Projet DAC

Analyse et synthèse de Détecteurs d'Anomalies sous contrainte de temps-Critique

Thèse de Doctorat en Automatique et Traitement du Signal

(English version on page 6)

Mots-clés

Automatique - Traitement du Signal - Systèmes cyber-physiques - Sûreté - Sécurité - Détecteur d'anomalies (attaques, défauts) - Temps-critique - Optimisation Convexe

Informations pratiques

- Localisation : Ecole Centrale de Lyon, France
- Durée : 36 mois démarrant entre le 01/09/2024 et le 01/11/2024
- Date limite de candidature : 05/05/2024

Equipe d'encadrement

Gérard Scorletti (directeur de thèse), Ecole Centrale de Lyon, Lab. Ampère
Anton Korniienko, Ecole Centrale de Lyon, Lab. Ampère
Arthur Perodou, Ecole Centrale de Lyon, Lab. Ampère
Contact : **{gerard.scorletti ; anton.korniienko ; arthur.perodou}@ec-lyon.fr**

Collaboration potentielle

Une collaboration pourra être envisagée avec l'IMS Bordeaux (Ali Zolghadri, Christophe Combastel), incluant une possibilité d'accueil du/de la doctorant·e en visite à l'IMS.

Profil recherché

Tout·e candidat·e, titulaire d'un diplôme d'ingénieur·e ou d'un master, avec un **excellent dossier académique**, de cursus **spécialisé en Automatique et/ou Traitement du Signal OU de cursus généraliste** avec de bonnes compétences en **Mathématiques Appliquées**. Un intérêt dans le développement de méthodes à base d'optimisation et une expertise en MATLAB seraient aussi appréciées.

Contexte de travail du doctorat

L'École Centrale de Lyon (ECL) est un établissement public à caractère scientifique, culturel et professionnel. Membre du Groupe des Ecoles Centrales et du réseau des Écoles Nationales d'Ingénieurs, l'ECL forme des ingénieur·es généralistes de haut niveau, des ingénieur·es de spécialité, des étudiant·es en master et des docteur·es. L'établissement accueille 2500 élèves-ingénieur·es (étudiant·es et apprenti·es), 300 étudiant·es en master et plus de 250 doctorant·es. Il est caractérisé par une recherche reconnue adossée à 6 laboratoires de recherche. L'activité de recherche de l'ECL est orientée vers et pour le monde économique au travers de nombreux contrats industriels.

Le laboratoire Ampère est une unité mixte de recherche (CNRS, Ecole Centrale de Lyon, INSA Lyon, Université Lyon 1) de plus de 150 chercheur·euses basée à Lyon, France, qui travaille sur l'utilisation rationnelle de l'énergie dans les systèmes en relation avec leur environnement. Les travaux de recherche conduits au département Automatique pour l'Ingénierie des Systèmes (AIS) concernent le développement de méthodologies et d'outils visant l'optimisation et la maîtrise du comportement dynamique des systèmes et ce dans de très nombreux domaines d'applications, en collaboration avec les autres départements du laboratoire et d'autres laboratoires en sciences de l'ingénieur·e. L'association des dimensions théoriques et appliquées de ces recherches constitue sa grande originalité.

L'équipe d'encadrement a travaillé au cours des dernières années sur les possibilités offertes par les approches d'Automatique et de Traitement du Signal pour le développement de méthodes de conception/compréhension des systèmes relevant de différentes disciplines (Electronique, Energie Electrique, Mécanique, Biologie, etc.). En particulier, une expertise a été développée sur la conception de systèmes obtenus par l'interconnexion de sous-systèmes, pour lesquelles la combinaison de l'approche entrée-sortie avec des outils d'optimisation (convexe [BTN01, BV04]) apparaît particulièrement efficace. Des résultats probants ont déjà été obtenus, allant de contributions méthodologiques en amont (ex : [PKZS23, ACPKS23, LKD$^+$17]) jusqu'à leur application sur des problématiques avec un fort intérêt pratique (ex : [PKS$^+$21, KSCB16, GFS11]), et même au dépôt de brevet (ex : [PKZ$^+$17, CGK10, CK13]). Récemment, certains membres de l'équipe se sont mis à explorer la thématique de la sécurité des systèmes cyber-physiques (ex : [PCZ21b, PCZ21a, EMSZ20]).

