sur la santé publique, la sécurité et peut entraîner des pertes économiques importantes [Loukas (2015)].

Le développement rapide des technologies de l'information et de la communication rend les systèmes SCADA modernes de plus en plus vulnérables aux attaques cyberné- tiques, non seulement sur les éléments cyber-infrastructures mais aussi sur les éléments physiques. La sécurité des systèmes SCADA contre les attaques malveillantes a fait l'objet de nombreuses recherches ces dernières années, en particulier après l'incident Stuxnet en 2010 [Kriaa et al. (2012)].

Les méthodes proposées pour améliorer la sécurité des infrastructures critiques peuvent être classées en deux grandes catégories : la protection et la surveillance. La protection des systèmes SCADA se concentre principalement sur la confidentialité, l'intégrité et la disponibilité des données par des mesures de sécurité de l'information [Tariq et al. (2019a)]. La surveillance des systèmes SCADA, en revanche, consiste à distinguer leur fonctionnement normal de leur fonctionnement anormal et à identifier les différents types d'attaques malveillantes (fig.1).

La sécurité des systèmes industriels cyber-physiques attire beaucoup d'attention depuis que le tristement célèbre logiciel malveillant Stuxnet a révélé le potentiel des attaques de sécurité réussies menées contre ces systèmes. Plusieurs auteurs ont étudié les exigences de prise en compte des nouveaux problèmes de sécurité lors de la conception des mécanismes pour les systèmes cyber-physiques. Cardenas et al. [Cardenas et al. (2008)] définissent la question du contrôle de la sécurité en analysant séparément le problème d'abord d'une information du point de vue de la sécurité, puis en examinant des questions de contrôle

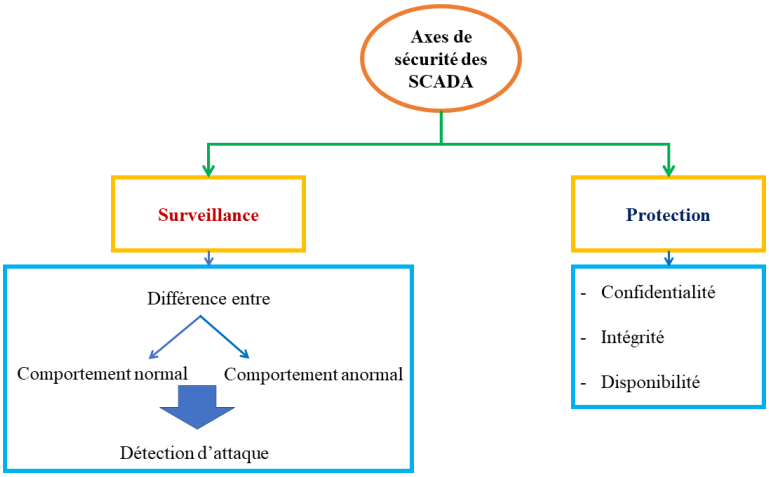

FIGURE 1 – Méthodes proposées pour l'amélioration de la sécurité des SCADA

spécifiques. Cardenas et al. [Cardenas et al. (2009)] soulignent également pour la première fois la différence entre la sécurité des TIC d'entreprise et la sécurité des systèmes cyber-physiques.

Dans la littérature, certains auteurs proposent l'utilisation d'une attestation physique au niveau de la couche cybernétique [Roth and Mcmillin (2016)], par exemple, un filigrane physique envoyé par la couche cybernétique à la couche physique, pour vérifier le comportement correct des processus physiques [Mo et al. (2015)]. [Barbosa et al. (2014)]. Arvani et al. [Arvani (2014)] décrivent un modèle de détection d'intrusion en utilisant des transformations d'ondelettes discrètes. Do et al. étudient dans [Do et al. (2014)] des stratégies pour traiter les cyber-attaques physiques à l'aide de méthodes de détection statistique. Ces propositions ne sont valables que lorsque les adversaires mènent des attaques sans avoir la capacité d'acquérir la connaissance des processus.
Le travail décrit dans cette thèse vise à traiter cette problématique. On s'intéresse particulièrement à la gestion de la surveillance des systèmes de supervision et de contrôle contre les attaques cyber-physiques.

1.2 Objectifs et contributions

Le terme de système cyber-physique, récemment inventé, intègre une infrastructure physique et un cadre cybernétique, dans le but de réduire la complexité et les coûts des systèmes de contrôle traditionnels dans les environnements industriels, par exemple : les systèmes de contrôle industriels sont à leur tour composés de capteurs, d'actionneurs et d'autres dispositifs de terrain qui interagissent avec les processus physiques. L'évolution technologique amène ces systèmes à combiner une couche physique qui englobe le cadre physique et une couche cybernétique qui englobe le cadre de communication et decalcul

[Genge et al. (2015)] via, par exemple, les protocoles SCADA.

Pour résoudre le problème de cybersécurité des SCADA, des méthodes du point de vue technologie de communication et de l'information existent. Ces méthodes permettent de fournir des solutions intégrées dans la couche de contrôle et de surveillance contre les cyberattaques. Par contre, ces solutions ne peuvent pas être intégrées dans la partie physique du SCADA. De plus, même dans la couche de contrôle de supervision, les attaquants ont parfois réussi à cacher une méthode de programmation spécifique pour modifier les signaux d'un actionneur et d'un capteur ainsi que pour reprogrammer les contrôleurs du système SCADA.

Cette thèse vise à aborder les questions de la cybersécurité des systèmes SCADA contre les attaques qui changent le comportement du système en modifiant les valeurs des capteurs ou bien la partie contrôle du système : ce type d'attaque connu sous le nom de "deception attack" en anglais, ou "attaque par tromperie" en français, peut passer sans être détecté par les systèmes de détection informatiques. Pour ce faire, notre première contri- bution est un examen du contexte général de sécurité des systèmes de contrôle industriel. Nous y décrivons les principales caractéristiques de ces systèmes et soulignons leur rôle important dans la gestion des installations vitales, économiques et nationales. Nous dé- taillons les différents profils d'attaquants et leurs motivations. Nous énumérons également quelques cyber-attaques importantes afin d'illustrer l'évolution et l'amélioration continue des vecteurs d'attaque.

Ensuite, nous proposons une nouvelle méthode pour modéliser les attaques qui changent le comportement du système SCADA (un changement de valeur sur un capteur ou sur la commande). Pour ce faire, nous avons utilisé l'outil de modélisation des systèmes pluri-disciplinaires Bond graph (BG).

Enfin, une première application pratique sur un système de véhicule intelligent (Robu- Car, disponible au laboratoire CRIStAL) a été effectuée pour détecter le type d'attaque mentionné ci-dessus, puis une seconde sur le système de robots Turtlebot.

1.3 Structure de la thèse

Cette thèse est organisée comme suit. Le chapitre 1 présente l'idée générale de la thèse, l'objectif et les principales contributions au sujet. Dans le chapitre 2 nous présentons le contexte général du système SCADA. Un paysage de vulnérabilités et de menaces visant les systèmes de contrôle industriel : nous offrons un large aperçu du contexte de sécurité des systèmes SCADA, en détaillant leurs caractéristiques et en apportant une description de leurs vulnérabilités et des menaces qui peuvent les cibler. Dans le troisième chapitre, nous présentons la méthode de détection des défauts dans les systèmes pluridisciplinaires utilisant les bond graph, méthode qui va être adaptée par la suite pour modéliser et détecter les cyberattaques dans les SCADA. Le quatrième chapitre

donne une vue d'ensemble de notre approche et l'application de notre méthode sur un système de véhicule autonome est présentée. Enfin, le cinquième chapitre présente une étude expérimentale sur la détection des attaques (modification d'une valeur capteur) sur un robot mobile autonome. Le dernier chapitre conclut la thèse et aborde les futurs travaux.

1.4 Liste des publications

Conférence Internationale

I. Zerdazi and M. Fezari, "SCADA Attack Modeling Using Bond Graph," 2019 Interna- tional Conference on Information and Communication Technologies for Disaster Manage- ment (ICT-DM), Paris, France, 2019, pp. 1-2. [Zerdazi and Fezari (2019)].

Publication dans une revue internationale référenciée

I. Zerdazi, M. Fezari and M. Ouziala, "Detection of Deception Attacks in Supervisory Control Systems Using Bond Graph," 2020 Journal of Automatic Control and Computer Sciences. Vol 54(2), pp :156–167. [Zerdazi et al. (2020)]

CHAPITRE 2

Les systèmes de supervision et de contrôle

Contents

Introduction

La sécurité des processus industriels et des infrastructures critiques a fait l'objet de beaucoup d'attention ces dernières années avec la croissance des cybermenaces contre ces processus qui sont contrôlés par des systèmes (SCADA) [Boyer (2009); Kang et al. (2009)]. L'utilisation massive des technologies de l'information et de la communication (TIC) dans les systèmes SCADA a ouvert de nouvelles voies pour mener des cyberattaques contre les infrastructures critiques qui se reposent de plus en plus sur des systèmes d'information [Stouffer et al. (2011)]. L'accès non autorisé à un système SCADA à des fins d'actions malveillantes ou de terrorisme pourrait avoir de graves conséquences sur les infrastructures critiques.

Le présent chapitre décrit le rôle important des systèmes SCADA dans le contrôle et la surveillance des infrastructures critiques, en abordant aussi, parmi leurs diverses vulnérabilités de sécurité, celles qui ont majoré les risques encourus par les infrastructures et conduit à de multiples cyberattaques dans les décennies passées.

Il est organisé comme suit : la section 2.1 donne un bref aperçu des systèmes SCADA et de leur architecture. La section 2.2 présente les différentes vulnérabilités de réseaux SCADA et détaille les récentes cyberattaques contre ce type de système cyber-physique. La section 2.3 décrit les approches existantes en matière de détection et d'attaque et la section 2.4 donne une conclusion sur la capacité des systèmes de détection traditionnels d'attaque à protéger les infrastructures industrielles et critiques.

2.1 Généralités sur les systèmes SCADA

L'industrie d'aujourd'hui est sous la contrainte d'autres exigences comme la localisa- tion des installations industrielles sur plusieurs sites géographiquement éloignés les uns des autres et aussi l'obligation de garantir le bon fonctionnement de toute l'instrumentation (capteurs, actionneurs . . . etc.). Cela a donc poussé les industriels à opter pour des solu- tions leur permettant d'assurer en permanence et à distance le contrôle et la surveillance de leurs installations, dans l'objectif de garantir :

—une plus grande rentabilité,

—une sécurité plus poussée,

—une sauvegarde de l'environnement,

—etc.

Grâce aux technologies de la communication numérique, notamment les services Web, la téléphonie mobile et la télégestion des installations industrielles, les systèmes SCADA ont très vite évolué et sont devenus incontournables, surtout pour des industries de moyenne et grande échelles.

Les systèmes SCADA sont des systèmes hautement distribués utilisés pour contrô- ler des installations géographiquement dispersées, souvent sur des milliers de kilomètres carrés, où l'acquisition et le contrôle des données sont essentiels au bon fonctionnement du système [Stouffer et al. (2015); Bailey and Wright (2003)]. Ils permettent aux opéra- teurs d'effectuer une surveillance et un contrôle centralisé des sites distants par le biais des réseaux de communication longue distance, y compris la surveillance des alarmes et le traitement des données d'états. De plus, les systèmes SCADA recueillent des données à partir d'une ou plusieurs installations éloignées, afin de les afficher graphiquement ou textuellement et de les transférer à un ordinateur central pour les enregistrer dans les bases de données. Cela permettra aux opérateurs de surveiller et de contrôler en temps réel l'ensemble du système à partir d'un emplacement central et d'envoyer des instruc- tions de contrôle à ces installations. Par conséquent, le SCADA rend inutile l'affectation d'un opérateur à des endroits éloignés ou à des visites fréquentes lorsque ces installations fonctionnent normalement.

Les types de signaux couramment utilisés par les systèmes SCADA pour la surveillance et le contrôle sont la température, la pression, le débit, la vitesse du moteur, l'état du générateur, les relais, etc. Un système SCADA peut contenir des centaines à des centaines de milliers de dispositifs d'entrées/sorties. Par exemple, une application SCADA très sim- plifiée consisterait à surveiller les niveaux d'eau de diverses sources comme les réservoirs et les citernes, lorsque le niveau d'eau dépasse un seuil prédéfini, SCADA active le système de pompage afin de transférer l'eau vers les réservoirs secondaires de niveau inférieur.

2.1.1 Les applications SCADA

La technologie SCADA a été appliquée au contrôle et à la surveillance des processus industriels et des infrastructures critiques répartis sur de vastes zones. Les systèmes étudiés nécessitent une intervention fréquente, régulière ou immédiate dans certains cas critiques. Il est important de noter que plus de 90% des infrastructures critiques des États-Unis sont contrôlées par SCADA et des systèmes industriels équivalents. De même, les systèmes SCADA sont utilisés pour surveiller la majorité des installations critiques en Europe. Les signaux recueillis à distance comprennent des alarmes, des indications d'état, des mesures liées au procédé étudié, etc. Les signaux envoyés par l'emplacement central du SCADA vers le site distant se limitent généralement à des changements discrets de bits binaires ou à des valeurs analogiques adressées à certains appareils au cours du processus. Les signaux analogiques communs que les systèmes SCADA doivent surveiller et contrôler sont les grandeurs physiques telles que la température, la pression, le débit et la vitesse du moteur. D'autre part, les signaux numériques typiques à surveiller et à contrôler sont les commutateurs de niveau, les commutateurs de pression, l'état du générateur, les relais et les moteurs, et un exemple de changement de bit binaire serait une instruction ordonnant l'arrêt d'un moteur. Très nombreux sont les domaines d'applications que nous pouvons énumérer, entre autres [Nicola et al. (2018)] :

—surveillance de systèmes industriels répartis géographiquement,
—industrie de l'eau (production, distribution, irrigation, eaux usées)
—production et distribution de l'énergie électrique
—industrie des hydrocarbures,
—industrie des produits chimiques,
—les opérateurs téléphoniques et de communication,
—enseignements et recherches scientifiques

2.1.2 L'architecture d'un système SCADA

Les systèmes SCADA sont utilisés dans de nombreux secteurs d'activité tels que les transports, l'énergie, les télécommunications et la distribution d'eau. La plupart de ces secteurs sont définis en Europe comme des secteurs critiques et, par conséquent, doivent être protégés. Les systèmes SCADA sont des systèmes cyber-physiques, composés de matériels et logiciels. Le matériel permet le transfert des données et des informations entre les différents composants des systèmes SCADA. Il comprend le centre de contrôle du processus industriel étudié, les équipements de communication tels que radio, ligne té- léphonique, câble ou satellite, et un ou plusieurs sites géographiquement distribués qui contrôlent et surveillent les actionneurs et les capteurs. Le logiciel est programmé pour indiquer au système quelles variables surveiller et quand le faire, quelles plages de para- mètres sont acceptables dans les modes de fonctionnement normaux du procédé étudié,

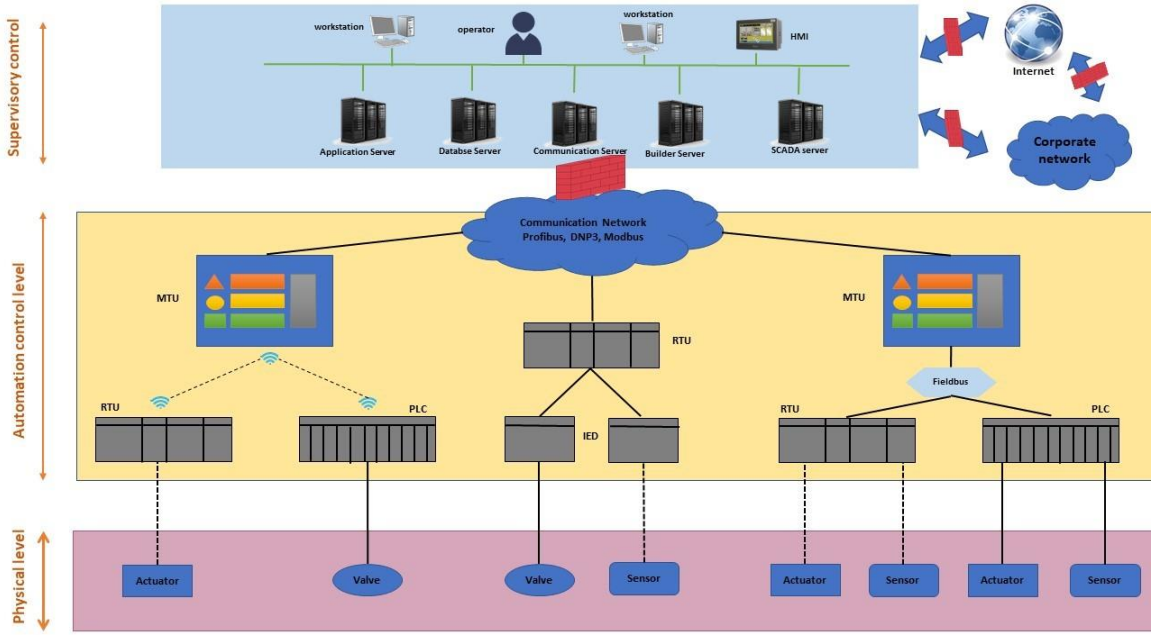

FIGURE 2 – Exemple d'architecture générale d'un SCADA

et quelle réponse déclencher lorsque les paramètres dépassent les valeurs acceptables.

Sous sa forme la plus simple, un système SCADA est composé essentiellement de (fig.2)(fig.3), [Stouffer et al. (2015)] :

- MTU (Master Terminal Unit) : il s'agit essentiellement d'une unité terminal maître qui peut être un automate programmable performant ou encore un PC automate, voire un DCS (systèmes de contrôle distribué) …etc.
- RTU (Remote Terminal Unit) : il s'agit essentiellement d'équipements automa- tiques de mesure et de contrôle. Les Automates programmables industriels (API) ou PLC (Programmable Logic Controller) peuvent être considérés comme des RTU.
- Un ou plusieurs serveurs locaux HMI (Human Machine Interface). C'est à ce ni- veau que les informations et les données relatives à l'installation industrielle sont centralisées. Il s'agit souvent d'un ordinateur serveur (équipé d'un système d'exploi- tation pour serveur comme par exemple Windows 2008 server ou encore Windows 2012 server). Ce PC serveur doit être équipé d'un logiciel de supervision et de surveillance souvent associé à un HMI (Interface Homme Machine), avec une confi- guration particulière pour que les vues des différentes installations industrielles surveillées soient publiées en tant que site sur ce serveur et puissent ensuite être visitées, entre autres à l'aide de navigateurs web, en tenant bien sûr compte des droits d'accès et des différentes sécurités qui lui sont associées.
- Des postes HMI clients locaux et/ou distants (en utilisant les technologies de com- munication tels que le WEB, le GSM …etc.) permettant à des personnes autorisées

d'intervenir sur le processus.

- Des interfaces et des passerelles de communication (Switch, Routeurs, points d'ac- cès, ponts, adaptateurs, …etc.)

2.1.3 Réseaux de communication SCADA

Le réseau de communication SCADA relie les différents composants du système de commande, c'est-à-dire les automates, les capteurs et les actionneurs. L'utilisation des réseaux de communication pour connecter les différents composants des systèmes de contrôle ajoute plus de flexibilité dans le système et réduit le coût de mise en œuvre de nouvelles installations.

Cependant, l'utilisation des réseaux de communication pour décentraliser les systèmes de contrôle traditionnels se fait au prix d'une complexité accrue de la conception des contrôles. Par exemple, l'analyse et la conception de l'ensemble du système doivent éga- lement faire face à de nouveaux défis théoriques dus à la perte des mesures et à l'échan- tillonnage variable dans le temps. L'intégration du système de contrôle (souvent appelé espace physique) et du réseau de communication (cyberespace) crée un nouveau degré d'interaction entre ces deux domaines.

Les protocoles de communication utilisés dans les systèmes de contrôle traditionnels doivent respecter les contraintes imposées par les normes industrielles. Certains proto- coles (comme Modbus, DNP et Profinet) ne sont pas conçus pour assurer la sécurité des informations dans le réseau traditionnel. Cependant, les réseaux de communication ac- tuels utilisent ces protocoles sur les communications TCP/IP et UDP/IP (ex., Modbus via TCP, DNP via TCP ou UDP, et Profinet via TCP). Bien que de telles combinaisons puissent fournir certains éléments de sécurité au niveau de leur couche de transport ou de réseau, cela ne suffit pas pour assurer la protection des données de contrôle.

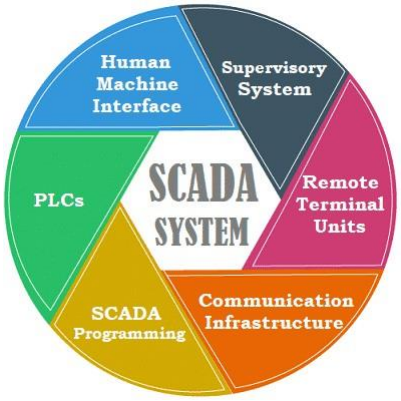

FIGURE 3 – Composants d'un SCADA [Raghvendra (2015)]

Il est à noter que l'architecture des systèmes SCADA a évolué au fil du temps en fonc-

tion des besoins des industriels et des développements technologiques [Adams (2004)]. Partant des protocoles de bus de terrain en série (comme par exemple Modbus, Profibus), en passant par les réseaux industriels basés sur l'Ethernet (par exemple, Modbus-TCP/IP, Ethernet/IP), allant jusqu'à l'utilisation des réseaux sans fil et des technologies de communication (par exemple, WLAN, WiMax ou Bluetooth). La normalisation des protocoles de communication a rendu les systèmes SCADA modernes plus vulnérables aux cyber- attaques. Plus précisément, de puissants attaquants peuvent s'introduire dans les canaux de communication, ce qui leur permet de modifier les signaux de commande, de contrôle ou les mesures des capteurs pour perturber le système.

- **systèmes SCADA monolitiques** : ils utilisent des unités centrales, les réseaux sont généralement inexistants, chaque système centralisé est autonome et ne com- porte pas de fonctions de connectivité. Ils utilisent des protocoles de communication propriétaires (fig.4).

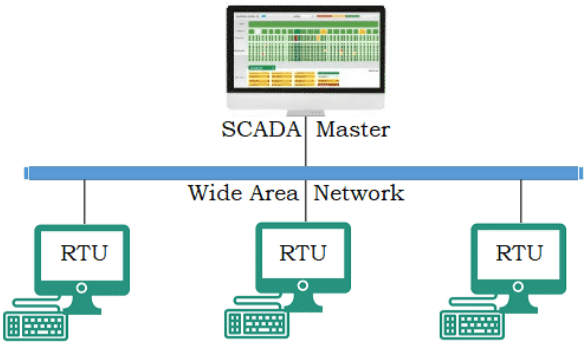

FIGURE 4 – SCADA de première génération [Raghvendra (2015)]

- **Systèmes SCADA distribués** : la génération suivante de systèmes SCADA a tiré parti des développements et des améliorations de la miniaturisation des systèmes et de la technologie des réseaux locaux (LAN). Elle utilisait des mini-stations in- formatiques plus petites et moins coûteuses que leur ordinateur central de première génération. Le système de contrôle était réparti sur plusieurs stations connectées par un réseau local. Chaque station était dédiée à la surveillance d'une tâche par- ticulière. Les protocoles de communication utilisés étaient encore propriétaires et non standards, et les mesures de sécurité n'ont pas été appliquées. (fig.5).

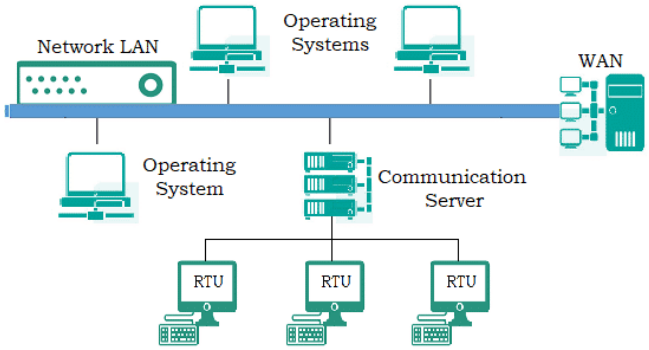

FIGURE 5 – Architecture SCADA distribuée [Raghvendra (2015)]

- **Systèmes SCADA en réseau** : la principale amélioration de la troisième gé- nération est l'ouverture de l'architecture du système, l'utilisation de normes et de protocoles ouverts et la possibilité de distribuer la fonctionnalité SCADA sur un réseau étendu (WAN) et non pas seulement sur un réseau local. Par consé- quent, ces systèmes sont composés de plusieurs SCADA répartis sur de vastes zones géographiques. En outre, l'utilisation de systèmes standards facilite la tâche de l'utilisateur pour connecter des périphériques tiers (tels que des moniteurs, des imprimantes, des lecteurs de disques, lecteurs de bandes magnétiques, etc.) au système (fig.6).

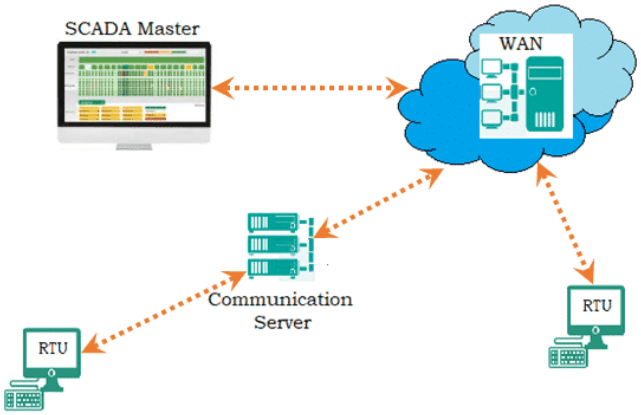

FIGURE 6 – Architecture SCADA en réseau [Raghvendra (2015)]

- **Internet des objets de quatrième génération** : l'industrie 4.0 (fig.7), égale- ment appelée "usine intelligente", fait référence à l'utilisation croissante et à l'in- tégration de la technologie de l'Internet des objets (IoT) dans les systèmes de contrôle industriel [Waidner and Kasper (2016)]. Elle résulte de la convergence des technologies de l'information (TI) et des technologies opérationnelles (OT) dans l'ensemble de la chaîne d'approvisionnement manufacturière. Ainsi, grâce à l'Inter- net des objets, les systèmes cyberphysiques communiquent et coopèrent entre eux et avec les humains en temps réel, et via l'informatique en nuage, pour améliorer

l'efficacité et de la productivité des systèmes de production. [Lee et al. (2014)].

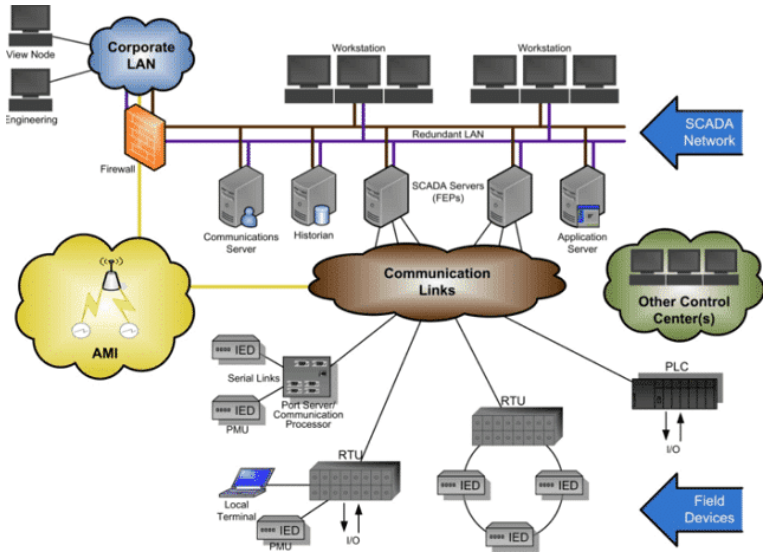

FIGURE 7 – Architecture SCADA IOT [Raghvendra (2015)]

Le domaine d'application des systèmes SCADA est donc très large et comprend la majorité des procédés industriels et des infrastructures critiques. Au cours des dernières années, plusieurs pays ont démontré leur volonté de développer des méthodes efficaces applicables contre les cybermenaces croissantes auxquelles ces infrastructures sont aujourd'hui confrontées. La Russie semble vouloir se joindre aux États-Unis d'Amérique pour créer un front commun contre la cybercriminalité et le cyberterrorisme, et la Chine améliore sa capacité nationale dans le domaine de la cybercriminalité. De nombreux pays de l'Union européenne ont adopté leur législation et leur réponse organisationnelle à ce danger réel, et les institutions européennes ont créé les Systèmes d'information de l'Agence nationale de sécurité en 2009 suite aux rapports sur le cyberterrorisme. La France a fait de la protection du SCADA une priorité de la recherche et du développement au niveau national.

Dans la suite, nous présentons l'évaluation des risques des réseaux SCADA, et nous décrivons quelques cyber-attaques récentes sur les réseaux SCADA.

2.2 Sécurité des systèmes SCADA

L'évolution de l'architecture SCADA et des technologies de communication rend les systèmes SCADA modernes de plus en plus vulnérables aux attaques cyber physiques, non seulement sur les infrastructures physiques, mais aussi sur le réseau de communication et le centre de contrôle [Fouladirad and Nikiforov (2005)]. En outre, les cyberattaques sont devenues un choix intéressant d'adversaires malveillants pour saboter les infrastructures critiques, car elles sont moins coûteuses, moins risquées et plus faciles à exécuter que

les méthodes physiques traditionnelles. Parfois, les adversaires malveillants intègrent les activités cybernétiques et physiques de manière coordonnée pour causer des dommages plus catastrophiques. De nombreux efforts de recherche ont été consacrés à l'amélioration de la sécurité des systèmes SCADA contre les cyberattaques. Par exemple, nous trouvons dans Nazir et al. [Nazir et al. (2017)] une classification des différentes méthodes proposées pour sécuriser les SCADA.

Afin de proposer une méthode appropriée pour sécuriser les systèmes SCADA contre les attaques malveillantes et protéger le processus industriel, il est nécessaire de faire un bilan des vulnérabilités des systèmes de supervision et d'examiner les cyberattaques préexistantes. En effet, l'analyse des vulnérabilités aide à comprendre quels sont les points sensibles des systèmes et comment ils pourraient être exploités pour lancer des attaques malveillantes. L'enquête sur les cyber incidents, d'autre part, nous donne une idée générale de la manière selon laquelle les attentats ont été perpétrés dans le passé, de sorte que des mesures de protection puissent être développées et mises en œuvre pour éviter de futures attaques.

2.2.1 Vulnérabilités des systèmes SCADA

Les vulnérabilités des protocoles de communication entre les composantes du SCADA et l'utilisation intensive d'Internet et des technologies de communication ont fait aug- menter les risques de cyber-attaques et ont ouvert de nouvelles voies pour réaliser des cyber-attaques contre des infrastructures critiques qui reposent sur les réseaux SCADA. Au cours de la dernière décennie, on a assisté à plusieurs cyber-attaques intentionnelles contre ces systèmes industriels. Les responsables de la plupart de ces cyber-attaques ont profité des vulnérabilités des infrastructures critiques, ont obtenu un accès non auto- risé aux réseaux SCADA qui surveillent les processus physiques, ont collecté des données échangées entre les installations et les opérateurs, ont placé des malwares qui ont perturbé le fonctionnement normal du système, etc. Selon [Fovino (2013)] on peut citer quelques vulnérabilités des SCADA, telles que : les vulnérabilités architecturales, les vulnérabili- tés des protocoles de communications, les vulnérabilités des logiciels et du matériel, les vulnérabilités de la politique de sécurité.

1. **Les vulnérabilités architecturales :** En général, les architectures SCADA mo- dernes ne sont pas si différentes du principe des architectures utilisées dans les années 80 et 90, à l'exception du passage d'un environnement "isolé" à un environ- nement "ouvert". Cette caractéristique avancée rend les systèmes SCADA modernes de plus en plus vulnérables aux cyber-attaques. Tout d'abord, la majorité des ré- seaux SCADA stocke les données du processus dans des unités d'historisation du réseau de l'entreprise. Cette flexibilité laisse une porte dérobée aux malwares infor- matiques pour entrer dans le réseau du processus par le biais du réseau d'entreprise.

Deuxièmement, un grand nombre de systèmes SCADA utilise des applications web pour surveiller les processus physiques : cette connexion directe à l'internet pourrait être une voie pour les pirates informatiques pour pénétrer dans le réseau SCADA [Poulsen (2003)]. De plus, les points d'accès locaux aux appareils de terrain pour- raient constituer une autre porte permettant aux agents malveillants de pénétrer dans le réseau de terrain du système. Enfin, les adversaires peuvent s'introduire dans le réseau SCADA en se connectant au réseau du fournisseur, qui est disponible dans les systèmes SCADA modernes [Yuan et al. (2011)].

2. **Les vulnérabilités des protocoles de communication :** Historiquement, per- suadés que leurs systèmes seraient isolés des autres réseaux, les concepteurs de SCADA n'ont pas accordé beaucoup d'attention aux problèmes de sécurité tels que le mécanisme de vérification de l'intégrité, le mécanisme d'authentification, l'anti-répudiation et le mécanisme d'anti-rejeu. De nombreux protocoles de communication SCADA, notamment Modbus, DNP3 et Allen-Bradley Ethernet/IP, ne disposent pas de fonctions d'authentification permettant de prouver l'origine ou la fraîcheur du trafic réseau [Reaves and Morris (2009)]. Ces systèmes sont donc susceptibles de faire l'objet d'un déni de service (DoS), les attaques de type "man- in-the-middle" et les attaques par rediffusion.
   Les systèmes SCADA traditionnels, mis en œuvre avec des protocoles de communication propriétaires, étaient considérés comme sûrs. Cependant, la "sécurité par l'obscurité" n'est pas évidente dans le monde moderne. La technologie de l'information a évolué rapidement, conduisant à l'adoption, dans la majorité des systèmes SCADA modernes, de protocoles de communication communs tels que Ethernet, TCP/IP ou les réseaux sans fil [Wei Gao et al. (2010)] comme les fréquences radio, la communication par satellite, IEEE 802.x et Bluetooth.
3. **Les vulnérabilités des logiciels et du matériel :** Afin de répondre aux exi- gences industrielles, les systèmes SCADA sont devenus de plus en plus complexes, tant au niveau des logiciels que du matériel. Il est inévitable que les systèmes SCADA modernes contiennent des défauts de logiciel et des pannes de matériel. Les défauts logiciels typiques peuvent être répertoriés comme [Zhu et al. (2011)] : dépassement de tampon, injection SQL, chaîne de format, etc. En fait, le cyber- incident [Poulsen (2003); Kabay (2010)] était dû aux vulnérabilités du logiciel MS- SQL. En outre, les systèmes SCADA sont des systèmes d'exploitation en temps réel, ce qui empêche les systèmes de mettre en œuvre les algorithmes de cryptage traditionnels en raison de l'exigence de disponibilité des données. Cette demande en temps réel rend difficile la mise en œuvre d'algorithmes de cryptage des données, exposant les systèmes SCADA à des attaques d'intégrité.
4. **Les vulnérabilités de la politique de sécurité :** Plusieurs politiques de sé- curité, telles que les correctifs ou la mise à jour des anti-virus, peuvent avoir un

impact négatif sur les systèmes SCADA. L'utilisation de plusieurs correctifs et logi- ciels anti-virus permet souvent (1) d'accéder au réseau Internet, ce qui peut rendre les systèmes dépendants d'agents malveillants et (2) d'exiger un redémarrage du système, ce qui peut entraîner la perturbation des systèmes. Une excellente démonstration de cette vulnérabilité est le cyber-incident mis en cause dans l'arrêt d'une centrale nucléaire après une mise à jour du logiciel [Krebs (2008)]. Il est donc préférable d'utiliser des correctifs logiciels et de mettre rarement à jour le logiciel anti-virus afin de conserver le réseau de processus aussi isolé quepossible.

2.2.2 Les attaques spécifiques aux systèmes SCADA

Au-delà des vulnérabilités dues à la dépendance croissante de leurs communications à internet, les systèmes SCADA sont aujourd'hui confrontés à des menaces importantes de cyberattaques en raison des vulnérabilités de protocoles de communication mis en œuvre dans ces réseaux [Morris and Pavurapu (2010); Fovino et al. (2009)].

Dans le passage suivant nous présentons par ordre chronologique des cybers incidents survenus aux SCADA [Yaseen (2019)].

Explosion d'un gazoduc en Sibérie. (1982).

Le premier cyber-incident visant la sécurité des infrasructures critiques pourrait être l'explosion du gazoduc en Sibérie en 1982. On pensait qu'un cheval de Troie avait été implanté dans le système SCADA qui contrôlait le gazoduc sibérien. En modifiant la co-opération des pompes, des turbines et des vannes, le programme malveillant avait fait augmenter la pression dans les gazoducs bien au-delà du niveau acceptable, ce qui avait conduit à une explosion d'une puissance de trois kilotonnes de TNT [Agudo (1995); Tsang (2010)].

Explosion d'un pipeline en Russie. (1999).

En 1999, des pirates informatiques se sont introduits dans Gazprom, la plus grande compagnie de gaz russe, grâce à la collaboration d'un employé mécontent. On pensait que l'attaquant avait utilisé un cheval de Troie pour prendre le contrôle du tableau de distribution central qui contrôlait le flux de gaz dans les conduits. Cet incident a été rapporté en 2000 par le ministère de l'Intérieur de Russie [Cárdenas et al. (2011); Tsang (2010)].

Maroochy en Australie. (2000).

En 2000, M. Boden, un ex-employé mécontent, a utilisé un ordinateur portable et un émetteur radio pour prendre le contrôle de 150 stations de pompage des eaux usées dans le comté de Maroochy, dans le Queensland [Slay and Miller (2008)], en Australie. Sur une

période de trois mois, il a déversé un million de litres d'eaux usées non traitées dans un égout pluvial d'où elles s'écoulaient vers les cours d'eau locaux. L'attaque a été motivée par sa vengeance après qu'il a échoué à obtenir un emploi au Conseil du comté de Ma- roochy.

Infection par ver dans une centrale nucléaire - Slammer aux États-Unis. (2003). En janvier 2003, un ver Slammer a pénétré dans un réseau informatique privé de la centrale nucléaire de Davis-Besse, dans l'Ohio, et a désactivé un système de surveillance de sécurité pendant près de cinq heures, bien que le personnel de la centrale ait cru que le réseau était protégé par un pare-feu [Poulsen (2003)]. Le ver Slammer s'est propagé du réseau d'entreprise aux systèmes SCADA qui contrôlent la centrale nucléaire en ex- ploitant les vulnérabilités du MS-SQL. Il a été rapporté que l'IHM et les ordinateurs de traitement de la centrale avaient été touchés pendant des heures, causant d'importants problèmes aux opérateurs du système.

Panne de la centrale de production hydroélectrique de Taum Sauk aux États- Unis.(2005).

L'incident de Taum Sauk du 14 décembre 2005 [Watkins and Rogers (2008)] n'était pas une attaque mais une défaillance d'une centrale hydroélectrique. Pour diverses rai- sons, notamment des défauts de conception/construction, des erreurs d'instrumentation et des erreurs humaines ont été attribuées à la défaillance catastrophique d'un réservoir supérieur. Il a été rapporté dans [Watkins and Rogers (2008)] que les capteurs n'ont pas indiqué que le réservoir était plein et que les pompes n'ont pas été arrêtées avant que l'eau ne déborde pendant environ 5-6 minutes. Ce débordement a affaibli le mur de protection, ce qui a entraîné l'effondrement du réservoir. Bien que cet incident ne soit pas une at- taque, le type des faiblesses qui l'ont causé peut être exploité pour réaliser des attaques indétectables dans des infrastructures critiques. Par exemple, les auteurs [Amin et al. (2013)] ont conçu des attaques furtives sur un canal d'irrigation SCADA en envoyant des signaux de retour compromis (c'est-à-dire de fausses mesures de capteurs) au centre de contrôle.

Stuxnet en Iran. (2010).

En 2010, le malware complexe Stuxnet [Brunner et al. (2010); Knoepfel (2013)] a été découvert en Iran. Il visait les automates connectés à une centrifugeuse nucléaire utili- sée pour l'enrichissement de l'uranium. Stuxnet installe un programme malveillant qui remplace le fichier original des automates d'une manière indétectable par l'opérateur de l'automate [Chen and Abu-Nimeh (2011)]. Le but ultime de Stuxnet était de saboter les centrales nucléaires où les fluctuations de vitesse pouvaient faire voler les centrifugeuses

en éclats et les détruire [Langner (2011)].

Telvnet au Canada. (2012).

Une brèche dans le pare-feu interne et les systèmes de sécurité de Telvent Canada [Rashid (2012)], une entreprise qui fournit des outils d'administration et de surveillance à distance au secteur de l'énergie, a été découverte le 10 septembre 2012. Après avoir pénétré dans le réseau, les intrus ont volé des fichiers de projets liés au produit OASyS SCADA, un outil d'administration à distance permettant aux entreprises de combiner des équipements informatiques plus anciens avec les technologies modernes de "réseau intelligent". Il est très probable que les adversaires aient recueilli des informations sur le nouveau produit afin de découvrir les vulnérabilités du logiciel et de mieux préparer de futures attaques contre les systèmes SCADA du secteur de l'énergie.

Shamoon en Arabie Saoudite.(2012).

En 2012, l'attaque Shamoon, basée sur un logiciel malveillant, a été découverte. Shamoon a été utilisé pour le cyber-espionnage dans le secteur de l'énergie, et il visait une entreprise pétro-chimique au Moyen-Orient [Zhioua (2013)]. L'objectif principal de Shamoon était d'effacer les données des ordinateurs fonctionnant sous Microsoft Windows, puis de modifier le Master Boot Record (MBR) du support de stockage, rendant l'ordi- nateur inaccessible. Shamoon a permis la destruction complète du contenu d'environ 30 000 postes de travail de cette installation.

Empoisonnement de l'eau potable aux États-Unis (2013).

L'incident [Credeur (2013)] s'est produit à la station d'épuration de Carters Lake dans le comté de Murray, au nord-ouest d'Atlanta, aux États-Unis, le 26 avril 2013. On pense que quelqu'un est entré dans la station de traitement de l'eau et a manipulé l'équipement qui contrôle la quantité de chlore et de fluorure à ajouter à l'eau. Bien que cet incident ne soit pas une cyber-attaque, des scénarios d'attaque similaires peuvent être réalisés si le réseau d'eau est connecté à Internet. Par exemple, au lieu d'entrer directement dans la station, les intrus peuvent s'introduire dans le réseau SCADA et modifier les points de consigne des niveaux de chlore et de fluorure.

BlackEnergy en Ukraine. (2015).

BlackEnergy est un cheval de Troie qui est utilisé pour mener des attaques DDoS, du cyber-espionnage et des attaques de destruction d'informations. Vers 2014, un groupe spé- cifique d'utilisateurs de BlackEnergy a commencé à déployer des plugins liés au SCADA pour les victimes des SCI (Systèmes de Contrôle Industriel) et des marchés de l'énergie dans le monde entier. Cela indiquait un ensemble de compétences unique, bien supérieur

à la moyenne des maîtres de réseau de zombies DDoS.
Depuis la mi-2015, le groupe APT BlackEnergy utilise activement des courriels de harpon- nage transportant des documents Excel malveillants avec des macros destinés à infecter les ordinateurs d'un réseau ciblé. Cependant, en janvier 2016, les chercheurs de Kaspersky Lab ont découvert un nouveau document malveillant, qui infecte le système avec un che- val de Troie BlackEnergy. Contrairement aux documents Excel utilisés lors des attaques précédentes, il s'agissait d'un document Microsoft Word.
A l'ouverture du document, l'utilisateur se voit présenter un dialogue recommandant d'ac- tiver des macros afin de pouvoir en visualiser le contenu. L'activation des macros déclenche l'infection par le malware BlackEnergy [Robert M. Lee and Conway (2016)].

Attaque d'un pipeline aux États-Unis (2018).

En mars 2018, une attaque massive a compromis les systèmes de données alimentant les principaux gazoducs sur tout le territoire américain. Les attaquants ont piraté le système de communication électronique d'un vendeur qui gère les échanges de documents d'ordinateur à ordinateur avec les clients [Krauss (2018)].

Le tableau suivant donne une classification des différentes attaques selon le secteur (tab.2.1).