Contexte scientifique du projet

La problématique de la sécurité des systèmes consiste à pouvoir **assurer la satisfaction des spécifications d'un cahier des charges en présence de comportements malveillants ou d'événements imprévus**. Historiquement divisée en la lutte contre des attaques physiques et la protection des technologies de l'information, l'augmentation significative de cyber-attaques contre des systèmes commandés (infrastructures industrielles, réseaux électriques, drones, ...) ces deux dernières décennies [DPF$^+$19, SRE$^+$19] et la limitation des approches classiques a

rendu nécessaire de développer une approche systémique de la sécurité des systèmes [SAJ15], prenant notamment en compte l'interaction entre les mondes cyber et physique (Fig. 1). D'un côté, les méthodes traditionnelles de sécurité des technologies de l'information se concentrent principalement sur la protection de l'information, et ne prennent pas directement en compte les répercussions physiques possibles de cyber-attaques. De l'autre, les approches classiques d'Automatique et de Traitement du Signal permettent de traiter la tolérance à des perturbations indépendantes, mais ne prennent pas en compte de possibles attaques d'acteurs rationnels malveillants. Ainsi, au cours de la dernière décennie, des approches ont été développées pour la prévention, la détection et l'atténuation des attaques sur les systèmes commandés [CST19, DPF+19].

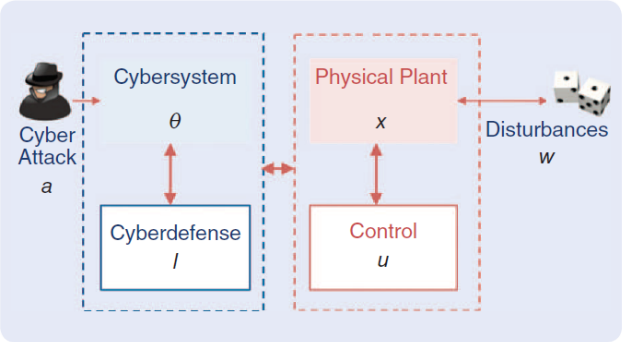

FIGURE 1 – Nécessité de considérer l'interconnexion entre mondes cyber et physique [ZB15]

Un **enjeu** important est de **trouver un compromis approprié entre le niveau de sécurité souhaité et la satisfaction d'un cahier des charges fonctionnel**. Cela est notamment dû à la difficulté d'évaluer le risque, et particulièrement la probabilité d'occurrence, d'une attaque du fait de l'hétérogénéité des attaquants, aussi bien en termes d'objectifs que de ressources [TSSJ15].

Problématique et Objectifs de la thèse

Dans ce contexte, l'ambition de cette thèse est de s'attaquer à la **problématique de l'analyse et la synthèse efficaces de détecteurs d'anomalies** (attaques, défauts) **sous contrainte de temps-critique**. Le **temps-critique** est l'horizon temporel maximal pour lequel un système est considéré comme étant dans un état sûr après l'apparition d'une anomalie, c'est-à-dire que le système n'est pas dans un état critique et est encore capable de revenir à un mode normal (Fig. 2). Cette **métrique de sécurité introduite récemment** [PCZ21a] apparaît comme pertinente à chaque étape du processus de **gestion de risque (analyse, prévention, détection, atténuation)**. La motivation sous-jacente est qu'une augmentation du temps-critique laisse davantage de temps aux mécanismes de défense, y compris les opérateurs humains, pour détecter et atténuer les anomalies.

La **performance des détecteurs d'anomalies** est traditionnellement évaluée selon trois critères : le **taux de détection**, le **taux de fausse alarme** et le **retard à la détection**. Lors de la **synthèse** d'un détecteur, **seuls les deux premiers critères** sont considérés. L'estimation du **retard à la détection**, et la vérification que le système ne rentre pas dans un état critique avant la détection (c'est-à-dire que le retard à la détection soit inférieur au temps-critique), est alors **estimé dans une phase post-synthèse** à l'aide de simulations.