Secteur	Attaque	Année	Pays
Pétrole et gaz	Explosion d'un gazoduc	1982	Sibérie
	Explosion d'un pipeline	1999	Russie
	Shamoon	2012	Arabie Saoudite
	Attaque d'un pipeline	2018	Etats Unis
Energie	Production hydraulique	2005	Etats-Unis
	Tevnet	2012	Canada
	BlackEnergy	2015	Ukraine
Eau et Assainissement	Marrochy	2000	Australie
	Explosion de l'eau potable	2013	Etats-Unis
Nucléaire	Slammer	2003	Etats-Unis
	Stuxnet	2010	Iran

Tableau 2.1 – Classification des attaques SCADA par secteur

2.2.3 Aspects de sécurité dans les systèmes SCADA

Les trois niveaux de sécurité de haut niveau qui s'appliquent aux systèmes de supervi- sion industriel, dans tous les niveaux sont la confidentialité, l'intégrité et la disponibilité (CIA Triad en anglais).

1. **Confidentialité :** C'est la capacité à empêcher la divulgation d'informations à des personnes ou à des systèmes. Elle peut être assurée par le cryptage des données

personnelles pendant leur transmission et en limitant l'accès aux lieux où elles sont stockées (la base de données, fichiers et sauvegardes). Une violation de la confidentialité se produit lorsqu'une partie non autorisée tente d'accéder aux dossiers personnels de l'industrie [Pham et al. (2010)]. La confidentialité est obtenue en empêchant l'adversaire de modifier l'état du système physique par l'écoute des canaux de communication entre les capteurs et le contrôleur et aussi entre le contrôleur et l'actionneur.

2. **Intégrité :** L'intégrité se réfère à la conservation des données sans modification, sauf si elle est effectuée par un utilisateur autorisé. L'intégrité est atteinte lors- qu'un adversaire modifie ou supprime accidentellement ou dans l'intention de nuire des données importantes. Ainsi, les destinataires reçoivent des données fausses et supposent qu'elles sont vraies. L'intégrité est obtenue en prévenant, détectant ou bloquant les attaques par tromperie (Deception attack) sur les informations envoyées et reçues par les capteurs et les actionneurs ou les contrôleurs [Madden et al. (2010)].
3. **Disponibilité :** Pour qu'un système puisse remplir sa fonction, le service doit être disponible quand il est nécessaire. La haute disponibilité des CPS vise à fournir un service en empêchant toute interruption de calcul, de contrôle et de communication. Le système doit être capable de fournir le service même en cas de panne matérielle, de mise à niveau du système, de panne de courant ou d'attaques par déni de service [Work et al. (2008)].

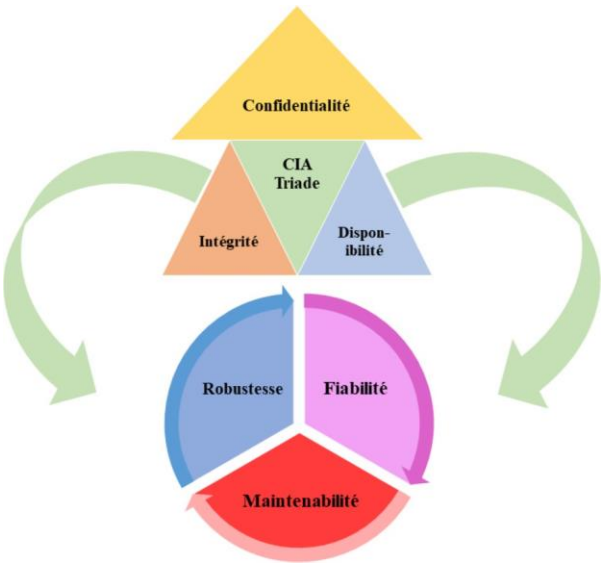

FIGURE 8 – Aspects de sécurités dans les SCADA

Les objectifs de sécurité sont toujours suivis par la sécurité, la fiabilité, la robustesse et la maintenabilité du système (l'objectif suprême pour les systèmes critiques) (fig.8). Selon la CIA triade, une perte d'intégrité et de disponibilité entraîne des attaques de tromperie

(Deception attack). Un type particulier d'attaque par tromperie est l'attaque par réponse (replay attack) sur la mesure d'un capteur. Les attaques par injection de fausses données (false data injection) constituent une autre catégorie d'attaques par tromperie [Tariq et al. (2019b)].

2.2.4 Les attaques cyber-physiques contre les SCADA

Les cyberattaques visant les systèmes SCADA peuvent être classées en attaque par tromperie (deception attack) et en attaque par déni de service (DoS), qui entraînent respectivement une perte d'intégrité et de disponibilité. L'intégrité des systèmes SCADA peut être définie comme la capacité à maintenir les actions opérationnelles en prévenant, détectant, et faisant face aux attaques par tromperie. Les attaques par tromperie peuvent inclure une mesure de capteur ou une entrée de contrôle incorrecte, un enregistrement incorrect de temps ou une mauvaise identité de dispositif d'envoi. Un adversaire peut lancer ses attaques en obtenant les clés secrètes utilisées par les dispositifs d'envoi, ou en compromettant certains des capteurs et des actionneurs. La disponibilité des systèmes SCADA peut être définie comme la capacité à maintenir les actions opérationnelles du système en empêchant ou en faisant face aux attaques par déni de service contre les entrées de mesure et de contrôle des capteurs. Pour lancer une attaque DoS, l'adversaire peut brouiller les canaux de communication, empêcher les appareils de terrain d'envoyer des données, ou inonder le réseau de communication par des données aléatoires.

Les attaques par tromperie visant l'intégrité ont récemment fait l'objet d'une plus grande attention. Un type particulier d'attaques par tromperie, appellée "attaque par rejeu" ("replay attack") sur les mesures des capteurs, a été analysé dans [Mo and Sinopoli (2009)]. Les auteurs ont examiné le cas où tous les capteurs existants étaient attaqués et ont proposé des contre-mesures appropriées pour détecter l'attaque. Dans le scénario de cette attaque, l'agresseur n'a aucune connaissance préalable du système, mais il est capable d'accéder aux données du capteur et de les falsifier.

Une autre classe d'attaque par tromperie, les attaques par injection de fausses données ("false data injection"), a également été étudiée dans des travaux récents. Par exemple, dans le cas des réseaux électriques, un attaquant ayant une parfaite connaissance des modèles a été initialement envisagé dans [Rahman and Mohsenian-Rad (2013)]. Dans le travail présenté dans [Kosut et al. (2010)], l'auteur considère les attaques furtives avec des ressources limitées et propose des méthodes de détection améliorées tandis que l'auteur de [Sandberg et al. (2010)] a analysé le nombre minimum de capteurs requis pour les attaques furtives, sur la base de laquelle des mesures de sécurité ont été proposées. Les conséquences de ces attaques ont également été analysées dans [Teixeira et al. (2012); Xie et al. (2010)]. Les attaques par injection de fausses données dans les systèmes de contrôle dynamique ont également été examinées. Dans [Smith (2011)], l'auteur caractérise l'ensemble des

politiques d'attaque pour les attaques secrètes (indétectables) par injection de fausses données avec une connaissance détaillée du modèle et un accès complet à tous les canaux de capteurs et d'actionneurs, tandis que [Pasqualetti et al. (2011)] décrit l'ensemble des attaques par injection de fausses données indétectables pour les attaquants anonymes avec des informations complètes, mais pouvant compromettre seulement un sous-ensemble des capteurs et actionneurs existants. Dans ces scénarios d'attaque, la confidentialité a également été atteinte, car l'agresseur avait accès à la mesure et à l'actionneur, donc aux informations complètes.

Dans le passage suivant, nous définissons les différentes attaques cyberphysiques citées précédemment :

Attaque DoS "Denial of Service attack" : L'objectif d'une attaque par déni de service est de perturber la communication entre la MTU et les RTU, ou entre les RTU et les capteurs, ou les RTU et les actionneurs. Ce type d'attaque permet de couper le lien entre les différentes parties du système afin de perturber le contrôle de la boucle de retour [Yuan et al. (2013)]. Ces attaques sont capables de déconnecter le contrôleur du dispositif physique. L'isolation évite de surveiller le processus et rend le système vulnérable à l'action d'un éventuel attaquant.

Attaque par rejeu "Replay attack" : Parmi les attaques cyber physiques les plus critiques, il y a les attaques par rediffusion (replay attack). Lorsqu'une attaque de ce type est menée, l'attaquant enregistre d'abord les mesures provenant des capteurs. Puis, dans une phase ultérieure de l'attaque, l'attaquant remplace les données réelles par les données enregistrées, ce qui entraîne une détérioration des performances du système de contrôle et permet potentiellement d'autres types d'attaques sans être découvert. Pour détecter l'attaque, il est nécessaire d'ajouter une protection au signal de contrôle d'entrée [Mo et al. (2014)].

Attaques par injection de fausses données "False data injection attack" : Ces attaques se concentrent sur des systèmes dont l'état est instable. Elles visent à modifier les mesures des capteurs afin de rendre certains états instables inobservables [Pasqualetti et al. (2015); Mo et al. (2010)]. Ces attaques exploitent une vulnérabilité des systèmes comme les attaques Zéro Dynamique (Zero Dynamic attack). La solution pour éviter ces attaques est de mettre à jour l'architecture afin de supprimer les vulnérabilités.

2.3 Méthodes existantes pour sécuriser les SCADA

Les méthodes proposées pour résoudre le problème de la cybersécurité des systèmes SCADA peuvent être classées en deux grandes catégories : les technologies de l'information, principalement basées sur le cryptage et la sécurité des données, et la théorie du contrôle sécurisé, qui étudie la manière dont les cyberattaques affectent la dynamique physique du système de contrôle [Cardenas et al. (2008)]. Les outils de sécurité utilisant

uniquement la sécurité de l'information ne sont pas suffisants pour un contrôle sécurisé des systèmes SCADA car ils ne peuvent pas décrire le macro comportement du système. Par conséquent, ils doivent être complétés par la théorie du contrôle sécurisé.

La catégorie de technologie de l'information (IT) vise principalement à garantir les principes de CIA triade cités ci-dessus. Des outils et des méthodes [Ten et al. (2010); Cárdenas et al. (2011); Stouffer et al. (2015); Krutz (2005)] ont été proposés dans la litté- rature pour améliorer la sécurité des systèmes SCADA contre les cyberattaques. Quelques exemples parmi d'autres, on peut citer (1) les normes de sécurité et les meilleures pra- tiques [Leszczyna (2018); Nicholson et al. (2012)], (2) pare-feu et segmentation du réseau [Zhu and Sastry (2010)], (3) les Honeynets, comme le projet SCADA Honeynet [Potham- setty and Franz (2005)], sont utilisés pour empêcher les adversaires d'attaquer le système réel. Ils peuvent être utilisés pour collecter des informations sur l'attaque sans exposer un système réel à un risque d'exploitation et donc améliorer la sécurité du SCADA, et (4) les systèmes de détection d'intrusions. Dans la littérature, divers systèmes de détection d'intrusion (IDS) ont été proposés pour les systèmes SCADA. Almalawi et al [Almalawi et al. (2014)] ont proposé un IDS non supervisé basé sur les anomalies pour la détection des attaques d'intégrité. En utilisant la technique de regroupement des données, un IDS qui peut identifier les états normaux et critiques du réseau SCADA est proposé [Yang et al. (2014)]. Lin et al [Lin et al. (2018)] ont conçu un IDS pour détecter les commandes de contrôle liées aux attaques dans le SCADA. Pour détecter les attaques par fausses in- jection des données ("false data injection attack"), différentes solutions [Esmalifalak et al. (2017); Guo et al. (2017)] ont également été proposées.

On estime qu'une utilisation appropriée des mesures de sécurité de l'information sus-mentionnées peut contribuer à réduire le nombre de cyber incidents ainsi que leurs conséquences. Cependant, ces méthodes sont principalement applicables pour protéger les systèmes SCADA contre les cyber incidents sur la couche de communication. Parfois les pare-feux peuvent être utilisés pour empêcher l'intrusion dans les systèmes SCADA par le biais des réseaux des fournisseurs et des terminaux locaux. Cependant, l'incident Stuxnet [Falliere (2010)] a clairement montré que ces outils informatiques ne pouvaient offrir que les mécanismes nécessaires à la sécurité des systèmes SCADA. La protection complète de ces systèmes à grande échelle contre les attaques cyberphysiques nécessite une stra- tégie de défense en profondeur [Cárdenas et al. (2008); Cardenas et al. (2009)], où les infrastructures critiques sont protégées par des couches de sécurité.

En outre, les systèmes SCADA sont très différents des systèmes informatiques sur de nombreux aspects. Premièrement, l'exigence de fonctionnement continu empêche les systèmes SCADA d'appliquer des solutions de sécurité informatique comme les mises à jour de logiciels anti-virus. Deuxièmement, il est extrêmement difficile de mettre en œuvre des solutions de sécurité pour les couches inférieures des systèmes SCADA. Par exemple, des algorithmes de cryptage avancés, qui nécessitent une quantité énorme de ressources

informatiques, ne peuvent pas être mis en œuvre dans les canaux de communication entre les API et les capteurs/actionneurs en raison des exigences strictes en matière de temps réel [Zhu et al. (2011)]. De plus, les technologies sans fil sont souvent utilisées pour la transmission de données sur de longues périodes. Les distances dues à la dispersion géographique des caractéristiques. Enfin, la principale différence entre les systèmes SCADA et les systèmes informatiques repose sur l'interaction entre la partie contrôle du système et la partie physique. Cependant, les solutions traditionnelles basées sur les technologies de l'information n'exploitent pas la compatibilité du cyberespace (c'est-à-dire les algorithmes de contrôle, les signaux de commande, les signaux de contrôle et les mesures des capteurs) avec la couche physique (c'est-à-dire les actionneurs, les capteurs ou les processus phy- siques), étant ainsi inefficace contre les cyber-attaques physiques visant à perturber les processus physiques [Pasqualetti et al. (2013)].

La catégorie théorie du contrôle se concentre principalement sur l'analyse de la sécurité des systèmes de contrôle en réseau contre les cyberattaques. L'approche générale consiste à étudier l'impact négatif de différents types de cyberattaques sur des systèmes particuliers. En particulier, un effort de recherche important a été consacré à l'étude des vulnérabilités des systèmes de contrôle en réseau, à la conception d'attaques furtives/déceptives qui peuvent partiellement ou totalement contourner les détecteurs d'anomalies traditionnels, et à la proposition de contre-mesures pour révéler les attaques indétectables. Un domaine actif, dans la catégorie de théorie du contrôle, est le diagnostic des défauts, ainsi que le contrôle tolérant aux défauts.

La différence entre un système SCADA et les systèmes informatiques réside dans l'intéraction du premier avec le monde physique [Cárdenas et al. (2008)]. L'approche de la sécurité de l'information se concentre sur l'amélioration de la sécurité des systèmes SCADA par des mesures de sécurité. La compatibilité entre la couche cybernétique et l'infrastruc- ture physique n'est pas été prise en considération. Cependant, le travail présenté dans [Teixeira et al. (2015)] a démontré que les outils FDI (Fault Detection and Isolation) peuvent être utilisés pour détecter et atténuer l'impact négatif des cyberattaques sur les systèmes de contrôle et de supervision en réseau.

La sécurité en profondeur des systèmes SCADA contre les cyberattaques nécessite l'utilisation à la fois de l'approche de sécurité de l'information, l'approche du contrôle de la théorie, et l'approche de détection et d'isolation d'attaque. Les méthodes basées sur les TI nous fournissent des contre-mesures pour protéger les infrastructures critiques de sécurité contre les cyber-attaques sur le centre de contrôle. Les méthodes basées sur la théorie du contrôle sécurisé se concentrent principalement sur (1) l'étude des vulnérabilités des systèmes de contrôle en réseaux modélisés par une forme d'espace d'état à temps discret, (2) la conception d'attaques furtives/déceptives pour contourner partiellement ou complètement les détecteurs d'anomalies traditionnels, et (3) la proposition de contre- mesures pour révéler ces attaques indétectables. L'approche FDI, d'autre part, traite

de la détection et de l'identification des cyberattaques en adaptant les techniques FDI traditionnelles pour attaquer des scénarios de détection-isolation.

2.4 Conclusion

Dans ce chapitre, nous avons montré le rôle important des systèmes SCADA pour la surveillance et le contrôle à distance des processus industriels et des infrastructures critiques. Nous avons détaillé les différentes applications des systèmes SCADA, et nous avons montré que les protocoles de communication utilisés dans les réseaux SCADA présentent de nombreuses vulnérabilités lorsqu'il s'agit de vérifier l'authentification et l'intégrité des paquets transmis. Nous avons également montré que l'utilisation massive des technolo- gies de l'information et de communication à ouvert de nouvelles voies pour mener des cyberattaques contres ces infrastructures, et que la complexité des attaques a rendu la tâche extrêmement difficile pour les systèmes de détection d'intrusion traditionnels. Ces systèmes ont besoin d'aide afin de fournir une protection ultime aux infrastructures cri- tiques, et c'est là qu'interviennent les méthodes de contrôle théorique pour détecter les attaques cyber-physiques, en considérant tout type de systèmes.

Bien que l'approche de la sécurité de l'information puisse fournir certaines méthodes de protection qui aident à améliorer la sécurité des systèmes SCADA, ces méthodes semblent insuffisantes pour la défense en profondeur des systèmes contre les attaques malveillantes pouvant contourner les couches de sécurité de l'information, comme dans le cas de l'incident Stuxnet en 2010. C'est pourquoi l'approche de contrôle sécurisé est considérée comme un partenaire complémentaire des méthodes basées sur les TI pour protéger les SCI à grande échelle contre les cyberattaques. Cependant, les méthodes de contrôle sécurisé se sont principalement concentrées sur l'étude des vulnérabilités des systèmes de contrôle en réseau, la conception d'attaques furtives/déceptives sur les systèmes et ensuite la propo- sition de certaines contre-mesures pour rendre ces attaques détectables. L'approche FDI, en revanche, se concentre sur la détection et l'identification des attaques détectables et identifiables.

CHAPITRE 3

Bond graph pour la surveillance des systèmes

Contents

Introduction

Dans un effort de réduction de la complexité et des coûts, les systèmes de contrôle industriels traditionnels sont mis à niveau avec de nouvelles capacités de calcul, de communication et d'interconnexion. L'adoption de nouvelles capacités de communication se fait au prix d'introduire de nouvelles menaces pour la sécurité qui doivent être traitées de manière globale, tant en termes de sûreté et de sécurité (au sens traditionnel du terme TIC). L'utilisation d'une approche de sécurité inadéquate peut avoir un effet négatif sur un grand nombre de ressources, y compris les actifs des réseaux gouvernementaux et les infrastructures critiques. Les coûts associés, notamment en ce qui concerne les conditions de perte d'opportunités commerciales et les dépenses pour réparer les incidents, sont cen- sés être réduits. En conséquence, la question de l'évaluation des mécanismes de sécurité cyber physique est un sujet de recherche sensible.

On se propose d'aborder, dans ce chapitre, la méthode de surveillance des systèmes utilisant les Bond graphs (BG). Comme nous l'avons expliqué dans le chapitre précédent, les outils FDI peuvent être utilisés pour détecter et atténuer l'impact négatif des cyberat- taques sur les systèmes contrôlés en réseau (NCS), y compris les SCADA. Dans ce travail, nous proposons d'adapter les méthodes de détection et d'isolation des défauts (FDI) pour détecter les attaques dans les systèmes SCADA. Nous commençons par présenter l'outil de modélisation Bond graph, et la méthode de modélisation. Ensuite, nous expliquerons les différentes étapes de détection des défauts. Ces méthodes qui vont être adaptées par la suite pour la modélisation et la détection des attaques.

3.1 Etat de l'art

Au XIXe siècle, Lord Kelvin et James Clerk Maxwell ont tous deux observé qu'un large éventail de phénomènes donnait lieu à des formes d'équations similaires, en trouvant des analogies entre le flux de chaleur et la force électrique et entre les lignes de force et les courants de fluide. Dans les années 1940 et 1950, H.M. (Hank) Paynter a travaillé sur des projets d'ingénierie interdisciplinaires comprenant des centrales hydroélectriques, l'informatique analogique et numérique, la dynamique non linéaire et le contrôle [Paynter (1992)]. Grâce à cette expérience, il a observé que des formes similaires d'équations sont générées par des systèmes dynamiques dans une grande variété de domaines (par exemple électrique, fluide et mécanique) ; en d'autres termes, ces systèmes sont analogues. Paynter a intégré la notion de port d'énergie dans sa méthodologie, et c'est ainsi que les Bond Graphs ont été inventés. Depuis, son groupe et de nombreux autres ont développé les concepts de base de la modélisation bond-graph en une méthodologie mature.

La nature des bonds graphs sépare la structure du système des équations, ce qui fait du BG une solution idéale pour visualiser les caractéristiques essentielles d'un système. En effet, en créant des BG, la conception et l'analyse de la structure d'un système (peut-être la partie la plus importante de la tâche de modélisation) peuvent être effectuées en utili- sant un crayon et du papier. Les modélisations peuvent ainsi se focaliser sur les relations entre les composants et les sous-systèmes plutôt que sur les détails de la mise en œuvre de leurs logiciels de modélisation particuliers. Avant même l'utilisation d'un ordinateur, les bond graphs peuvent fournir à un ingénieur des informations sur les états contraints, les boucles algébriques et les avantages et conséquences des approximations et simplifications potentielles. De nombreux outils de modélisation informatique sont disponibles pour gé- nérer et traiter les BG. Ces outils ont généralement des capacités qui vont bien au-delà de celles des logiciels traditionnels de diagrammes de blocs, y compris la génération de représentations symboliques, l'inversion de modèles et l'identification paramétrique, ainsi que la capacité de produire des simulations, des réponses en fréquence et d'autres aides à la conception. Les ingénieurs peuvent donc utiliser les modèles BG non seulement pour effectuer des analyses numériques simples, mais aussi, et surtout, pour obtenir un aperçu qualitatif [Damić and Montgomery (2015)].

Définition 3.3.1 *Bond Graph [Loureiro et al. (2012)] est un outil graphique spéci- fique qui permet de représenter la structure énergétique commune des systèmes. Il permet de mieux comprendre le comportement des systèmes. Sous forme vectorielle, ils donnent une description concise des systèmes complexes. De plus, les notations de causalité four- nissent un outil non seulement pour la formulation des équations des systèmes, mais aussi pour la discussion basée sur l'intuition du comportement des systèmes, à savoir la contrô- labilité, l'observabilité, le diagnostic des défauts, etc.*

3.1.1 Théorie de base des bond graphs

Un bond graph est un diagramme utilisé pour modéliser un système physique. Il représente une interface entre le système physique et son modèle mathématique [Filippo et al. (1991)]. La méthodologie de modélisation est basée sur deux grands principes : la représentation graphique des échanges d'énergie entre les composants du système et l'analogie énergétique entre les différents domaines physiques. Comme le montre la figure 1, l'échange de puissance entre deux éléments A et B est représenté par une demi-flèche (appelée "liaison") qui comprend deux variables : l'effort $.e/$ et le flux $.f/$, dont le produit $.e \times f/$ représentelapuissanceinstantanéeportéeparcetteliaison.Lesensdutransfert de puissance est indiqué par une demi-flèche comme présenté dans la (fig.9).