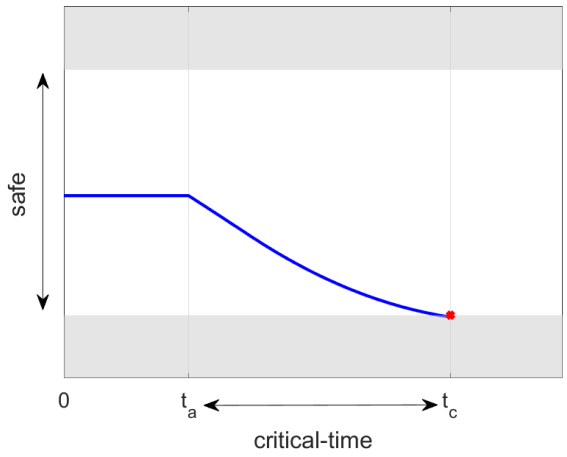

FIGURE 2 – Le temps-critique est l'horizon temporel maximal pour lequel un système est considéré comme étant dans un état sûr après l'apparition d'une anomalie (attaque, défaut).

Le **premier objectif** de cette thèse est de **développer une méthode d'analyse algorithmiquement efficace permettant de garantir formellement si le retard à la détection d'un filtre dans le pire-cas est inférieur au temps-critique**. Pour cela, les recherches pourront s'appuyer sur des travaux existants [PCZ21b, EMSZ20, BTMS17] sur le calcul du temps-critique et de la technique dite de la simulation robuste, et les étendre à des systèmes d'intérêt plus pratique (systèmes linéaires temps-invariants incertains). Le **deuxième objectif** sera de proposer une méthode permettant de prendre en compte la contrainte du temps-critique directement lors de la **synthèse du filtre de détection**. Un enjeu important pour ce deuxième objectif sera l'obtention d'une méthode algorithmiquement efficace, ce qui pourra nécessiter la simplification du problème (relaxation de contraintes, reformulation ou approximation pertinente du problème, etc.). Ces deux premiers objectifs se placent dans le contexte d'anomalies fulgurantes, c'est-à-dire ayant un fort impact sur le système en un temps limité. Le **troisième objectif** sera alors de synthétiser un détecteur d'anomalies de façon à **garantir un temps-critique minimum pour les attaques dites furtives**, c'est-à-dire des attaques conçues pour ne pas être détectées par le filtre.

Les contributions attendues étant essentiellement méthodologiques, les résultats seront principalement valorisés par des communications dans des conférences internationales et des publications dans des journaux de référence en Automatique.

Processus de recrutement

Les candidat·es intéressé·es, ou souhaitant plus d'information, sont vivement invité·es à se manifester en envoyant un mail contenant un CV + un court message de présentation et de motivation à l'équipe d'encadrement (voir adresses mails au début de ce document).

Le processus de recrutement se déroule en trois étapes :

1. **Candidature jusqu'au 05/05/2024**. **Audition au fil de l'eau** par l'équipe d'encadrement et sélection du/de la candidat·e.
2. Audition par le conseil de l'Ecole Doctorale EEA fin-Mai/début Juin.
3. Résultat final : première quinzaine de Juin.

Revenus et avantages

Rémunération de 2100€ brut mensuel [1]. La personne recrutée le souhaitant aura aussi l'opportunité d'intervenir dans les enseignements de l'équipe Automatique et Traitement du Signal de l'Ecole Centrale de Lyon, s'assurant ainsi un complément de salaire tout en profitant d'une expérience valorisable par la suite.

Perspectives professionnelles après le doctorat

Le/La docteur·e développera un ensemble de compétences qui seront valorisables dans de nombreux environnements professionnels. Sont notamment ciblés les métiers suivants : chercheur·euse, docteur·e-ingénieur·e, ingénieur·e R&D dans un établissement public ou dans le secteur privé, selon la formation initiale et les centres d'intérêts de la personne recrutée.

1. voir `https://www.enseignementsup-recherche.gouv.fr/fr/le-financement-doctoral-46472`

Project DAC

Analysis and synthesis of Anomaly Detectors under Critical-time constraints

PhD thesis in System, Control and Signal Processing

Keywords

System and Control Theory - Signal Processing - Cyber-physical systems - Safety - Security - Anomaly detector (attack, fault) - Critical-time - Convex Optimization

Practical Information

- Localization : Ecole Centrale de Lyon, Lyon (France)
- Duration : 36 month starting between 01/09/2024 and 01/11/2024
- Application deadline : 05/05/2024

Advisors

Prof. Gérard Scorletti (thesis director), Ecole Centrale de Lyon, Ampère-lab
Prof. Anton Korniienko, Ecole Centrale de Lyon, Ampère-lab
Dr. Arthur Perodou, Ecole Centrale de Lyon, Ampère-lab
Contact : **{gerard.scorletti ; anton.korniienko ; arthur.perodou}@ec-lyon.fr**

Potential collaboration

A collaboration with the IMS-lab (Prof. Ali Zolghadri, Dr. Christophe Combastel) in Bordeaux is considered, including the possibility of a visit of the PhD student to the IMS-lab.

Candidate profile

Any candidate holding an engineering degree or a Master's degree, with an **excellent academic record**, **specialized in System and Control or Signal Processing OR a general degree** with good skills in **Applied Mathematics**. An interest in the development of optimization-based methods and experience with MATLAB would also be appreciated.

Working environment

The École Centrale de Lyon (ECL) is a public scientific, cultural and professional institution. Mmember of the Ecoles Centrales group and the Écoles Nationales d'Ingénieurs network, ECL trains high-level generalist engineers, specialized engineers, masters students and doctoral candidates. The school hosts 2,500 engineering students and trainees, 300 master students and more than 250 doctoral students. It is characterized by recognized research supported by 6 research laboratories. ECL's research activities are directed to and for the business world through numerous industrial contracts.

The Ampère-lab is a joint research unit (CNRS, Ecole Centrale de Lyon, INSA Lyon, Université Lyon 1) of more than 150 researchers based in Lyon, France, working on the rational use of energy in systems in relation to their environment. The research carried out by the Automatique pour l'Ingénierie des Systèmes (AIS) department includes the development of methods and tools for optimizing and controlling the dynamic behavior of systems in a wide range of application domains, in collaboration with other departments of the laboratory and other engineering laboratories. The combination of theoretical and applied dimensions of this research constitutes its great originality.

Over the last few years, the advisors have been working on the possibilities offered by Systems, Control and Signal approaches for the development of methods for the design/understanding of systems from different disciplines (electronics, electrical engineering, mechanics, biology, etc.). In particular, expertise has been developed in the design of systems obtained by interconnecting subsystems, for which the combination of the input-output approach with (convex [BTN01, BV04]) optimization tools seems to be particularly effective. Convincing results have already been obtained, ranging from upstream methodological contributions (e.g. [PKZS23, ACPKS23, LKD$^+$17]) to their application to problems of strong practical interest (e.g. [PKS$^+$21, KSCB16, GFS11]), and even to patent deposit (e.g. [PKZ$^+$17, CGK10, CK13]). Recently, some team members have begun to explore the topic of the security of cyber-physical systems (e.g., [PCZ21b, PCZ21a, EMSZ20]).

Scientific background of the project

The challenge of system security is **to ensure that the specifications are met even in the face of malicious behavior or unforeseen events**. Historically divided into the fight against physical attacks and the protection of information technologies, the significant increase in cyber-attacks against controlled systems (industrial infrastructures, power grids, drones, ...) over the last two decades [DPF$^+$19, SRE$^+$19] and the limitations of conventional approaches have made it **necessary to develop a systemic approach to system security** [SAJ15], taking into account in particular the interaction between the cyber and physical worlds (Fig. 3). On the one hand, traditional IT security methods focus primarily on protecting information and do not directly consider the possible physical consequences of cyber-attacks. On the other hand, classical Control and Signal Processing approaches address tolerance to independent

disturbances, but do not consider possible attacks by malicious rational actors. Thus, over the last decade, approaches have been developed to prevent, detect, and mitigate attacks on controlled systems [CST19, DPF+19].

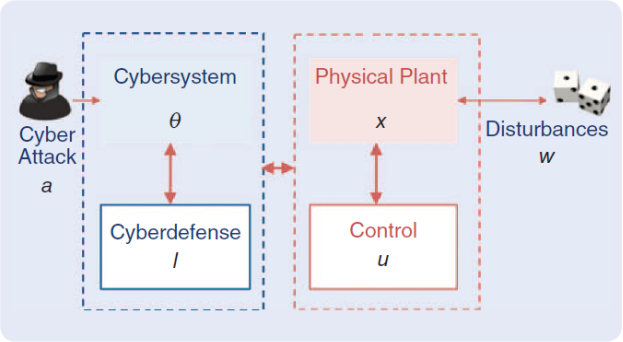

FIGURE 3 – The need to consider the interconnectedness of the cyber and physical worlds [ZB15]

An important issue is **to find an appropriate trade-off between the desired level of security and the satisfaction of a functional specification**. This is due in particular to the difficulty of assessing the risk, and especially the likelihood, of an attack due to the heterogeneity of attackers, both in terms of objectives and resources [TSSJ15].