La méthode du bond graph est une approche de modélisation dans laquelle les transferts d'énergie entre les composants sont reliés par des liens qui spécifient le transfert d'énergie entre les composants du système.

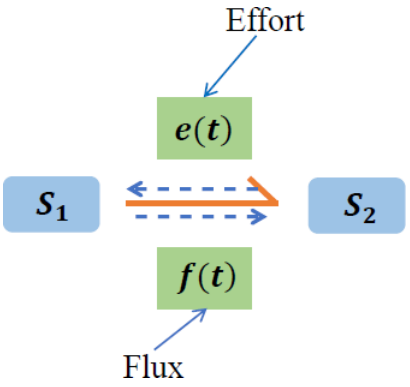

FIGURE 9 – Le principe du Bond Graph

Les variables $e.t/$ et $f.t/$ représentent respectivement l'effort et le flux entre les systèmes $S1$ et $S2$ dont le produit $P.t/$ D $e.t/ \times f.t/$ n'est rien d'autre que la puissance instantanée transférée entre les systèmes $S1$ et $S2$. Les deux variables $e.t/$ et $f.t/$ sont dites conjuguées l'une del'autre.

3.1.2 Variables de puissance des Bond Graphs

Le langage bond graph vise à décrire des systèmes physiques de classe générale par les échanges de puissance. Les facteurs de puissance, c'est-à-dire l'effort et le flux, ont des interprétations différentes dans différents domaines physiques. Cependant, la puissance peut toujours être utilisée comme une référence généralisée pour modéliser des systèmes se trouvant dans plusieurs domaines énergétiques. Un de ces systèmes peut être un mo- teur électrique alimentant une pompe hydraulique ou un moteur thermique relié à un amortisseur ; où la forme d'énergie varie au sein dusystème.

Dans le tableau suivant, nous présentons les variables d'effort et de flux dans certains domaines physiques (tab.3.1) :

Bond graph	**Transfert**	**Rotation**	**Electrique**	**Hydraulique**
Effort e	Force FN	Moment de torsion $\iota\ N — m$	Voltage $V\ V$	Pression PPa
Flux f	Vitesse $Vm{=}s$	Vitesse angulaire ▲ $rad{=}s$	Courant IA	Flux $Qm^3{=}s$

Tableau 3.1 – Présentation effort et flux dans différents domaines

3.1.3 Composants du bond graph

(Tab.3.1) : présente les composants bond graph avec des exemples analogues dans 4 domaines de l'ingénierie.

- Se peut correspondre à une source de tension idéale ou à une force appliquée, S_e est une source d'effort.
- Sf peut correspondre à une source de courant idéal ou à une vitesse appliquée, S_f est une source de flux.
- De peut correspondre à un voltmètre.
- R peut correspondre à une résistance électrique ou à un amortisseur mécanique, énergie dissipée.
- C peut correspondre à un condensateur électrique ou à un ressort mécanique, stocke l'énergie
- I peut correspondre à un inducteur électrique ou à une masse mécanique, stocke l'énergie.
- SS composants (non indiqués dans le tableau) modèle de paires de capteurs et d'actionneurs colocalisés : $Se — Df$ ou $Sf — De$. Ces composants représentent également les ports d'énergie des composants composés (fig.10).

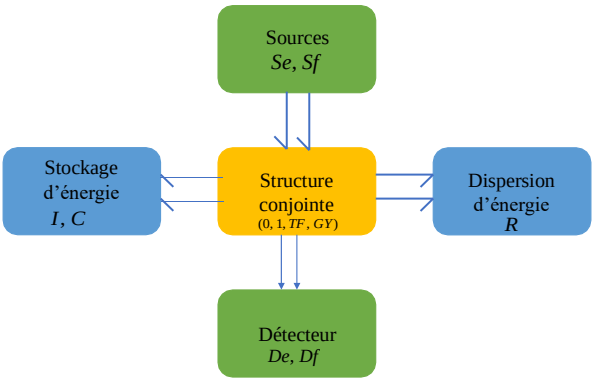

FIGURE 10 – Composants bond graph

Dans le cas linéaire, les équations correspondantes pour les composantes R, C et Ien termes de variables génériques du (tab.3.1) sont, respectivement, (eqs. 3.1, 3.2, 3.3):

$$R \text{ fe D } rf \tag{3.1}$$

$$c \begin{pmatrix} e \text{ D } \frac{q}{c} \\ q_1 \text{ D } f \end{pmatrix} \tag{3.2}$$

$$I \begin{pmatrix} f \text{ D } \frac{p}{m} \\ p_1 \text{ D } e \end{pmatrix} \tag{3.3}$$

où r , c et m sont des constantes décrivant le système physique correspondant. Dans le domaine électrique, (2) correspond à la loi d'Ohm et (3) à la loi de Coulomb ; dans le domaine mécanique, (3) correspond à la loi de Hooke, tandis que (5) correspond à la deuxième loi de Newton.

Les signaux analogues du tableau (tab.3.1) : conduisent aux composantes analogues de ce tableau. La première colonne donne la composante générique du bond graph, tandis que les autres colonnes donnent les composantes analogiques spécifiques audomaine.

Bond graph	Transfert	Rotation	Electrique	Hydraulique
S_e D_e	Force appliquée Force capteur $F\ N$	Moment appliqué Moment capteur $T\ N{=}m$	Voltage appliqué Voltmètre $V\ V$	Pression appliquée Pression capteur $P\ Pa$
S_f D_f	Vitesse appliquée Indicateur vitesse $v\ r{=}s$	Rotation appliquée Tachéomètre [!]nr/s	Courant appliqué Ampèremètre $i\ A$	Flux appliqué Débimètre $Q\ m^3{=}s$
C	Ressort $K\ N{=}m$	Torsion ressort $K\ \ N — m{=}rad$	Condensateur $C\ F$	Batterie $K\ Pa{=}m^3$
I	Masse $m\ kg$	Moment d'inertie $J\ kg — m^2$	Inducteur $L\ H$	Inertie flux $I\ kg{=}m^4$
R	Amortisseur $d\ \ N —s{=}m$	Rotation amortisseur $d\ N — m — s{=}rad$	Résistance R \!	Résistance flux $k\ Pa — s{=}m^3$

Tableau 3.2 – Présentation des composants analogiques dans différents domaines par rapport au bond graph

3.1.4 Conversion de puissance avec des transformateurs et des gyrateurs

Les variables d'effort et de flux dans chaque domaine physique du tableau (tab.3.2) ont des unités différentes et ne peuvent donc pas être directement reliées. Cependant, comme la puissance est la référence universelle des systèmes physiques, les composants TF (un transformateur générique) et GY (un gyrateur générique) du graphique (11 (a))

et (11 (b)) fournissent un moyen de convertir la puissance et donc de relier différents domaines. La composante TF généralise un transformateur électrique, qui a la propriété que le rapport des tensions (efforts) aux deux bornes est l'inverse du rapport des courants, ce qui est cohérent avec le fait que la puissance est conservée, dans le sens où la puissance instantanée au port d'entrée est égale à la puissance instantanée au port de sortie à chaque instant.

(a) (b)

FIGURE 11 – Transformateur et Gyrateur

La composante TF assure une conversion de puissance telle que $e_1 = ne_2$ et $f_1 = nf_2$. La composante GY fournit une conversion de puissance telle que $e_2 = kf_1$ et $e_1 = kf_2$, où k est la constante de champ magnétique arrière du moteur.

Dans le cas linéaire, les composantes TF et GY ont les équations suivantes (eqs. 3.4, 3.5)

$$TF \begin{cases} e_2 = ne_2 & .1/ \\ f_1 = nf_2 & .2/ \end{cases} \tag{3.4}$$

$$GY \begin{cases} e_2 = kf_1 & .3/ \\ e_1 = kf_2 & .4/ \end{cases} \tag{3.5}$$

où n et k sont des constantes non dimensionnelles décrivant le système physique correspondant. Les paires (1)-(2) et (3)-(4) décrivent toutes deux des composants économes en énergie puisque, dans les deux cas, la puissance d'entrée et celle de sortie sont les mêmes, c'est-à-dire $e2f2 = e1f1$.

3.1.5 Jonctions bond graph

Les jonctions sont des éléments dans les bond graphs qui sont responsables de la mise en œuvre de la loi d'économie d'énergie. Il existe deux types de jonctions : l'effort commun et le flux commun.

Une jonction effort commun, également connue sous **jonction 0**, est un point de jonction de plusieurs liens énergétiques à effort égal. Considérons le cas général de trois liaisons se rencontrant à un nœud 0, comme le montre la (fig. 12).

Sous réserve d'efforts communs, il peut être écrit (eq. 3.6) :

$$e_1 = e_2 = e_3 \tag{3.6}$$

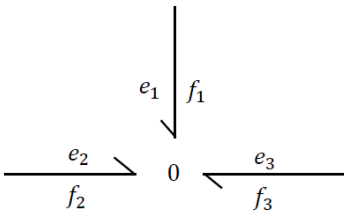

FIGURE 12 – Jonction effort commun

L'application de la loi sur les conservations d'énergie en résultera (eq. 3.7) :

$$f_1 \mathrm{C} f_2 \mathrm{C} f_3 \mathrm{D} 0 \tag{3.7}$$

De même une jonction de flux commun, également connue sous **jonction 1**, est un point de jonction de plusieurs liaisons énergétiques à flux égaux. (fig. 13) illustre trois liaisons se rencontrant à un nœud unique et les équations sont les suivantes (eqs. 3.8, 3.9), dans l'hypothèse d'un flux commun :

$$f_1 \mathrm{D} f_2 \mathrm{D} f_3 \tag{3.8}$$

$$e_1 \mathrm{C} e_2 \mathrm{C} e_3 \mathrm{D} 0 \tag{3.9}$$

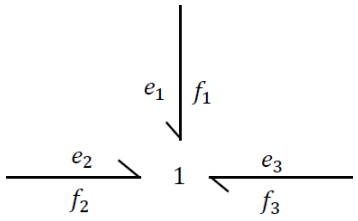

FIGURE 13 – Jonction flux commun

3.1.6 La causalité

Les outils de modélisation conduisent finalement à la dérivation des équations de mouvement des systèmes. Pour les bond graphs, ce processus commence par la spécification des variables d'état. Pour cette raison, les BG utilisent une technique dans laquelle des traits de causalité sont insérés.

Définition 3.3.2 *Causalité ; Pour les éléments I et C, la relation entre leurs efforts et leurs flux est déterminée par des intégrales. Considérons l'élément I, par exemple, pour lequel le flux est obtenu à partir de l'intégration de son effort* (eqs. 3.10, 3.11):

$$f\,.t/ \mathrm{D} \frac{1}{I} \int e.t/dt \tag{3.10}$$

Dans les éléments C , c'est le contraire, puisque l'effort et le flux changent de place dans l'équation 3.11 :

$$e.t/ = \frac{1}{C}\int f.t/dt \tag{3.11}$$

(Eq. 3.10) signifie que dans un élément I , l'effort est la cause du transfert d'énergie. En d'autres termes, lorsque l'effort est reçu par l'élément, le flux est généré après un délai. Un exemple est la masse dans les systèmes mécaniques. L'application d'une force à une masse produit de la vitesse. En fait, au temps zéro, il y a une force mais la vitesse est nulle. Au bout d'un certain temps, la vitesse se produit. Ainsi, dans les éléments I , le flux est toujours en retard sur l'effort. On dit que l'effort dans ces éléments est la cause et que le flux est l'effet.

Elément	Symbol basique	Trait causal	Alternative
I	$\longrightarrow I$	$\longrightarrow\!\vert\ I$	A éviter
C	$\longrightarrow C$	$\vert\!\longrightarrow C$	A éviter
R	$\longrightarrow R$	$\vert\!\longrightarrow R$	$\longrightarrow\!\vert\ R$
S_e	$S_e\longrightarrow$	$S_e\longrightarrow\!\vert$	Aucune
S_f	$S_f\longrightarrow$	$S_f\vert\!\longrightarrow$	Aucune
TF	$\longrightarrow TF\longrightarrow$	$\vert\!\longrightarrow TF\vert\!\longrightarrow$	$\longrightarrow\!\vert\ TF\longrightarrow$
GY	$\longrightarrow GY\longrightarrow$	$\vert\!\longrightarrow GY\longrightarrow\!\vert$	$\longrightarrow\!\vert\ GY\vert\!\longrightarrow$

FIGURE 14 – Traits de causalités des élements bond graph

La dernière colonne du tableau de la figure (fig. 14) indique qu'il existe d'autres affectations de causalité pour les éléments du bond graph. Pour les éléments I et C , les traits alternatifs se trouvent aux autres extrémités. En fait, les traits donnés aux éléments I et C indiqués dans le tableau de la figure (fig. 14) sont appelés causalité intégrale puisque la relation entre le flux et l'effort de ces éléments est de type intégral. Cependant, dans un système physique, il est possible que les éléments I et C reçoivent une causalité alterna- tive (appelée causalité différentielle). Il est recommandé d'éviter ce type de causalité, si possible. Pour les éléments R, la causalité n'est pas importante et les deux formes peuvent être attribuées. Pour les sources, aucune autre forme d'attribution de la causalité n'est autorisée.

Les jonctions sont très importantes lorsque des traits de causalité sont attribués. La raison est que, dans chaque jonction, il n'y a qu'une seule bande qui contrôle la propriété de cette jonction (c'est-à-dire le flux ou l'effort) : elle est appelée "Bande forte". Cela signifie notamment que dans un nœud unique, tous les éléments reliés ont des flux égaux, le flux est imposé par un seul des éléments. Par exemple, si une source de flux est connectée à un nœud, évidemment tous les éléments auront le flux de la source. Par convention, la liaison forte dans une jonction à flux commun reçoit la trait causale à l'extérieur de la jonction et les autres liaisons reçoivent leurs traits causaux à l'intérieur de la jonction.

Pour une jonction à effort commun, c'est l'inverse qui s'applique (c'est-à-dire que la liaison forte reçoit le trait causal à l'intérieur de la jonction). La figure (fig. 15) illustre les traits de causalité des jonctions à flux commun et à effort commun. Il est clair que dans une jonction 0, un seul trait apparaît à l'intérieur de la jonction et que dans une jonction 1, un seul trait apparaît à l'extérieur de la jonction. L'existence de plus d'un lien fort dans une jonction indique une atteinte à la loi de conservation de l'énergie et le résultat est donc invalide.

Affectation de causalité

La procédure d'attribution de la causalité dans un bond graph n'est pas unique et chacun peut utiliser une manière différente d'insérer les traits. Cependant, il y a quelques points utiles à prendre en compte avant d'attribuer les traits de causalité.

- Les sources sont de bons points de départ car leurs traits sont précis
- Attribuer des causalités intégrales pour tous les éléments I et C.
- Désignation de traits de causalité un par un pour éviter les erreurs.
- Vérification de toutes les jonctions et assurance qu'il n'y a qu'un seul lien solide dans chaque jonction.

La figure (fig. 15) suivante illustre la méthode d'affectation des causalités dans les jonctions "1" et "0".

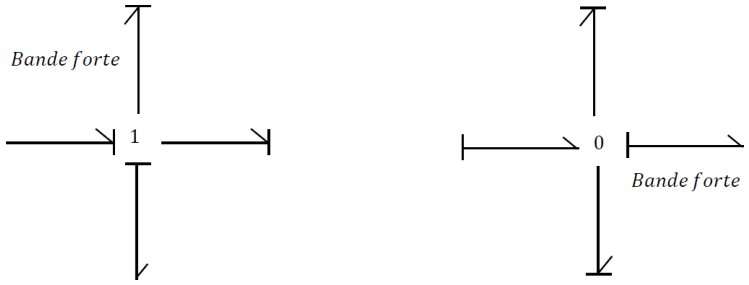

FIGURE 15 – Traits causaux des jonctions 1 et 0 typiques

3.2 Surveillance des systèmes par BG

Selon [Touati (2002)], l'objectif de la représentation bond graph est d'utiliser un seul outil pour la modélisation, la génération des relations de redondances analytiques (RRA) et l'analyse structurelle.

3.2.1 L'analyse structurelle par bond graph

L'analyse structurelle est un outil puissant permettant l'étude de plusieurs propriétés d'un système dynamique. En effet, cette étude peut s'effectuer directement sur le modèle

graphique moyennant les propriétés structurelles et causales de l'outil utilisé. Efficace même pour les très grands systèmes, l'analyse structurelle permet de déterminer certaines propriétés structurelles du système telles que l'observabilité, la commandabilité et la surveillabilité. Ces propriétés sont nécessaires pour la génération des RRAs [Samantaray et al. (2006)].

3.2.2 Surveillance structurelle

Selon [Djeziri (2007)], un sous-système est sous-déterminé si lors de la dualisation des détecteurs sur un modèle bond graph destiné à la surveillance (mis en causalité dérivée), les éléments dynamiques ne peuvent pas être mis en causalité dérivée. Par conséquent, les modèles bond graph qui ne peuvent pas être mis en causalité dérivée (même avec la dualisation des détecteurs) ne sont pas surveillables. On peut alors soit ajouter des capteurs, soit mettre le bond graph en causalité intégrale.

La présence des conditions initiales dans le calcul peut aussi être éliminée par des dérivations successives, étant donné que la dérivation d'une relation de redondance analytique est une relation de redondance analytique.

La surveillance des systèmes pluridisciplinaires en utilisant bond graph consiste à: 1.La modélisation du système ;

2.La génération des relations de redondance analytique (ARRs) ; 3.La génération de la matrice de signature (FSM);

4.La génération des seuils adaptatifs.

Dans les sections suivantes nous allons expliquer le processus de chacunes des méthodes citées ci-dessus.

3.2.3 Génération des relations de redondance analytique

Les relations de redondance analytique (RRA) [Cocquempot (2004)] jouent un rôle important dans les méthodes de détection et d'isolation des défauts (FDI) basées sur des modèles.

Les RRAs établissent des contraintes entre des variables connues (les variables d'en- trées et les variables de sorties mesurées) et comprennent également, en général, des paramètres de modèles connus. Dans des conditions de mode normal, l'évaluation numé- rique des RRAs devrait produire des valeurs égales à zéro. En pratique, le résultat de l'évaluation d'une RRA, sa valeur de sortie, est aussi appellé résidu. Si le système mesuré est sujet à des défauts dans certains composants du système, alors les valeurs de certains résidus peuvent être en dehors des seuils donnés et peuvent servir d'indicateurs de dé- fauts. L'analyse structurelle des relations de redondance analytique montre si les défauts peuvent être isolés ou non.

Défninition 3.3.3 *RRA ; une Relation de Redondance Analytique est une contrainte déduite du modèle de système qui ne contient que des variables observées, et qui peut donc être évaluée à partir de n'importe quelle observation . Elle est notée r=0, appelé résidu du RRA*.

Définition 3.3.4 *Résidu est un indicateur de défaut qui exprime l'incohérence entre les informations disponibles et les informations théoriques fournies par un modèle*.

Les RRAs [Borutzky (2011)] sont des contraintes algébriques qui proviennent des jonc- tions. Chaque jonction apporte une équation de continuité pour les flux ou les efforts. En utilisant les équations constitutives des éléments des BG et en éliminant les variables inconnues, les RRA peuvent être obtenues sous forme symbolique si les non linéarités permettent les éliminations nécessaires. La forme de l'ensemble des RRA n'est pas unique et dépend du choix des méthodes de calcul, des causalités dans un BG et de la procédure qui est appliquée. En outre, les méthodes algébriques indiquées par des chemins de causa- lité dans le BG et composants non linéaires peuvent empêcher l'élimination des variables inconnues.

Étant donné que les variables inconnues peuvent être éliminées, l'analyse structurelle de chaque équation résultante conduit à ce que l'on appelle une **signature** en termes de variables connues et de paramètres des composants du système pour chaque résidu. En résumant les variables de puissance à deux jonctions ils peuvent donner lieu à la même signature. C'est-à-dire que la dérivation des RRA de toutes les jonctions d'un BG produirait des informations redondantes. Les RRA sont dérivées uniquement à partir de ces jonctions de bond graph avec un détecteur qui y est connecté. Le détecteur modélise la mesure d'une variable de processus (présentée par la jonction commune variable).

Algorithme de génération des RRA par bond graph

L'algorithme suivant permet de générer des RRAs de façon systématique à partir d'un modèle bond graph. Voici dans l'ordre les étapes à suivre [Djeziri et al. (2006)] :

1. mettre le modèle bond graph en causalité dérivée préférentielle (en inversant la causalité des détecteurs si possible);
2. Identifier les jonctions " 0" et "1" contenant au moins un détecteur ;
   - □ éliminer les variables inconnues en parcourant les chemins causaux sur le bond graph,
   - □ pour tout détecteur dont la causalité est inversée une RRA est déduite,
   - □ pour tout détecteur dont la causalité ne peut pas être inversée une RRA est déduite en mettant à égalité sa sortie avec la sortie d'un autre détecteur de même nature (redondance matérielle)
3. Écrire les équations structurelles des jonctions observées qui seront alors des RRAs condidates :

$$\begin{cases} b_i f_i \subset S f_i \supset 0 & \text{pour une jonction } 0 \\ b_i e_i \subset S_i e_i \supset 0 & \text{pour une jonction } 1 \end{cases}$$

$$b \supset -1$$

Si la demi-flèche entre ou sort de la jonction, les variables inconnues effort $.e/$ et flux $.f/$ sont alors éliminées par un parcours de chemin causal de la variable connue ($SSf \Vdash f_m$ et $SSe \Vdash e_m$) vers l'inconnue. La RRA issue de la jonction "*0*" représente le flux et celle issue de la jonction "*1*" représente l'effort. Chacune des RRAs sera sensible aux défauts pouvant affecter le composant parcouru par le chemin causal pour l'élimination des variables inconnues.

4. Une RRA est obtenue à partir de chaque régulateur en comparant sa sortie mesurée avec la sortie prédite par son algorithme de commande;
5. Refaire les étapes 3 et 4.