Problem and Objectives of the thesis

In this context, the ambition of this thesis is to tackle the **problem of efficient analysis and synthesis of anomaly detectors** (attacks, faults) **under critical-time constraint**. The **critical-time** is the maximum time horizon for which a system is considered to be safe after the occurrence of an anomaly, i.e. the system is not in a critical state and is still able to return to a normal mode (Fig. 4). This **recently introduced security metric** [PCZ21a] seems to be relevant at every stage of the **risk management process (analysis, prevention, detection, mitigation)**. The underlying motivation is that an increase in critical-time gives defense mechanisms, including human operators, more time to detect and mitigate anomalies.

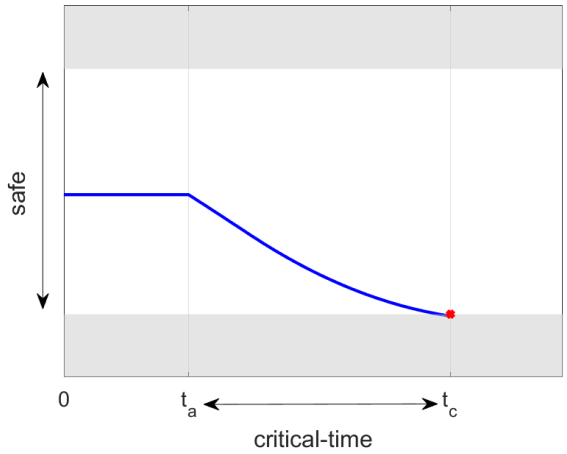

FIGURE 4 – The critical-time is the maximum time horizon for which a system is considered to be safe after the occurrence of an anomaly (attack, failure).

The performance of anomaly detectors is traditionally evaluated according to three criteria : **detection rate**, **false alarm rate** and **detection delay**. **When synthesizing a detector,**

only the first two criteria are considered. The estimation of the **detection delay** and the verification that the system does not enter a critical state before detection (i.e. that the detection delay is less than the critical time) are then **estimated in a post-synthesis phase** using simulations.

The **first objective** of this thesis is **to develop an algorithmically efficient analysis method that allows to formally guarantee whether the worst-case detection delay of a given filter is less than the critical time**. To achieve this, the research could build on previous work [PCZ21b,EMSZ20,BTMS17] on critical time computation and robust simulation techniques, and extend them to systems of practical interest (such as uncertain linear time-varying systems). The **second objective** is to propose a method able to take into account the critical-time constraint directly in the **synthesis of the detection filter**. An important challenge will be to obtain of an algorithmically efficient method, which may require to simplify the problem (constraints relaxation, reformulation or relevant approximation of the problem, etc.). These first two objectives take place in the context of sharp anomalies, i.e. with a severe impact on the system in a reduced amount of time. The **third objective** will be to synthesize an anomaly detector in order to **guarantee a minimum critical-time for the so-called stealthy attacks**, i.e. attacks designed not to be detected by the filter.

As the expected contributions are mainly methodological, the results will be valorized mainly through presentations at international conferences and publications in leading journals in the field of Control and System theory.

Recruitment process

Interested candidates, or those wishing more information, are warmly invited to send an e-mail containing a CV + a short message of presentation and motivation to the advisors team (see e-mail addresses at the beginning of this document).

The recruitment process consists of three stages :

1. **Application until 05/05/2024**. **Oral interview** by the advisors team and selection of the candidate.
2. Oral interview by the EEA Doctoral School Board in late May/early June.
3. Final result : first half of June.

Income and Benefits

Salary of 2100€ (gross) per month.

Career prospects after a PhD

The future PhD will develop a set of skills that can be applied in a wide range of professional environments. In particular, the following careers are targeted : researcher, PhD engineer, R&D engineer, in the public or private sector.

Références

[ACPKS23] J. Ayala-Cuevas, A. Perodou, A. Korniienko, and G. Scorletti. A frequency-domain Integral Quadratic Constraint approach to the analysis of Harmonically Time-Varying Systems. *Automatica*, 152 :110956, 2023.

[BTMS17] H. Ben-Talha, P. Massioni, and G. Scorletti. Robust Simulation of Continuous-Time Systems with Rational Dynamics. *International Journal of Robust and Nonlinear Control*, 27(16) :3097–3108, 2017.