   - Si les RRAs obtenues sont strictement différentes de celles déjà obtenues alors les garder, sinon continuer jusqu'à ce que toutes les équations des jonctions et celles des régulateurs soient explorées.

Définition 3.3.5 *Chemin causal* ; dans une représentation graphique, le chemin causal est une série de variables d'effort et de flux, successivement liées selon l'affectation de la causalité du modèle [Ngwompo et al. (2001)].

Définition 3.3.6 *Détecteur dualisé* [Benmoussa (2013)] ; consiste à le transformer en source d'effort (jonction 1) ou de flux (jonction 0) comme le montre la figure (16).

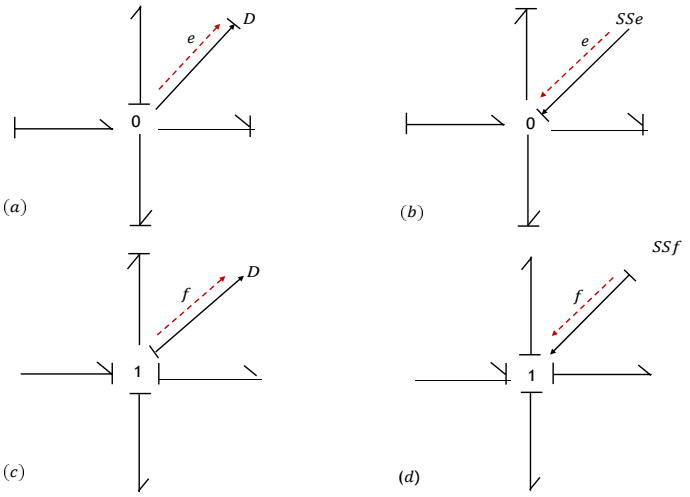

FIGURE 16 – (a) détecteur d'effort, (b) détecteur d'effort dualisé, (c) détecteur de flux, et (d) détecteur de flux dualisé

3.2.4 Matrice de signature des défauts

Le principe du calcul de la matrice de signature des défaut utilisé est celui développé dans [Touati (2012)]. **"La structure des résidus** r D $.r_1; r_2; :::; r_n/$ **forme une Matrice de Signature de Défauts (MSF) binaire ayant pour colonnes l'ensemble des ré- sidus et pour lignes l'ensemble des composants** C D $.C_1; C_2; :::; C_n/$ **qui peuvent être affectés par des défauts. Les éléments booléens de la matrice** $S_{i\,j}$ $.0; 1/$ **(tab. 3.3) nous renseignent sur la sensibilité des résidus aux défaillances. Les éléments de la MSF sont définis comme suit par l'équation (eq. 3.12):**

$$S_{ij} \begin{cases} 1; & Si\ la\ RRAj\ contient\ la\ \text{variable}\ C_i \\ 0; & Si\ non \end{cases} \quad (3.12)$$

	RRA_1	RRA_2	.....	RRA_n	Db	Ib
C_1	$S_{1;1}$	$S_{1;2}$	.....	$S_1; n$	Db_1	Ib_1
C_2	$S_{2;1}$	$S_{2;2}$	.....	$S_{2;n}$	Db_2	Ib_2
.....	.....	.....	.....	.....	.....	.....
C_{m-1}	$S_{m-1;1}$	$S_{m-1;2}$	.....	$S_{m-1;n}$	Db_{m-1}	Ib_{m-1}
C_m	$S_{m;1}$	$S_{m;2}$	.....	$S_{m;n}$	Db_m	Ib_m

Tableau 3.3 – La matrice de signature de défaut (FSM)

Le vecteur Db **représente la détectabilité d'un défaut. Les éléments de ce vecteur sont calculés en utilisant les équations suivantes (eqs. 3.13, 3.14) :**

$$Db_j \text{ D } 1\ si\ au\ moins\ une\ RRA\ contient\ la\ \text{variable}\ C_j \quad (3.13)$$

$$Db_j \text{ D } 0\ Si\ non \quad (3.14)$$

Le vecteur Ib **représente l'isolabilité structurelle d'un défaut. Les éléments de ce vecteur sont obtenus comme suit (eqs. 3.15, 3.16) :**

$$Ib_j \text{ D } 1\ si\ la\ signature\ \{S_{1;j}; S_{2;j}; :::; S_{n;j}\}\ est\ unique \quad (3.15)$$

$$Ib_j \text{ D } 0\ Si\ non \quad (3.16)$$

Deux défauts f_1 **et** f_2 **ne sont pas isolables s'ils ont la même signature".**

3.2.5 Génération des seuils adaptatifs

La relation de redondance analytique peut être décomposée en deux parties. La partie de référence qui est le résidu, elle ne contient que les valeurs de référence des mesures et des paramètres. La seconde est la partie incertaine ; cette partie est utilisée pour calculer le

seuil. Le seuil est calculé en tenant compte de la valeur absolue maximale des incertitudes. Les incertitudes sont considérées comme limitées.

Le problème de la détection, tel qu'il a été abordé dans les travaux précédents, consiste à comparer la partie référence (cas sans défaut) de la relation de redondance analytique (le résidu) et sa partie incertaine (le seuil adaptatif). En général, la comparaison est effectuée en temps réel. Un défaut est détecté si le résidu dépasse le seuil, sinon le système est en situation normale.

$$\begin{cases} r < th \quad pas\ de\ défaut\ \ F = \{f\} \\ r > th \quad cas\ \ défaut\ F = \{f_f\} \end{cases} \tag{3.17}$$

Un défaut entraîne généralement un effort ou un flux supplémentaire sur le résidu.

$$r_f(t) = r(t) + e_f$$

ef est le flux ou l'effort causé par la faute

Ce défaut est détecté si et seulement si le flux ou l'effort causé rend le résidu supérieur au seuil. .

$$\begin{cases} r < |Th| \quad pas\ de\ défaut \\ \text{présence défaut} \quad \cap \quad r + e_f > |Th| \end{cases} \tag{3.18}$$

3.3 Conclusion

Dans ce chapitre, nous avons présenté la méthode de détection de défauts par bond graph. Cette méthode peut être appliquée sur les systèmes dynamiques dans différents domaines. Le bond graph permet de modéliser le processus physique et la partie communication des systèmes. Le processus de surveillance de systèmes à base de bond graph est composé de 4 étapes, à savoir : la génération du modèle bond graph du système, la génération des relations de redondance analytique, le calcul de la matrice de signature et la génération des seuils adaptatifs pour la détection des défauts. Cette méthode va être adaptée par la suite pour la détection des attaques cyberphysqiues qui changent le comportement.

CHAPITRE 4

Modélisation et détection d'attaques par BG

Contents

Introduction

L'application des techniques traditionnelles de FDI à la détection et à l'isolation des cyberattaques a fait l'objet d'un effort de recherche considérable. Par exemple, les auteurs de [Cárdenas et al. (2011)] ont formulé le problème de la détection des cyberattaques contre les systèmes de contrôle des processus comme le problème du diagnostic des défauts. Les systèmes de contrôle des processus sont décrits comme un système linéaire invariant en temps discret. Les sorties estimées sont comparées aux mesures reçues, qui sont probablement compromises, pour générer la séquence de résidus. Les résidus sont ensuite évalués en utilisant soit des tests d'hypothèses séquentiels, soit des techniques de détection séquentielle de points de changement. Afin de contourner les paramètres inconnus, les auteurs proposent d'utiliser l'algorithme non paramétrique CUSUM pour détecter l'attaque. Les inconvénients de ce travail résident toutefois dans le fait qu'il n'a pas pris en compte ni les effets des bruits aléatoires, ni le problème de l'isolation.

Il a été démontré dans [Amin et al. (2013)] que l'une des attaques les plus puissantes visant les systèmes SCADA est l'attaque par tromperie. Un exemple spécifique de ce type d'attaque : l'adversaire peut lancer des cyberattaques sur les mesures des capteurs ("injection de fausses données", ou "false data injection attack") avec l'objectif d'introduire des erreurs arbitraires dans certaines variables d'état tout en contournant les mauvaises mesures de détection des données mises en place.

Dans ce chapitre, nous présentons une méthode de détection d'attaque par injection de fausses données par l'outil de modélisation des systèmes multidisciplinaires bond graph.

4.1 Attaque par injection de fausses données

Les attaques par injection de fausses données peuvent inclure une mesure de capteur ou une entrée de contrôle incorrecte [Mo and Sinopoli (2009)]. Le problème de ce type d'attaque a été abordé dans plusieurs travaux. Les auteurs de [Reaves and Morris (2009); Teixeira et al. (2010)] ont étudié les attaques furtives/de tromperie sur les réseaux électriques à courant alternatif en se basant sur des modèles de systèmes obsolètes, imprécis et incomplets. De plus, les auteurs de [Xie et al. (2010, 2011)] ont montré que les attaquants malveillants pouvaient modifier les mesures des capteurs afin de faire varier les variables d'état estimées pour profiter des prix de l'électricité.

Dans [Mo et al. (2010); Mo and Sinopoli (2010)], les auteurs ont étudié les impacts d'une attaque par injection de fausses données sur un système gaussien linéaire à temps discret et invariant. Le filtre de Kalman est utilisé pour effectuer une estimation de l'état et un détecteur de défaillance est employé pour détecter les situations anormales. L'objectif de l'agresseur est de tromper l'estimateur d'état en injectant un certain nombre de données erronées dans les mesures des capteurs transmises à l'État d'un estimateur sur un canal de communication. Selon une analyse de [Mo et al. (2010); Mo and Sinopoli (2010)], les attaques par injection de fausses données proposées dans [Pasqualetti et al. (2015)
] correspondent aux attaques de sortie qui rendent un mode instable (le cas échéant) du système non observable. L'analyse dans [Mo et al. (2010); Mo and Sinopoli (2010); Pasqualetti et al. (2015)] montre que les attaques par injection de fausses données sont inadaptées si le système n'a pas de pôle instable ou si certains capteurs "critiques" sont protégés.

Dans cette partie nous proposons de détecter l'attaque par injection de fausses données affectant les mesures du capteur et la partie contrôle/commande du systèmes SCADA par bond graph.

La différence entre BG et d'autres méthodes graphiques est que la première est directement issue du système physique, et non des équations de l'espace des états. De plus, d'après le modèle BG, les équations de l'espace des états peuvent être générés automatiquement à partir de logiciels spécialisés comme dans [Bouamama et al. (2005)], en utilisant une méthode systématique. Plusieurs problèmes ont été résolus de manière structurelle à l'aide de cette approche graphique, comme par exemple l'observabilité et la contrôlabilité, l'inversion du système, et les FDI [Bouamama et al. (2006)],[Samanta- ray and Ghoshal (2008)]. Dans ce manuscrit, la détection des attaques est basée sur la génération de RRA. Ensuite, en utilisant les ARRs, une matrice de signature de défaut (FSM) est générée et une décision de procédure logique est utilisée pour déterminer si une attaque est détectable et isolable.

4.1.1 Modélisation d'attaque par injection de fausses données sur la partie contrôle du SCADA

Dans un bond graph, un signal de contrôle est représenté avec une source d'effort ou de flux modulé, respectivement MSe , MSf. Ces sources sont généralement contrôlées par un signal de contrôle d'information. Ce signal est considéré comme SSI (pour Si- gnal d'Information), et le signal d'information modulée est considéré comme $MSI/$ (pour Signal d'Information Modulé)

En général, une attaque sur un signal de contrôle entraîne une modification de la valeur de ce signal de contrôle (par ajout ou soustraction appliqués sur cette valeur), qui peut être modélisée dans un bond graph par une source d'effort ou de flux supplémentaire en fonction de l'entrée contrôlée. Cela peut être présenté sous la forme (eq.4.1).

$$SSI^{Attacked} = SSI_C \pm SSI_{Att} \quad (4.1)$$

Où SSI_C est la valeur originale du signal de contrôle, et $SSI_{At\ t}$ est la valeur ajou- tée/soustraite par l'attaquant.

La représentation de l'attaque $SSI_{At\ t}$ par bond graph peut être visualisée dans (fig. 17).

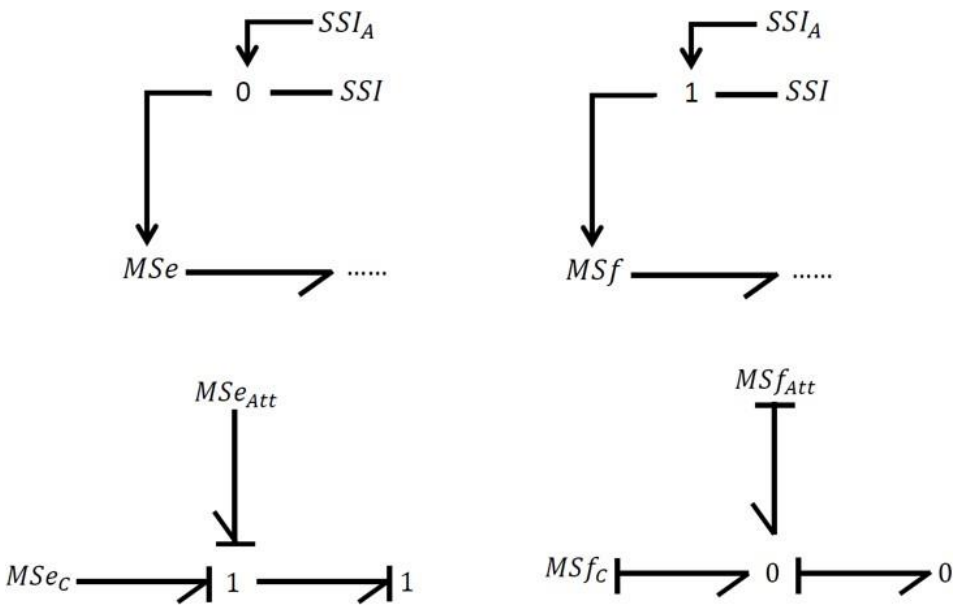

FIGURE 17 – Variable modulée effort/flux de la partie contrôle

4.1.2 Modélisation d'attaque sur le capteur

Semblable à l'attaque sur le signal de contrôle, l'injection de l'attaque sur le capteur se traduit généralement par un changement addition/soustraction appliqué à la valeur de mesure d'un capteur, qui peut être modélisé comme une source virtuelle d'effort ou de flux selon la nature du détecteur (effort ou flux).

La valeur du capteur attaqué peut être modélisée dans le cas d'effort et de flux respectivement par les équations suivantes (fig. 4.2,4.3) :

$$e_{Attaqué} = e_s - SSe_{Att} \quad (4.2)$$

$$f_{Attaqué} = f_s - SSf_{Att} \quad (4.3)$$

Où : e et f sont les capteurs attaqués, e_s et f_s les valeurs originales du signal du capteur, et SS_{Att} la valeur ajoutée/soustraite par l'attaquant de l'effort/du flux.

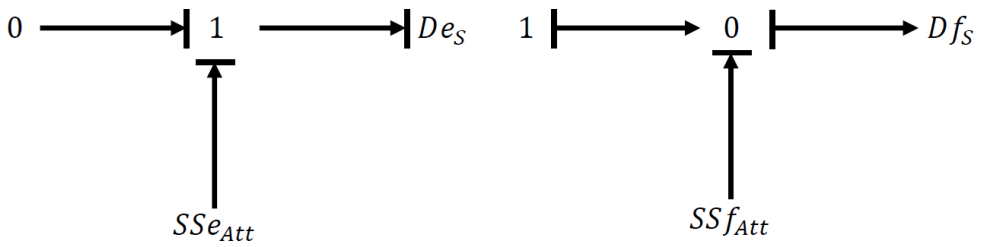

FIGURE 18 – Injection de fausse donnée sur le capteur

Après modélisation de l'attaque sur la partie contrôle et le capteur, nous allons suivre le processus de détection d'attaques par bond graph.

La détection d'une attaque entraîne la dualisation du capteur (capteur dualisé ==> le mettre en causalité dérivée). Dans notre cas, la représentation a pour résultat de dualiser le capteur attaqué modélisé précédemment. La dualisation consiste à changer la causalité du détecteur (De ou Df) et à le considérer comme un capteur d'effort/flux. La source d'effort/flux attaquée dépend de la somme du SSI (signal d'information) et de la valeur ajoutée.

Cela implique que, dans le cas effort d'un effort de capteur dualisé, l'équation peut être indiquée comme suit (eq. 4.4) :

$$SSe_{Attaqué} = SSe - SSe_{Att} \quad (4.4)$$

$$\overset{Attaqué}{SSe}$$

c'est l'effort attaqué dualisé. SS_e est la valeur réelle du capteur, et $SS_{eAt\ t}$ est la valeur ajoutée/soustraite par l'attaquant.

Et dans le cas de flux, le capteur dualisé donne l'équation (eq. 4.5) :

$$\overset{Attaqué}{SSf} = SSf - SSf_{Att} \tag{4.5}$$

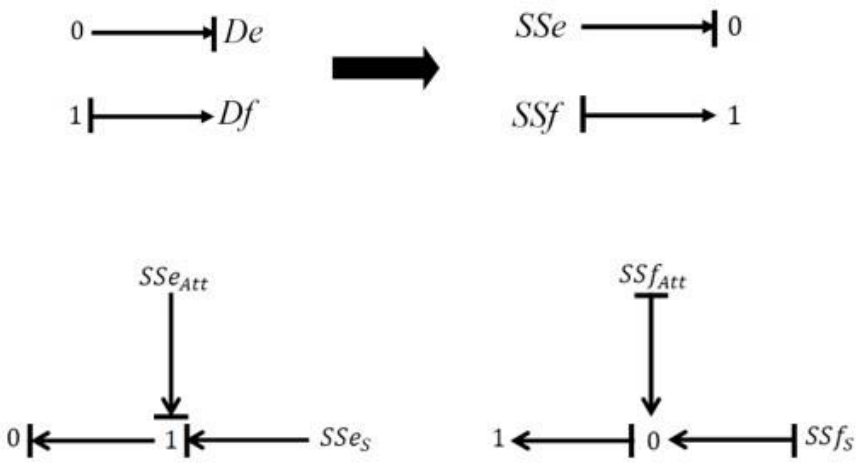

FIGURE 19 – Capteur effort/flux dualisé

La représentation des attaques sur le capteur par bong graph peut se faire de deux manières, la première étant présentée sur la figure (fig. 19). Dans [Touati (2002)], les auteurs ont présenté une deuxième façon de modéliser les incertitudes des mesures à l'aide du BG (fig. 20,21), qui représentent respectivement les cas du détecteur d'effort puis du détecteur de flux.

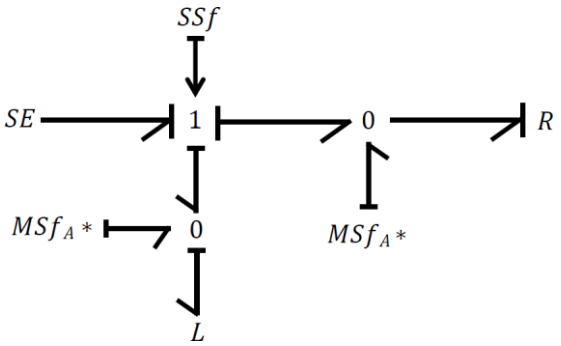

FIGURE 20 – Modélisation d'attaque sur le capteur "en cas d'effort"

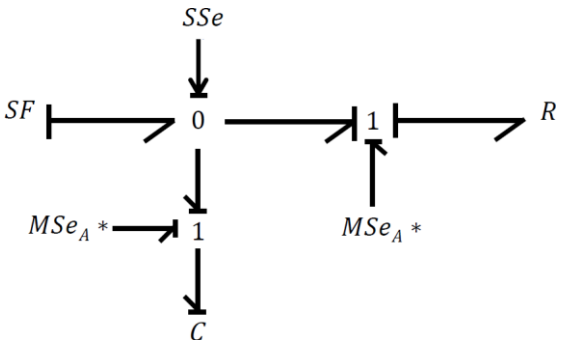

FIGURE 21 – Modélisation d'attaque sur le capteur "en cas de flux"

SE et SF représentent respectivement la source d'effort et de flux.

Dans la section suivante, nous allons adapter le processus de détection de défaut expliqué précédemment à la détection des attaques par injections de fausses données sur la commande et le capteur.

4.2 Détection d'attaque par bond graph

La méthode de détection des attaques par tromperie a été appliquée sur un système de robot de véhicule autonome (RobuCar) (fig. 22), disponible au laboratoir CRIStAL. Ici, nous avons appliqué la méthode de détection sur un quart de véhicule qui décrit la dynamique du système électromécanique utilisé pour faire tourner le contrôle décentralisé de la roue. Ce système dispose de trois capteurs : un capteur de courant, un capteur pour la vitesse angulaire et un capteur de la vitesse angulaire de la charge duvéhicule.

FIGURE 22 – Image du véhicule autonome RobuCar

4.2.1 Modèle de quart de véhicule

Le prototype de RobuCar est considéré comme une concaténation de quatre quarts de système symétrique de véhicule. Dans cette section, une modélisation détaillée des quarts

de RobuCar est présentée. Le quart de RobuCar de la Fig. (fig. 23) est considéré comme un système électromécanique composé de nombreuses pièces : partie électrique du moteur à courant continu, partie mécanique du moteur à courant continu, partie engrenages et partie roues, mécanisme de suspension, chaussée et environnement.

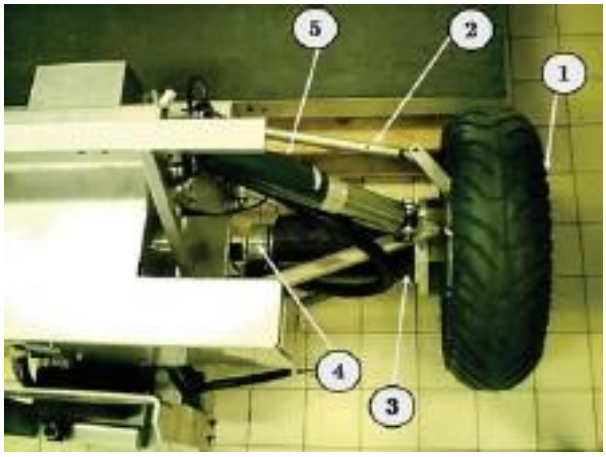

FIGURE 23 – Quart de véhicule intelligent et autonome avec 1 roue avant gauche, 2 axe de direction avant, 3 système électromécanique, 4 encodeur optique, 5 système de suspension

La figure (fig. 24) suivante montre les différents composants du quart du véhicule autonome RobuCar.