[BTN01] A. Ben-Tal and A. Nemirovski. *Lectures on Modern Convex Optimization : Analysis, Algorithms, and Engineering Applications*. Society for Industrial and Applied Mathematics, 2001.

[BV04] S. P. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[CGK10] E. Colinet, D. Galayko, and A. Korniienko. Device for generating clock signals for asymmetric comparison of phase, 2010. United States Patent WO/2011/051407 (PCT/EP2010/066405).

[CK13] E. Colinet and A. Korniienko. Device and method for compensating a signal propagation delay, 2013. US Patent 8,373,476.

[CST19] M. S. Chong, H. Sandberg, and A. M. H. Teixeira. A Tutorial Introduction to Security and Privacy for Cyber-Physical Systems. In *2019 18th European Control Conference (ECC)*, pages 968–978, 2019.

[DPF+19] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty. A Systems and Control Perspective of CPS security. *Annual Reviews in Control*, 47 :394–411, 2019.

[EMSZ20] C. Escudero, P. Massioni, G. Scorletti, and E. Zamaï. Security of Control Systems : Prevention of Aging Attacks by means of Convex Robust Simulation Forecasts. *IFAC-PapersOnLine*, 53(2) :4452–4459, 2020.

[GFS11] A. Goelzer, V. Fromion, and G. Scorletti. Cell Design in Bacteria as a Convex Optimization Problem. *Automatica*, 47(6) :1210–1218, 2011.

[KSCB16] A. Korniienko, G. Scorletti, E. Colinet, and E. Blanco. Performance Control for Interconnection of Identical Systems : Application to PLL network design. *International Journal of Robust and Nonlinear Control*, 26 :3–27, 01 2016.

[LKD+17] K. Laib, A. Korniienko, M. Dinh, G. Scorletti, and F. Morel. Hierarchical Robust Performance Analysis of Uncertain Large Scale Systems. *IEEE Transactions on Automatic Control*, 63(7) :2075–2090, 2017.

[PCZ21a] A. Perodou, C. Combastel, and A. Zolghadri. Critical-Time Analysis of Cyber-Physical Systems subject to Actuator Attacks and Faults. In *2021 60th IEEE Conference on Decision and Control (CDC)*, pages 4188–4193, Dec. 2021.

[PCZ21b] A. Perodou, C. Combastel, and A. Zolghadri. Towards Anomaly-Tolerant Systems by Dissipation Block Synthesis. In *2021 5th International Conference on Control and Fault-Tolerant Systems (SysTol)*, pages 19–24, Sept. 2021.

[PKS+21] A. Perodou, A. Korniienko, G. Scorletti, M. Zarudniev, J. B. David, and I. O'Connor. Frequency Design of Lossless Passive Electronic Filters : A State-Space Formulation of the Direct Synthesis Approach. *IEEE Transactions on Circuits and Systems I : Regular Papers*, 68(1) :161–174, 2021.

[PKZ+17] M. Pelissier, A. Korniienko, M. Zarudniev, G. Scorletti, O. Mokrenko, E. Blanco, P. Villard, and G. Billiot. Phase-locked loop with multiple degrees of freedom and its design and fabrication method, March 2017. US Patent 9,602,114.

[PKZS23] A. Perodou, A. Korniienko, M. Zarudniev, and G. Scorletti. Frequency Synthesis of Interconnected Homogeneous LTI Systems. *IEEE Transactions on Automatic Control*, 2023.

[SAJ15] H. Sandberg, S. Amin, and K. H. Johansson. Cyberphysical Security in Networked Control Systems : An Introduction to the Issue. *IEEE Control Systems Magazine*, 35(1) :20–23, 2015.

[SRE+19] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, and J. Quevedo. Bibliographical Review on Cyber Attacks from a Control Oriented Perspective. *Annual Reviews in Control*, 48 :103–128, 2019.

[TSSJ15] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson. Secure Control Systems : A Quantitative Risk Management Approach. *IEEE Control Systems Magazine*, 35(1) :24–45, 2015.

[ZB15] Q. Zhu and T. Basar. Game-Theoretic Methods for Robustness, Security, and Resilience of Cyberphysical Control Systems : Games-in-Games Principle for Optimal Cross-Layer Resilient Control Systems. *IEEE Control Systems Magazine*, 35(1) :46–65, 2015.