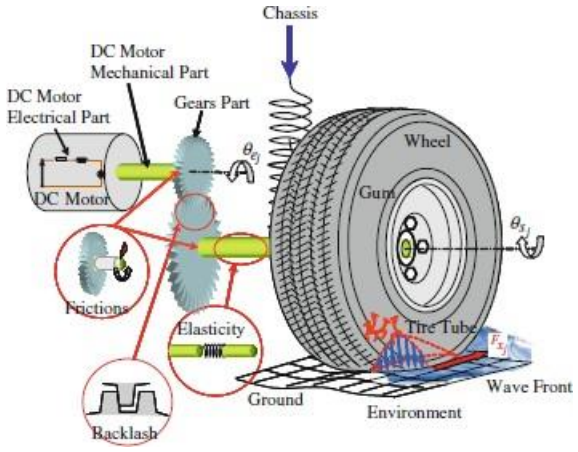

FIGURE 24 – Quart de véhicule intelligent et autonome, différents composants

4.2.2 Modélisation d'un quart de véhicule par bond graph

Selon la méthode de détection des attaques proposée, la première étape consiste à la modélisation du système (c'est-à-dire le mettre en causalité intégrale). Le système étudié est composé de trois parties distinctes : le moteur électrique à courant continu, le moteur mécanique à courant continu et la charge. Le système est équipé de trois détecteurs de

flux pour le courant, la vitesse angulaire du moteur et la vitesse angulaire de la charge, respectivement. Le modèle est représenté comme suit dans (fig. 25).

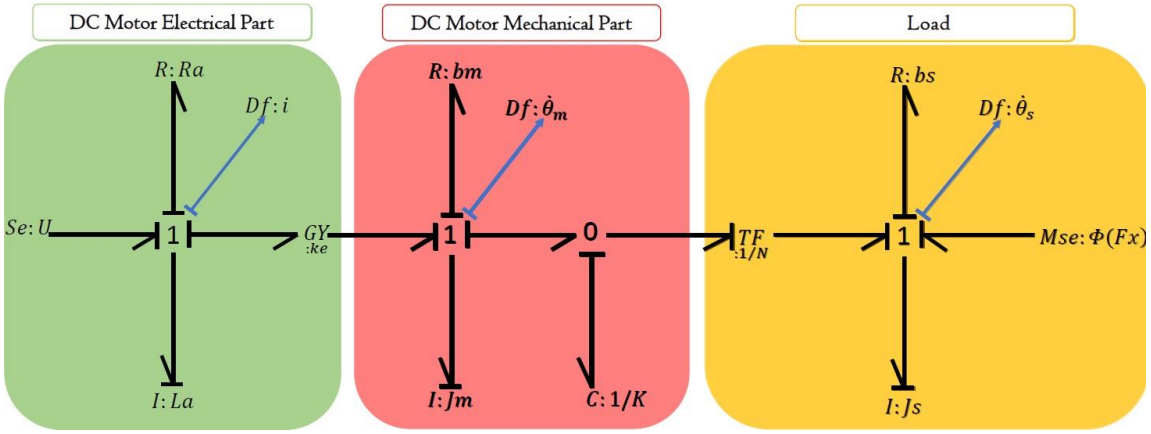

FIGURE 25 – Modèle bond graph en causalité intégrale de la roue RobuCar

Les symboles L_a, J_m et J_s dans la figure (fig. 25) représentent, respectivement, l'inductance électrique, l'inertie mécanique du moteur et l'inertie de la charge.

TF est le réducteur de vitesse.

C D $1=k$ est la rigidité de l'arbre.

R_a, b_m et b_s sont, respectivement, la résistance électrique, le frottement visqueux de la partie mécanique du moteur, et le frottement des charges visqueuses.

$M_{S\,e}$ représente l'interaction entre la roue et le sol.

Une fois le modèle bond graph de notre système généré, nous avons procédé à la génération des RRAs. Les relations de redondance analytique sont obtenues en mettant le modèle bond graph en causalité dérivée (c'est-à-dire dualisation du capteur). Les ARRs sont des équations dans lesquelles toutes les variables sont connues.

$$f.u;\ P;\mu/ \text{ D } 0 \tag{4.6}$$

u est le signal d'entrée

P sont les valeurs de paramètres

μ sont les valeurs de mesures

La génération des relations de ces équations permet de révéler les indicateurs d'attaque (résidu). En situation normale (sans attaque), ce résidu est statistiquement nul. Lorsqu'une attaque se produit, sa valeur s'éloigne de zéro.

Le modèle bond graph obtenu après avoir mis le détecteur en causalité dérivée est (fig. 26) :

Les ARRs peuvent être générées comme expliqué dans la section (3.2.3)

$$ARR_1 \text{ W } U - L_a\frac{di}{dt} - R_a i - Ke\dot{\theta}_m \text{ D } 0 \tag{4.7}$$

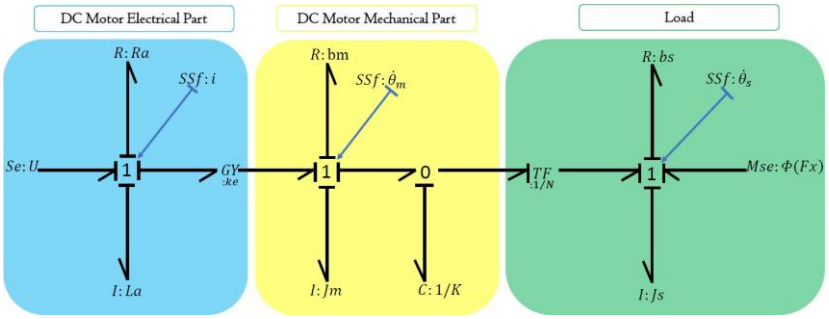

FIGURE 26 – Modèle bond graph en causalité dérivée de la roue RobuCar

$$ARR_2 \; \mathbb{W} Kei - b_m \dot{\theta}_m - J_m \frac{d\dot{\theta}_m}{dt} - K.\dot{\theta}_m - N\dot{\theta}_s \; / \mathbb{D} \; 0 \tag{4.8}$$

$$ARR_3 \; \mathbb{W} NK.\dot{\theta}_m - N\dot{\theta}_s / - b_s \dot{\theta}_s - J_s \frac{d\dot{\theta}_s}{dt} \; \mathbb{C} \; \hat{}.Fx / \mathbb{D} \; 0 \tag{4.9}$$

4.2.3 Génération de la matrice de signature d'attaque

Pour un bond graph, les relations de redondance analytique générées à partir du graphe sont utilisées pour former la matrice de signature de l'attaque.

La matrice ainsi obtenue est présentée dans le tableau (Tab. 4.1).

	ARR_1	ARR_2	ARR_3	AD_b	AI_b
Signal d'entrée (U)	1	0	0	1	1
Capteur de courant (i)	1	1	0	1	1
Capteur de vitesse angulaire du moteur ($\dot{\theta}_m$)	1	1	1	1	1
Capteurs de vitesse de charge angulaire ($\dot{\theta}_s$)	0	1	1	1	1

Tableau 4.1 – Matrice de signature d'attaque

Nous pouvons remarquer que les signatures des signaux sont unique, de ce fait, nous constatons que toutes les attaques seront détectables et isolables.

4.2.4 Calcul du seuil

L'évaluation des résidus peut être effectuée de manière dynamique en utilisant des paramètres et des incertitudes de mesure ou de manière statique en utilisant les caractéristiques statistiques des résidus [Djeziri et al. (2006)]. Dans notre étude, l'évaluation des résidus est effectuée par une méthode statistique utilisant les propriétés suivantes de la moyenne m et des normes déviation a. L'écart-type est utilisé pour mesurer la dispersion autour de la moyenne d'un ensemble de données lorsque les données analysées sont normalement distribuées. Dans [Djeziri et al. (2006)], la norme déviation a et la moyenne$m$

sont utilisées pour calculer l'enveloppement des données comme suit : 1.approximativement 68% des données seront dans l'interval : m — $a < x < m$ C a 2.approximativement 95% des données seront dans l'interval : m — $2a < x < m$ C$2a$ 3.approximativement 99% des données seront dans l'interval : m — $3a < x < m$ C$3a$

Où x est une valeur incluse dans un intervalle de données.

Dans notre cas, nous devons calculer des seuils. Afin de garantir que toutes les informations restent dans l'intervalle des seuils, nous prenons le seuil égal à m C $3a$, pour détecter l'attaque.

4.3 Résultat et discussion

Les résultats présentés ci-dessous ne prennent pas en compte les incertitudes des paramètres, mais nous considérons que le bruit de mesure du système peut être réduit à un signal de faible niveau.

Les valeurs des paramètres du système sont mentionnées dans le tableau suivant (Tab. 4.2) :

Parameters	values	unit(Si)
L_a	2.30	(H)
R_a	1.32	.▲/
J_m	0.002	$.N \times m \times s^2 = rad/$
b_m	0.003	$.N \times m \times s = rad/$
J_s	1.4	$.N \times m \times s^2 = rad/$
b_s	0.36	$.N \times m \times s = rad/$
N	0.0655 13	.N×m=A/
K	10	$.N \times m = rad/$

Tableau 4.2 – Paramètres du système

Avant de présenter les scénarios de détection d'attaques, on commence par présenter dans les figures (fig. 27, 28), les résultats de simulation du système dans le cas de son fonctionnement normal sans attaque.

Dans la figure (fig. 28) nous représentons la redondance analytique relative à l'évaluation de résidu en mode de fonctionnement normal. En effet, il est clair que le résidu oscille autour de zéro. Cela est dû à la présence du bruit de mesure. On constate que les résidus oscillent encore dans l'intervalle des seuils. Les trois RRAs sont obtenues après dualisation des trois capteurs mentionnés ci-dessus.

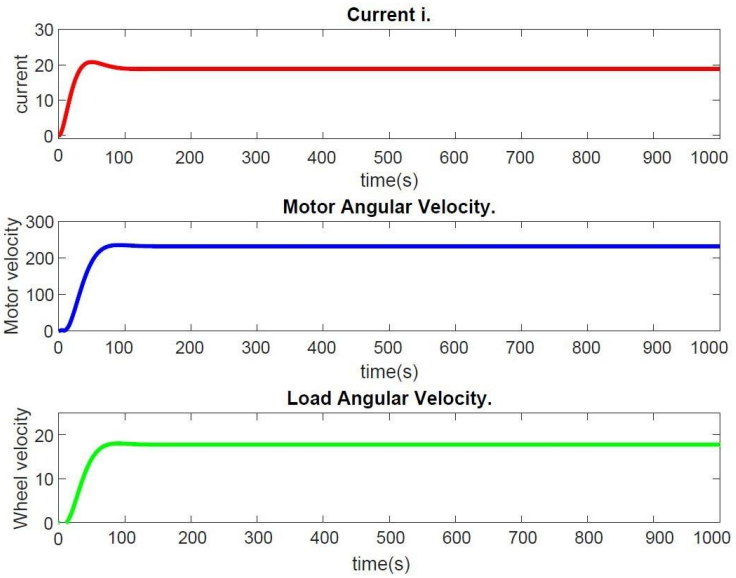

FIGURE 27 – Simulation des données du système

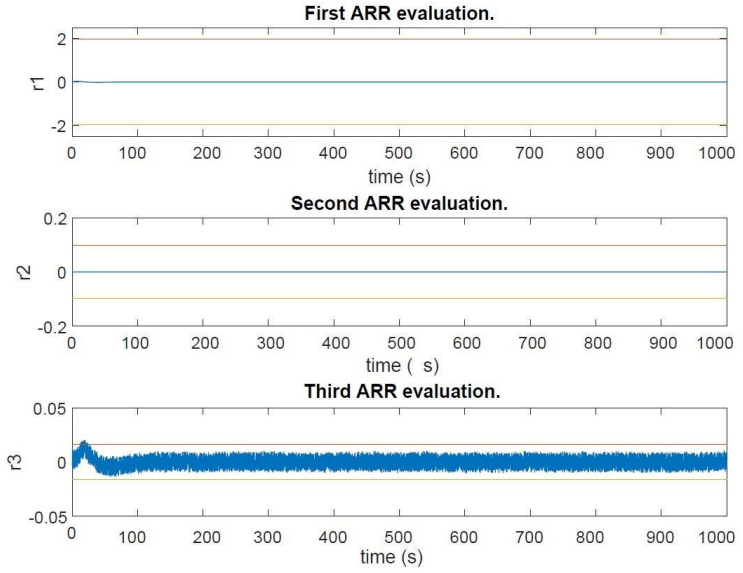

FIGURE 28 – RRAs obtenus dans le cas normal "sans attaque"

Deux scénarios d'attaques ont été appliqués sur le système. Le premier scénario concerne une attaque appliquée sur les mesures du capteur de courant à l'instant t D $40s$. Les résultats de l'attaque sont présentés dans la figure (fig. 29). Comme l'attaque est appliquée seulement sur les mesures du capteur de courant, les autres résultats sont en état normal.

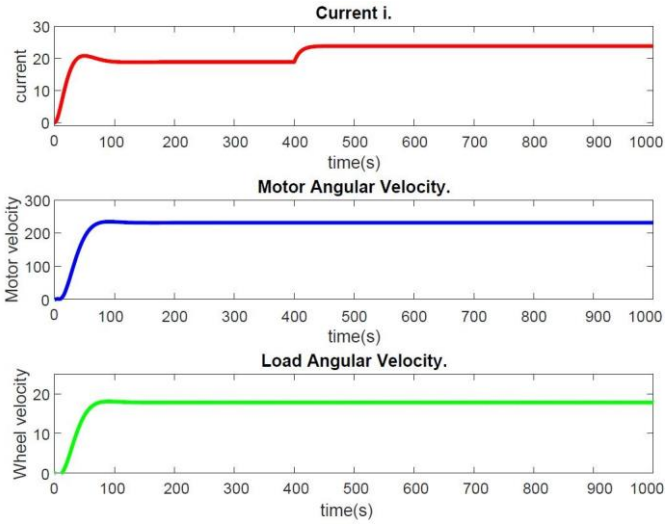

FIGURE 29 – Attaque détectée sur la mesure du capteur de courant Le

résultat de l'évaluation des résidus est représenté dans la figure (fig. 30).

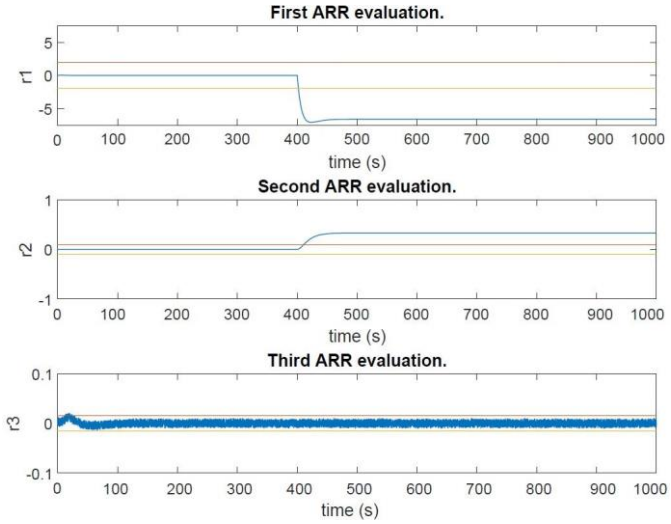

FIGURE 30 – Evaluation de résidu d'une attaque sur le capteur du courant

Le deuxième scénario d'attaque vise le capteur de la vitesse angulaire du moteur. Cette attaque a eu lieu à l'instant t D $40s$. Le résultat obtenu, présenté dans la figure (fig. 31), nous permet de détecter l'attaque.

Les résultats présentés dans la figure (fig. 31) montrent la modification des valeurs du capteur de vitesse angulaire du moteur à t=40s. Cette attaque a été détectée. Selon la matrice de signature de l'attaque, toutes les relations de redondance analytique sont

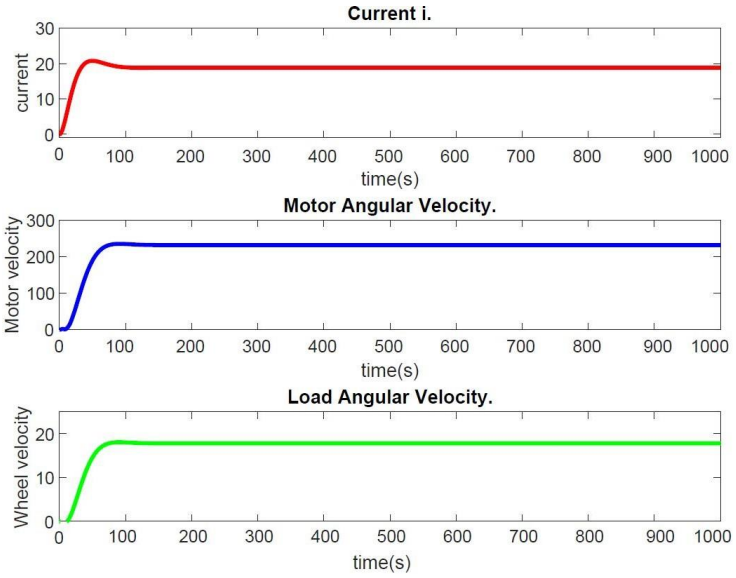

FIGURE 31 – La réponse de résidu sur l'attaque appliquée à la mesure capteur du vitesse angulaire du moteur

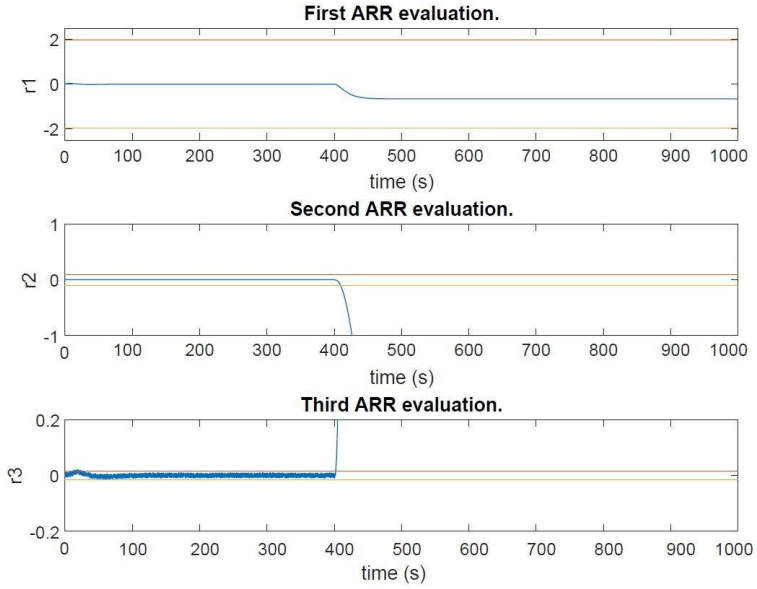

FIGURE 32 – La réponse de résidu sur l'attaque appliquée à la mesure capteur du vitesse angulaire du moteur

sensibles à cette attaque (fig. 31). Cette attaque a une signature unique ; en d'autres termes, elle est isolable.

4.4 Conclusion

Dans ce chapitre, nous avons présenté la méthodologie de détection et d'isolation des attaques de type injection de données fausses sur un quart de véhicule autonome intelligent RobuCar. Les simulations pratiquées en vue d'éprouver la dite méthode nous ont bien permis de détecter et d'isoler des attaques de ce type, ce qui est prometteur, mais nous manquons encore de données : c'est pourquoi il nous paraîtrait intéressant de répéter ces simulations, afin d'étudier les limites de notre procédé, d'évaluer les seuils sous lesquels il peut se révéler inexact voire inefficace, de préciser les probabilités de détecter faux-positifs et autres faux-négatifs (comment distinguer une panne d'une attaque ?), …

CHAPITRE 5

Détection d'attaques sur un robot mobile

Contents

5.1 Introduction

Ce chapitre présente une étude expérimentale sur la détection des attaques sur un ro- bot mobile autonome. Le robot utilisé dans cette étude est le Turtlebot. Les robots mobiles sont de plus en plus utilisés dans diverses applications tel que la logistique, l'automati- sation des ports, les opérations militaires et, récemment, dans le domaine de transport d'individus à l'image des véhicules autonomes Uber. Les informations, les commandes et les données sont transmises en utilisant les techniques de communication sans fil : on peut trouver les ondes radio, les ondes wifi et parfois même à travers les satellites. De ce fait, leurs vulnérabilités aux attaques malveillantes sont considérables et avoir un système de détection d'attaque s'avère nécessaire, si ce n'est indispensable.

Dans ce chapitre on commande le robot Turtlebot pour qu'il suive une trajectoire préparée a priori, cette dernière ayant été calculée de manière à ce qu'elle soit optimale. Dans un premier temps, on laisse le robot arriver à destination afin de vérifier la fiabilité des algorithmes de contrôle appliqués.

Après cette vérification, nous relançons la manipulation et attaquons le capteur Odo- métrie afin de fausser les informations, de sorte que le robot change de direction et perde sa trajectoire. L'attaque sera détectée une fois présente sur le système. L'expérience est faite en utilisant les deux logiciels ROS et MATLAB.

Comme montré sur la figure (fig. 33) nous présentons les différentes étapes d'une manière graphique. Comme nous proposons une alternative basée sur la redondance ma- térielle, dans le cas où les données nécessaires pour appliquer la méthode proposée seraient indisponibles.

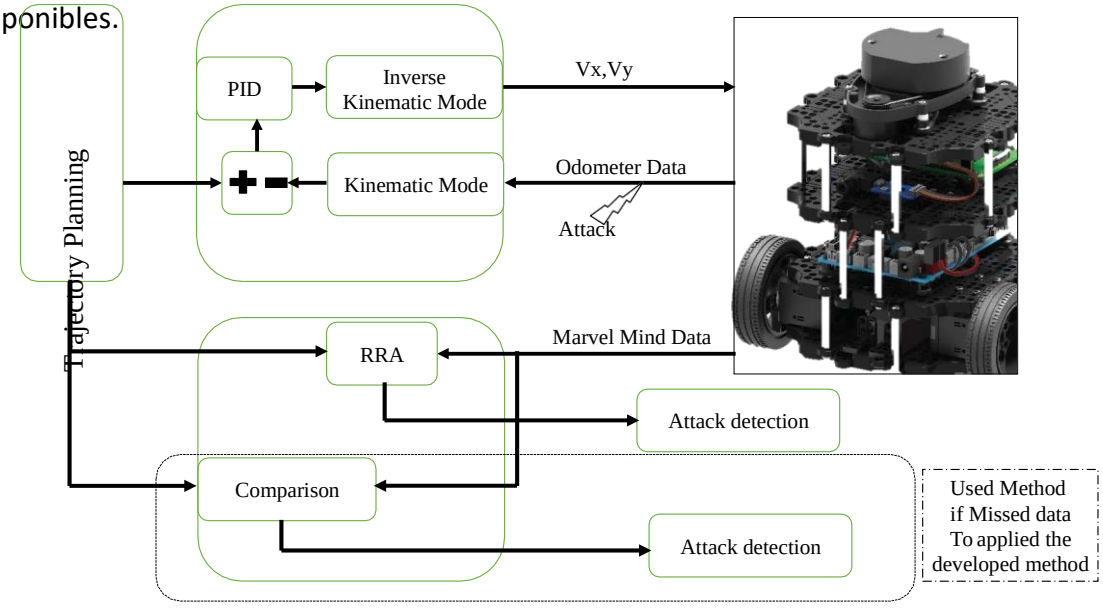

FIGURE 33 – Principe de la méthode de détection d'attaque sur le robot mobile

5.2 Matériels utilisés

5.2.1 Système d'exploitation pour Robot ROS

Le système d'exploitation du robot (ROS) n'est pas un système d'exploitation réel, mais plutôt une plateforme de développement logicielle ou un ensemble d'outils qui four- nissent la fonctionnalité d'un système d'exploitation sur un cluster d'ordinateurs hétéro- gènes. Son utilité n'est pas limitée aux robots mais, dans leur majorité, les outils fournis sont axés sur le travail avec du matériel périphérique. Le ROS est divisé en plus de 2000 paquets, chaque paquet fournissant des fonctionnalités spécialisées. Le nombre d'outils connectés à la plateforme est principale performance.

Le ROS fournit des fonctionnalités de matériel, les pilotes de périphériques, la communication entre les processus sur plusieurs machines, les outils de test et de visualisation, et bien plus encore.

La caractéristique principale du ROS est la façon dont le logiciel est exécuté et dont il communique, ce qui lui permet de concevoir des logiciels complexes sans avoir besoin de faire fonctionner un certain matériel. Le ROS permet de connecter un réseau de processus (nœuds) à un concentrateur central. Les nœuds peuvent être exécutés sur plusieurs appareils, et ils se connectent à ce concentrateur de différentes manières. En termes simples, il relie le matériel au logiciel afin de permettre un environnement de programmation avancé pour contrôler le matériel de bas niveau. Sans oublier qu'il dispose également d'outils puissants pour faire fonctionner les équipements en simulation, ainsi que des visualisations en 3D.

ROS fournit également des outils ou un ensemble de logiciels pour analyser, afficher, déboguer et organiser une application. A titre d'exemples, catkin qui est un système de gestion de paquets, génération et compilation automatiques de code, raviz qui est une interface utilisateur graphique pour afficher des modèles de robots et des applications dans un univers 2D, rasbag qui est un programme pour enregistrer et rejouer des séquences de sujets, et d'autres outils qui représentent le principal atout de ce système d'exploitation. Sans oublier les différentes bibliothèques conçues par la communauté robotique et qui visent à faciliter le développement en robotique, en fournissant des fonctionnalités de base, comme par exemple : Opencv pour la vision et Movelt pour la planification de mouvements.

5.2.2 Robot mobile

Un robot mobile a été utilisé pour la validation de l'approche proposée (TurtleBot3).

Turtlebot3

TurtleBot (fig. 34) est un kit de robot personnel à bas prix doté d'un logiciel libre. TurtleBot a été créé au Willow Garage par Melonee Wise et Tully Foote en novembre 2010. Avec TurtleBot, vous pourrez construire un robot capable de se déplacer dans votre maison, de voir en 3D et d'avoir suffisamment de puissance pour créer des applications passionnantes [Abci (2019)].

Le Turtlebot3 Burger de Robotis est composé de :

1. Un ordinateur embarqué (Raspberry Pi3) et son câble
2. Une carte de contrôle Open Source OpenCR ARM Cortex-M7 (programmable avec l'IDE Arduino)
3. Un châssis quatre servomoteurs Dynamixel série X (2 servomoteurs dans chaque roue)
4. Deux câbles USB deux câbles de connexion pour Dynamixel et Open CR
5. Des capteurs de navigation : un gyroscope, un accéléromètre et un magnétomètre 3 axes une batterie lithium polymère (11,1 V 1800 mAh/19.98 Wh 5C) et un câble d'extension
6. Des outils d'assemblage (179 pièces).

FIGURE 34 – Turtlebot3

La carte OpenCR (fig. 35) est développé pour les systèmes embarqués ROS afin de fournir du matériel et des logiciels entièrement libres. Tout ce qui concerne la carte ; les schémas, le Gerber du PCB, la nomenclature et le code source du micrologiciel pour le TurtleBot3 et l'OP3 sont libres d'être distribués sous des licences open-source pour les utilisateurs et la communauté ROS. La puce de la série STM32F7 à l'intérieur de la carte OpenCR est basée sur un ARM Cortex-M7 très puissant avec unité à virgule flottante. L'environnement de développement d'OpenCR est très ouvert, de l'IDE Arduino

et Scratch pour les jeunes étudiants au développement traditionnel de micrologiciels pour les experts.

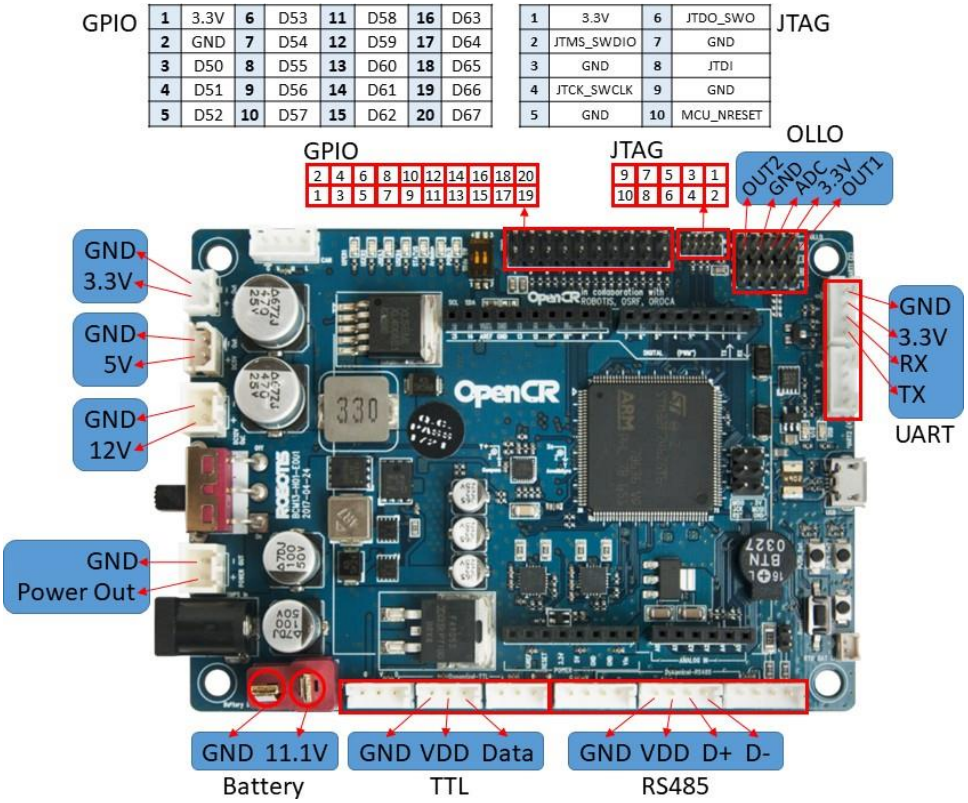

FIGURE 35 – Carte embarquée OpenCR

5.2.3 Système de navigation intérieure MarvelMind

MarvelMind (fig. 36) est un système de navigation intérieure prêt à l'emploi, conçu pour fournir des données de localisation précises à des robots. Il peut également être utilisé pour suivre des objets en mouvement grâce à des balises mobiles qui y sont fixées. Le système de navigation est composé de balises ultrasonores interconnectées par une interface radio dans une bande sans licence, une ou plusieurs balises mobiles installées sur les objets à suivre et un modem fournissant une passerelle vers le système à partir d'un autre ordinateur. Pour une localisation en trois dimensions, une ligne de visée non obstruée (ouie) entre une balise mobile et 3 balises fixes, ou plus, dans un rayon de 30 mètres doit être assurée. Pour une localisation en 2D, il faut au minimum deux balises fixes.

FIGURE 36 – Exemple MarvelMind

5.2.4 Système OptiTrack

L'OptiTrack (fig. 37) est un système qui consiste à capturer les mouvements d'un ob- jet se déplaçant dans une zone couverte par les caméras du système. Son fonctionnement est basé sur la photoprogrammétrie stéréoscopique où les données tridimensionnelles des points de l'objet sont à détecter. Ces points sont produits à partir de plusieurs caméras Prime 13 qui communiquent via Ethernet. Pour identifier les robots, des marqueurs détec- tables par les caméras sont utilisés, ainsi une configuration géométrique est donnée pour chaque robot en utilisant le logiciel Motive. Afin d'obtenir la position du robot à partir du logiciel sous ROS, le paquet vrpn-client-ros (Virtual Reality Peripheral Network) est utilisé.

FIGURE 37 – Système Optitrack

5.3 Expérience et Résultats

5.3.1 Modèle du Robot

Le robot Turtlebot est un robot mobile à deux roues motrices et une roue passive comme montré sur les figure (fig. 34). Le robot n'a pas de roue directionnelle donc il est considéré comme véhicule différentiel. La figure (fig. 39) présente le Bond graph mot du robot. Le modèle du robot sera comme suit : les roues seront modélisées entièrement en utilisant les bond graphs et le système directionnel sera modélisé comme bloc d'équation, les équations sont celles qui représentent la relation entre le comportement des roues et celui de châssis du robot, afin de faciliter le contrôle du turtlbot (fig.38).

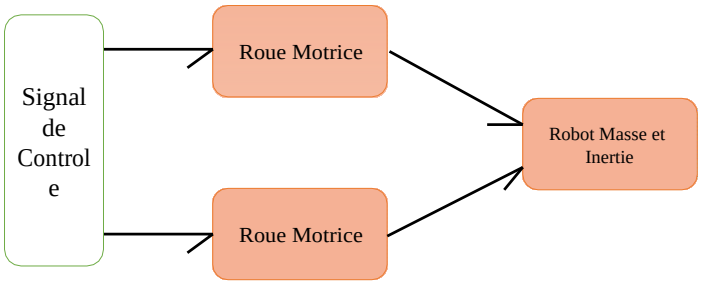

FIGURE 38 – Le Bond graph mot du Turtlrbot

$$\begin{cases} \dot{x} = \frac{R}{2}.(v_r + v_l)\cos\theta \\ \dot{y} = \frac{R}{2}.(v_r + v_l)\sin\theta \\ \dot{\theta} = \frac{R}{L}.(v_r - v_l) \end{cases} \tag{5.1}$$

$$\begin{pmatrix} v \\ \omega \end{pmatrix} = \begin{pmatrix} \frac{R}{2}.(v + v) \\ \frac{R}{L}.(v_r - v_l) \end{pmatrix} \tag{5.2}$$

5.3.2 Géneration des RRAs

Les RRAs seront générées en utilisant la méthode classique de génération des RRAs. Nous ne disposons pas de capteur de vitesse des roues mais nous disposons de capteur vitesse du robot et de sa position, donc nous pouvons avoir cette information en utilisant les équations qui gèrent le mouvement du robot.

$$F_r - J_w \frac{d\omega_r}{dt} - f\omega_r + \tau_{\frac{R}{2}} = 0 \tag{5.3}$$

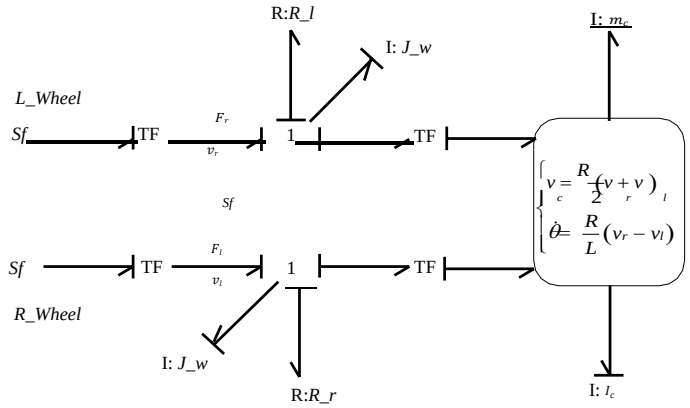

FIGURE 39 – Modèle Bond graph du Turtlebot3

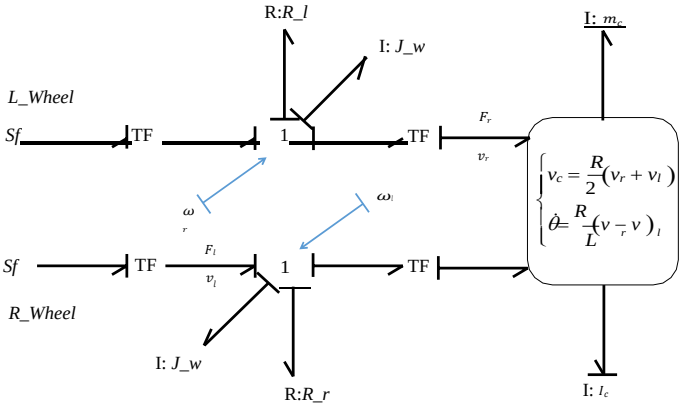

FIGURE 40 – Modele Bond graph du Turtlebot en causalité dérivée

$$F_l - J_w \frac{d!_l}{dt} - f!_l + \iota \frac{R}{2} = 0 \tag{5.4}$$

Avec, F_r force linéaire générée par la roue droite F_l force linéaire générée par la roue gauche, $!_l; !_r$ la vitesse angulaire des roues gauche et droite respectivement, ι est le couple généré par les mouvements du robot. R_l , R_r sont les frottements visqueux des deux roues celle de gauche et celle de droite avec $R_l = R_l = f$. Nous considérons ici que l'inertie des deux roues et la mêmeJ_w.

5.3.3 Calcul des seuils

Le seuil a été calculé en utilisant les mêmes valeurs présentées dans la section (Sec. 4.2.4).

5.3.4 Résultats expérimentaux

Cette section montre les résultats obtenus expérimentalement en utilisant les algorithmes développés précédemment. Le robot était programmé pour parcourir une trajectoire prédéfinie, calculée a priori d'une façon optimale. La figure (fig. 41) montre la trajectoire planifiée. Le premier scénario était que le robot parcourt la trajectoire sans attaque afin de vérifier la cohérence des algorithmes de contrôle. Le robot a réussi le suivi de cette trajectoire.

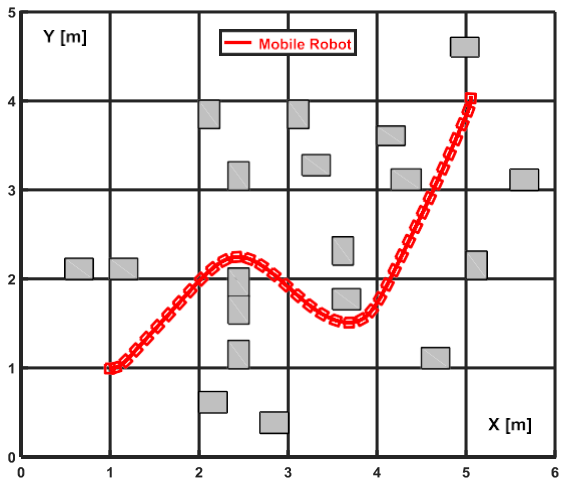

FIGURE 41 – Trajectoire planifiée

Les deux relations de redondance analytiques ont été vérifiées. Comme attendu, aucune déviation du comportement normal prévu n'est remarquée sauf quelques dépassements de

seuil sur la première relation de redondance analytique : cela est dû aux perturbations présentes sur les capteurs.

Les figures (fig. 42) et (fig. 43) montrent l'évaluation des deux équations de redon- dance analytique comme nous l'avons expliqué. Cette évolution montre que le robot a un comportement normal.

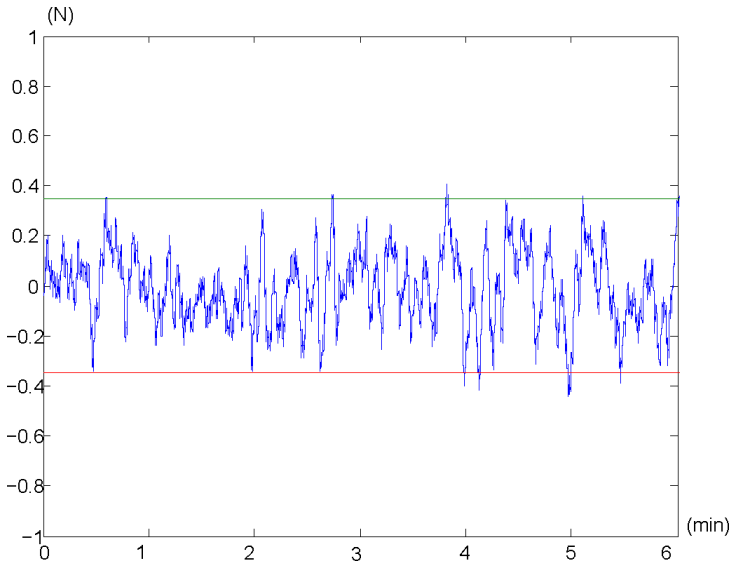

FIGURE 42 – Première relation de redondance analytique sans attaque

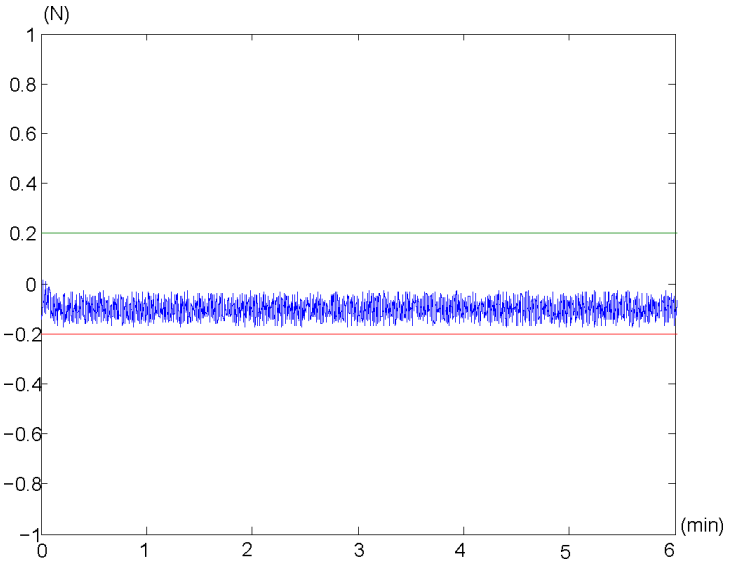

FIGURE 43 – Deuxième relation de redondance analytique sans attaque

Le deuxième scénario était que le robot serait attaqué quand il arriverait à la position (2.55 m,2.20 m), de manière à ce qu'il change de trajectoire et n'évite pas l'obstacle en face. La figure Fig (fig. 44) donne une explication graphique de ce scénario.

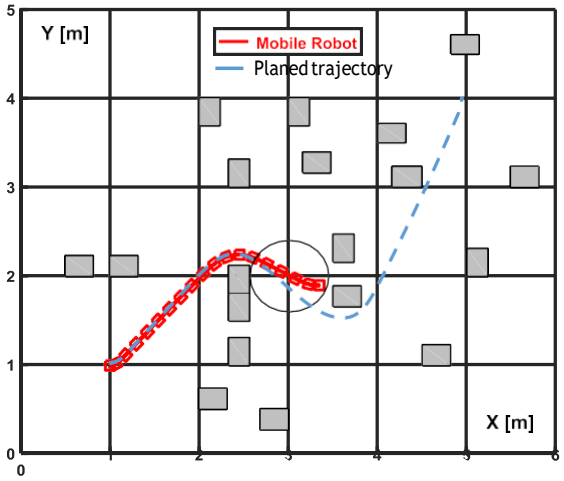

FIGURE 44 – Trajectoire sous attaque

En se référant aux figures (fig. 45), (fig. 46) représentant les évaluations des première et deuxième relations de redondance analytique, respectivement, le lecteur peut conclure à l'efficacité de la méthode proposée. La détection de l'attaque est faite. Un dépassement des seuils autorisé est clairement vu, or nous avons remarqué un retard de quelques milli-secondes à la détection, cela étant dû à l'utilisation des filtres et au temps de transmission des données.

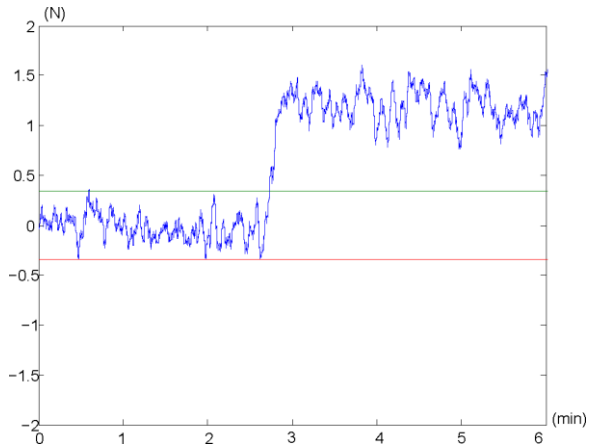

FIGURE 45 – Première relation de redondance analytique en présence d'attaque

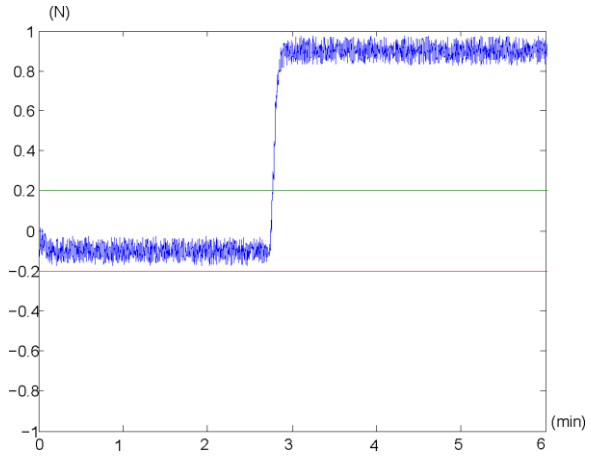

FIGURE 46 – Deuxième relation de redondance analytique en présence d'attaque

5.3.5 Conclusion

Ce chapitre s'intéresse à la sécurisation des robots mobiles et véhicules autonomes. Il présente une application de la méthode de détection développée dans cette thèse sur un robot mobile dédié à la recherche. En appliquant l'algorithme de détection d'attaque à base de bond graph, nous avons pu relever la présence d'une attaque sur le capteur odométrie : il serait désormais pertinent d'apprécier le domaine réel d'efficacité de cette détection, c'est-à-dire de définir précisément les limites en deça desquelles une attaque serait inaperçue ou mal interprétée par notre méthode.

Dans ce chapitre nous nous sommes intéressés au problème de la détection des attaques d'un point de vue automatique. Autrement dit, notre objectif était de détecter les attaques qui changent le comportement du système.

CHAPITRE 6

Conclusion générale

Cette thèse s'est intéressée au problème de surveillance et de détection des attaques cyberphysiques visant les systèmes de supervion et d'acquision des données SCADA. Les attaquants peuvents utiliser des techniques de la couche cyber et de la couche physique, d'abord pour contrôler les couches du réseaux, puis pour perturber les périphériques physiques. Ces attaques peuvent endommager le processus industriel et affecter la vie des personnes.

En termes de contribution, nous avons commencé cette thèse par décrire le système SCADA et son environnement physique et cyber. Nous avons fait un examen sur les différentes vulnérabilités et les attaques visant SCADA. Ensuite, nous avons donné une vue d'ensemble des différentes techniques existantes pour protéger les systèmes SCADA contre les attaques cyberphysiques du point de vue technologie de l'information et théorie du contrôle.

L'état de l'art a été complété par trois contributions principales. Tout d'abord, une première contribution a consisté à revisiter les approches de détection sur la partie cyber et physique, et à adapter des méthodes de détection et des défauts par bond graph à la détection des attaques.

Ensuite, dans une deuxième contribution, nous avons proposé une méthode de modélisation des attaques par tromperie plus précisément, les attaques par injection des données fausses qui changent le comportement du système, par le biais du changement des mesures des capteurs et de la commande. Cette modélisation a été effecuée à l'aide de l'outil de modélisation des systèmes pluridisciplinaires bond graph.

Pour la troisième contribution, nous avons proposé une méthode de détection des attaques mentionnées ci-dessus par la génération des relations de redondance analytique et l'évalution des résidus. Enfin, nous avons isolé l'attaque détectée à l'aide de la matrice de signature d'attaque. En fait, si une relation de redondance analytique a une signature unique, alors l'attaque est isolable.

Une contribution considérable de notre méthode sur un système de robots mobiles a été présentée. Cette contribution a été mise en place afin d'élargir l'utilisation de la méthode de détection de bond graph à la détection des attaques visant les systèmes commandés en réseaux.

En termes de perspectives des futures recherches (à la suite des travaux initiés dans le cadre de cette thèse), plusieurs actions restent à faire. Il convient de noter que les systèmes

SCADA doivent relever un grand nombre de défis. Cette thèse a abordé, avec une portée limitée, certains des défis de protection dans le domaine, en accordant une attention particulière à la détection des actions malveillantes qui changent le comportement du système. Néanmoins, les systèmes SCADA englobent de nombreux autres domaines qui doivent être traités ensemble afin d'améliorer leur résilience aux attaques et aux utilisations abusives. Dans cette optique, une première perspective comprendrait une analyse plus appro- fondie des attaques qui ne peuvent pas être détectées par les systèmes de détection infor- matique. En effet, les systèmes SCADA sont sujets à différents vecteurs d'attaque. Une adaptation de la méthode de modélisation de ces dernières par bond graph est prévue pour le futur. Comme deuxième perspective, on envisage la mise en place d'unmécanisme qui permet de faire la différence entre une attaque et un défaut de capteur ou de commande, en faisant une étude sur les différences et les ressemblances entre attaque et défaut.

Considérant les avantages des bonds graphs, nous pouvons aussi utiliser la méthode proposée ici pour le développement des algorithmes de contrôle tolérants aux attaques. Ces algorithmes seront un outil puissant pour lutter contre les dégâts qui peuvent être engendrés par les systèmes de la robotique mobile.

Bibliographie

Abci, B. (2019). *Approche informationnelle pour la navigation autonome tolérante aux défauts : application aux systèmes robotiques mobiles*. PhD thesis, Université de Lille.

Adams, T. (2004). Supervisory control and data acquisition (scada) systems. https: //www.cedengineering.com/userfiles/SCADA 20Systems.pdf.

Agudo, P. (1995). Gigantesque explosion d'un gazoduc dans le nord-est de la russie. https://www.humanite.fr/node/103270.

Almalawi, A., Yu, X., Tari, Z., Fahad, A., and Khalil, I. (2014). An unsupervised anomaly- based detection approach for integrity attacks on scada systems. *Computers Security*, 46 :94 – 110.

Amin, S., Litrico, X., Sastry, S., and Bayen, A. M. (2013). Cyber security of water scada systems—part i : Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, 21(5) :1963–1970.

Arvani, A. (2014). Detection and protection against intrusions on smart grid systems. *International Journal of Cyber-Security and Digital Forensics*, 3 :38–48.

Bailey, D. and Wright, E. (2003). *Practical SCADA for Industry*. Elsevier.

Barbosa, P., Brito, A., Almeida, H. O., and Clauß, S. (2014). Lightweight privacy for smart metering data by adding noise. In Cho, Y., Shin, S. Y., Kim, S., Hung, C., and Hong, J., editors, *Symposium on Applied Computing, SAC 2014, Gyeongju, Republic of Korea - March 24 - 28, 2014*, pages 531–538. ACM.

Benmoussa, S. (2013). Approche bond graph pour la détectabilité et l'isolabilité algé- briques de défauts composants.

Borutzky, W. (2011). *Incremental Bond Graphs*, pages 135–176. Springer New York, New York, NY.

Bouamama, B. O., Samantaray, A., Medjaher, K., Staroswiecki, M., and Dauphin-Tanguy, G. (2005). Model builder using functional and bond graph tools for fdi design. *Control Engineering Practice*, 13(7) :875 – 891. Control Applications of Optimisation.

Bouamama, B. O., Staroswiecki, M., and Samantaray, A. (2006). Software for supervision system design in process engineering industry. *IFAC Proceedings Volumes*, 39(13) :646

– 650. 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes.

Boyer, S. A. (2009). *Scada : Supervisory Control And Data Acquisition*. International Society of Automation, Research Triangle Park, NC, USA, 4th edition.

Brunner, M., Hofinger, H., Krauß, C., Roblee, C., Schoo, P., and Todt, S. (2010). Infiltra- ting critical infrastructures with next-generation attacks : W32.stuxnet as a showcase threat. *Fraunhofer SIT, Darmstadt*.

Cardenas, A., Amin, S., Sinopoli, B., Perrig, A., and Sastry, S. (2009). Challenges for securing cyber physical systems. *Proc. 1St Workshop Cyber-Phys. Syst. SecurityDHS*.

Cárdenas, A. A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., and Sastry, S. (2011). Attacks against process control systems : Risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communi- cations Security*, ASIACCS '11, page 355–366, New York, NY, USA. Association for Computing Machinery.

Cárdenas, A. A., Amin, S., and Sastry, S. (2008). Research challenges for the security of control systems. In *Proceedings of the 3rd Conference on Hot Topics in Security*, HOTSEC'08, USA. USENIX Association.

Cardenas, A. A., Amin, S., and Sastry, S. (2008). Secure control : Towards survivable cyber-physical systems. In *2008 The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500.

Chen, T. M. and Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer*, 44(4) :91–93.

Cocquempot, V. (2004). *Contribution à la surveillance des systèmes industriels complexes*. Habilitation à diriger des recherches, Université des Sciences et Technologies de Lille - Lille I.

Credeur, M. J. (2013). Fbi probes georgia water plant break-in on ter- ror concern. https://www.bloomberg.com/news/articles/2013-04-30/ fbi-probes-georgia-water-plant-break-in-on-terror-concern.

Damić, V. and Montgomery, J. (2015). *Bond Graph Modelling Overview*, pages 23–76. Springer Berlin Heidelberg, Berlin, Heidelberg.

Djeziri, M. A. (2007). *Fault Diagnosis of Uncertain Systems using Bond Graph Approach*. Theses, Ecole Centrale de Lille.

Djeziri, M. A., Merzouki, R., Bouamama, B. O., and Dauphin-Tanguy, G. (2006). Fault detection of backlash phenomenon in mechatronic system with parameter uncertainties using bond graph approach. In *2006 International Conference on Mechatronics and Automation*. IEEE.

Do, V. L., Fillatre, L., and Nikiforov, I. (2014). A statistical method for detecting cyber/physical attacks on scada systems. In *2014 IEEE Conference on Control Applica- tions (CCA)*, pages 364–369.

Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., and Han, Z. (2017). Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, 11(3) :1644–1652.

Falliere, N. (2010). Exploring stuxnet's plc infection pro- cess. https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=ad4b3d10-b808-414c-b4c3-ae4a2ed85560&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

Filippo, J. M.-D., Delgado, M., Brie, C., and Paynter, H. M. (1991). A survey of bond graphs : Theory, applications and programs. *Journal of the Franklin Institute*, 328(5) :565 – 606.

Fouladirad, M. and Nikiforov, I. (2005). Optimal statistical fault detection with nuisance parameters. *Automatica*, 41(7) :1157 – 1171.

Fovino, I. N. (2013). SCADA system cyber security. In *Secure Smart Embedded Devices, Platforms and Applications*, pages 451–471. Springer New York.

Fovino, I. N., Carcano, A., Masera, M., and Trombetta, A. (2009). An experimental investigation of malware attacks on SCADA systems. *International Journal of Critical Infrastructure Protection*, 2(4) :139–145.

Genge, B., Kiss, I., and Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, 10 :3 – 17.

Guo, Z., Shi, D., Johansson, K. H., and Shi, L. (2017). Optimal linear cyber-attack on remote state estimation. *IEEE Transactions on Control of Network Systems*, 4(1) :4–13.

Kabay, M. (2010). Attacks on power systems : Hackers, malware. https://www.networkworld.com/article/2217684/attacks-on-power-systems--hackers--malware.html.

Kang, D., Lee, J., Kim, S., and Park, J. (2009). Analysis on cyber threats to scada systems. In *2009 Transmission Distribution Conference Exposition : Asia and Pacific*, pages 1–4.

Knoepfel, S. (2013). Clarifying the international debate on stuxnet : Arguments for stuxnet as an act of war. In *Cyberspace and International Relations*, pages 117–124. Springer Berlin Heidelberg.

Kosut, O., Jia, L., Thomas, R. J., and Tong, L. (2010). Malicious data attacks on smart grid state estimation : Attack strategies and countermeasures. In *2010 First IEEE International Conference on Smart Grid Communications*. IEEE.

Krauss, C. (2018). Cyberattack shows vulnerability of gas pipeline net- work. https://www.nytimes.com/2018/04/04/business/energy-environment/ pipeline-cyberattack.html.

Krebs, B. (2008). Cyber incident blamed for nuclear power plant shut- down. https://www.waterfall-security.com/wp-content/uploads/2009/11/ CyberIncidentBlamedForNuclearPowerPlantShutdownJune08.pdf.

Kriaa, S., Bouissou, M., and Piètre-Cambacédès, L. (2012). Modeling the stuxnet at- tack with bdmp : Towards more formal risk assessments. In *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pages 1–8.

Krutz, R. L. (2005). *Securing SCADA Systems*. Wiley Pub.

Langner, R. (2011). Stuxnet : Dissecting a cyberwarfare weapon. *IEEE Security & Privacy Magazine*, 9(3) :49–51.

Lee, J., Bagheri, B., and Kao, H.-A. (2014). Recent advances and trends of cyber-physical systems and big data analytics in industrial informatics. ResearchGate. Keynote given at the 12th IEEE International Conference on Industrial Informatics (INDIN 2014), Porto Alegre, Brazil.

Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids – a com- prehensive survey. *Computer Standards Interfaces*, 56 :62 – 73.

Lin, H., Slagell, A., Kalbarczyk, Z. T., Sauer, P. W., and Iyer, R. K. (2018). Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. *IEEE Transactions on Smart Grid*, 9(1) :163–178.

Loukas, G. (2015). Cyber-physical attacks on industrial control systems. In *Cyber-Physical Attacks*, pages 105–144. Elsevier.

Loureiro, R., Merzouki, R., and Bouamama, B. O. (2012). Bond graph model based on structural diagnosability and recoverability analysis : Application to intelligent autono- mous vehicles. *IEEE Transactions on Vehicular Technology*, 61(3) :986–997.

Madden, J., McMillin, B., and Sinha, A. (2010). Environmental obfuscation of a cyber physical system - vehicle example. In *2010 IEEE 34th Annual Computer Software and Applications Conference Workshops*. IEEE.

Mo, Y., Chabukswar, R., and Sinopoli, B. (2014). Detecting integrity attacks on scada systems. *IEEE Transactions on Control Systems Technology*, 22(4) :1396–1407.

Mo, Y., Garone, E., Casavola, A., and Sinopoli, B. (2010). False data injection attacks against state estimation in wireless sensor networks. In *49th IEEE Conference on Decision and Control (CDC)*. IEEE.

Mo, Y. and Sinopoli, B. (2009). Secure control against replay attacks. In *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 911–918.

Mo, Y. and Sinopoli, B. (2010). False data injection attacks in control systems. *Preprints of the 1st Workshop on Secure Control Systems*.

Mo, Y., Weerakkody, S., and Sinopoli, B. (2015). Physical authentication of control systems : Designing watermarked control inputs to detect counterfeit sensor outputs. *IEEE Control Systems*, 35 :93–109.

Morris, T. and Pavurapu, K. (2010). A retrofit network transaction data logger and intrusion detection system for transmission and distribution substations. In *2010 IEEE International Conference on Power and Energy*. IEEE.

Nazir, S., Patel, S., and Patel, D. (2017). Assessing and augmenting scada cyber security : A survey of techniques. *Computers Security*, 70 :436 – 454.

Ngwompo, R. F., Scavarda, S., and Thomasset, D. (2001). Physical model-based inversion in control systems design using bond graph representation Part 1 : theory. *Proceedings of the Institution of Mechanical Engineers, Part I : Journal of Systems and Control Engineering*, 215(I2) :95–103.

Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H. (2012). Scada security in the light of cyber-warfare. *Computers Security*, 31(4) :418 – 436.

Nicola, M., Nicola, C.-I., Duta, M., et al. (2018). Scada systems architecture based on opc and web servers and integration of applications for industrial process control. *In- ternational Journal of Control Science and Engineering*, 8(1) :13–21.

Pasqualetti, F., Dorfler, F., and Bullo, F. (2011). Cyber-physical attacks in power net- works : Models, fundamental limitations and monitor design. In *IEEE Conference on Decision and Control and European Control Conference*. IEEE.

Pasqualetti, F., Dorfler, F., and Bullo, F. (2015). Control-theoretic methods for cyber- physical security : Geometric principles for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, 35(1) :110–127.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11):2715–2729.

Pasqualetti, F., Dörfler, F., and Bullo, F. (2015). Control-theoretic methods for cyber- physical security : Geometric principles for optimal cross-layer resilient control systems. *Control Systems, IEEE*, 35 :110–127.

Paynter, H. (1992). *An Epistemic Prehistory of Bond Graphs.in : Bond Graphs for Engi- neers. Breedveld, PC and Dauphin-Tanguy G. Eds*, pages 3–17. Elsevier.

Pham, N., Abdelzaher, T., and Nath, S. (2010). On bounding data stream privacy in distributed cyber-physical systems. In *2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*. IEEE.

Pothamsetty, V. and Franz, M. (2005). Scada honeynet project : Building honeypots for industrial networks. http://scadahoneynet.sourceforge.net/.

Poulsen, K. (2003). Slammer worm crashed ohio nuke plant network. https://www. securityfocus.com/news/6767.

Raghvendra, N. (2015). Scada system – components, hardware soft- ware architecture, types. https://electricalfundablog.com/ scada-system-components-architecture/.

Rahman, M. A. and Mohsenian-Rad, H. (2013). False data injection attacks against nonlinear state estimation in smart power grids. In *2013 IEEE Power & Energy Society General Meeting*. IEEE.

Rashid, F. Y. (2012). Telvent hit by sophisticated cyber-attack, scada admin tool compromised. https://www.securityweek.com/ telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised.

Reaves, B. and Morris, T. (2009). Discovery, infiltration, and denial of service in a process control system wireless network. In *2009 eCrime Researchers Summit*. IEEE.

Robert M. Lee, M. J. and Conway, T. (2016). Analysis of the cyber attack on the ukrainian power grid. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Roth, T. and Mcmillin, B. (2016). Physical attestation in the smart grid for distributed state verification. *IEEE Transactions on Dependable and Secure Computing*, PP :1–1.

Samantaray, A. and Ghoshal, S. (2008). Bicausal bond graphs for supervision : From fault detection and isolation to fault accommodation. *Journal of the Franklin Institute*, 345(1) :1 – 28.

Samantaray, A., Medjaher, K., Bouamama, B. O., Staroswiecki, M., and Dauphin-Tanguy, G. (2006). Diagnostic bond graphs for online fault detection and isolation. *Simulation Modelling Practice and Theory*, 14(3) :237–262.

Sandberg, H., Teixeira, A., and Johansson, K. H. (2010). On security indices for state estimators in power networks. In *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*.

Slay, J. and Miller, M. (2008). Lessons learned from the maroochy water breach. In Goetz, E. and Shenoi, S., editors, *Critical Infrastructure Protection*, pages 73–82, Boston, MA. Springer US.

Smith, R. S. (2011). A decoupled feedback structure for covertly appropriating networked control systems. *IFAC Proceedings Volumes*, 44(1) :90–95.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. (2015). Guide to industrial control systems (ICS) security. Technical report.

Stouffer, K. A., Falco, J. A., and Scarfone, K. A. (2011). Sp 800-82. guide to industrial control systems (ics) security : Supervisory control and data acquisition (scada) sys- tems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc). Technical report, Gaithersburg, MD, USA.

Tariq, N., Asim, M., and Khan, F. A. (2019a). Securing scada-based critical infrastruc- tures : Challenges and open issues. *Procedia Computer Science*, 155 :612–617.

Tariq, N., Asim, M., and Khan, F. A. (2019b). Securing SCADA-based critical infrastruc- tures : Challenges and open issues. *Procedia Computer Science*, 155 :612–617.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., and Sastry, S. S. (2010). Cyber security analysis of state estimators in electric power systems. In *49th IEEE Conference on Decision and Control (CDC)*. IEEE.

Teixeira, A., Sandberg, H., Dan, G., and Johansson, K. H. (2012). Optimal power flow : Closing the loop over corrupted data. In *2012 American Control Conference (ACC)*. IEEE.

Teixeira, A., Shames, I., Sandberg, H., and Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. *Automatica*, 51 :135–148.

Ten, C., Manimaran, G., and Liu, C. (2010). Cybersecurity for critical infrastructures : Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A : Systems and Humans*, 40(4) :853–865.

Touati, Y. (2002). *Contribution à la commande des systèmes complexes selon une approche orientée agents neuros-flous*. PhD thesis. Thèse de doctorat Université de Lille.

Touati, Y. (2012). Diagnostic robuste et estimation de défauts à base de modèle bond graph.

Tsang, R. (2010). Cyberthreats, vulnerabilities and attacks on scada networks.

Waidner, M. and Kasper, M. (2016). Security in industrie 4.0 — challenges and solutions for the fourth industrial revolution. In *Proceedings of the 2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. Research Publishing Services.

Watkins, C. M. and Rogers, J. D. (2008). Overview of the taum sauk pumped storage po- wer plant upper reservoir failure, reynolds county, mo. In *6th International Conference on Case Histories in Geothechnical Engineering, Arlington, VA*.

Wei Gao, Morris, T., Reaves, B., and Richey, D. (2010). On scada control system command and response injection and intrusion detection. In *2010 eCrime Researchers Summit*, pages 1–9.

Work, D., Bayen, A., and Jacobson, Q. (2008). Automotive cyber physical systems in the context of human mobility. In *Proceedings of the National Workshop on High-Confidence Automotive Cyber-Physical Systems, Troy, MI,USA*.

Xie, L., Mo, Y., and Sinopoli, B. (2010). False data injection attacks in electricity markets. In *2010 First IEEE International Conference on Smart GridCommunications*. IEEE.

Xie, L., Mo, Y., and Sinopoli, B. (2011). Integrity data attacks in power market operations. *IEEE Transactions on Smart Grid*, 2(4) :659–666.

Yang, Y., McLaughlin, K., Sezer, S., Littler, T., Im, E. G., Pranggono, B., and Wang, H. F. (2014). Multiattribute scada-specific intrusion detection system for power networks. *IEEE Transactions on Power Delivery*, 29(3) :1092–1102.

Yaseen, A. A. (2019). *Toward self-detection of cyber-physical attacks in control systems*. PhD thesis, Université de Lille 1.

Yuan, Y., Li, Z., and Ren, K. (2011). Modeling load redistribution attacks in power systems. *IEEE Transactions on Smart Grid*, 2(2) :382–390.

Yuan, Y., Zhu, Q., Sun, F., Wang, Q., and Basar, T. (2013). Resilient control of cyber- physical systems against denial-of-service attacks. In *2013 6th International Symposium on Resilient Control Systems (ISRCS)*. IEEE.

Zerdazi, I. and Fezari, M. (2019). Scada attack modeling using bond graph. In *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pages 1–2.

Zerdazi, I., Fezari, M., and Ouziala, M. (2020). Detection of deception attacks in super- visory control systems using bond graph. *Automatic Control and Computer Sciences*, 54(2) :156–167.

Zhioua, S. (2013). The middle east under malware attack dissecting cyber weapons. In *2013 IEEE 33rd International Conference on Distributed Computing Systems Work- shops*, pages 11–16.

Zhu, B., Joseph, A., and Sastry, S. (2011). A taxonomy of cyber attacks on SCADA systems. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE.

Zhu, B. and Sastry, S. (2010). Scada-specific intrusion detection/prevention systems : a survey and taxonomy. In *Proceedings of the 1st workshop on secure control systems (SCS)*, volume 11, page 7.