Offre de stage : Cybersécurité des systèmes de contrôle-commande industriels – Développement de modèles déterministes et probabilistes pour la détection et le diagnostic de cyber-attaques dans les ICS

Référence	CYBERINSTITUTE-INT-19001
Description	Depuis le début du XIX^{e} siècle, les systèmes de contrôle-commande industriels, de l'anglais *Industrial Control Systems* (ICS), subissent des cyberattaques visant à dégrader leur production et/ou endommager les équipements industriels (moteurs électriques, vérins, ...). Depuis une décennie, la cybersécurité des ICS est devenue une priorité dans de nombreux secteurs critiques tels que la production et distribution d'énergie (électrique, gaz, ...), le transport, la défense, la santé et également les systèmes de production. Bien qu'aujourd'hui les ICS dans les systèmes de production soient organisés suivant une architecture centralisée unifiée définie dans les années 1980 par les travaux de Purdue University, ils tendent désormais vers une architecture décentralisée. Cette transformation, communément désignée par Industrie 4.0, vise à implanter des équipements dits « intelligents », en d'autres termes avec des capacités de prise de décision et de communication conduisant au développement de systèmes cyber-physiques (Cyber-Physical Systems, CPS) au travers de communications de type Internet of Things (IoT). Cette transformation conduit à une augmentation du nombre de vulnérabilités et d'attaques déjà présentes au sein des ICS et ouvre de nouvelles perspectives à la cybersécurité. L'équipe de recherche Gestion et Conduite des Systèmes de Production (GCSP), au sein du Laboratoire G-SCOP, se focalise sur la sécurité des ICS proche des équipements industriels en fondant ses approches sur la base de modèles physiques et de commande. Parmi les approches développées, l'approche S.A.F.E (Security Approach based on Filter Execution) développée dans le cadre d'un partenariat avec la DGA a donné lieu à des résultats particulièrement intéressants que nous souhaitons poursuivre selon l'axe de la modélisation de systèmes physiques à des fins de détection. Dans le cadre de ce stage pour le Grenoble Alpes Cybersecurity Institute, vous rejoindrez le laboratoire G-SCOP au sein de l'équipe de recherche travaillant sur les thématiques de la cybersécurité des ICS. Vous travaillerez sur un axe de recherche de travaux en cours (Escudero et al., 2018) concernant l'analyse et la modélisation de vulnérabilités d'équipements industriels à des fins de développements de mécanismes de détection et de diagnostic d'attaques visant à détruire tels équipements.
Prérequis	Le ou la candidat(e) doit avoir un profil de formation Bac+5 et pouvoir justifier de solides compétences en modélisation des systèmes physiques et de connaissances basiques sur le fonctionnement d'un ICS (automate programmable industriel, SCADA). Des connaissances en MatLab sont également appréciées à des fins de simulations des modèles développés. De plus, des capacités de communication orale et écrite sont nécessaires en français et en anglais. <u>Bibliographie</u> [1] Escudero, Sicard, Zamaï. Process-Aware Model based IDSs for Industrial Control Systems Cybersecurity: Approaches, Limits and Further Research. *IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA 2018)*, Sep 2018, Torino, Italy. [2] Sicard, Zamaï, Flaus. Critical States Distance Filter Based Approach for Detection and Blockage of Cyberattacks in Industrial Control Systems. In: *Sayed-Mouchaweh M.(eds). Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical Systems*, Springer, Cham, 2018 [3] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. The Cybersecurity Landscape in Industrial Control Systems. *Proceedings of the IEEE*. [4] Urbina, David I. et al. Limiting the Impact of Stealthy Attacks on Industrial Control Systems. *ACM Conference on Computer and Communications Security* (2016).

Encadrant(s)	Eric Zamaï, Cédric Escudero, Franck Sicard
Candidature	Envoyer CV, lettre de motivation avec recommandations de 2 référents (dont responsable de la formation), relevés de notes de M1 (obligatoire) et relevé de notes de M2 (si possible) à cyberalps-contact@univ-grenoble-alpes.fr Pour plus d'information sur le stage, contacter eric.zamai@grenoble-inp.fr
Localisation	Laboratoire G-SCOP
Date de début	Février 2019
Durée	5 à 6 mois
Gratification	Selon réglementation en vigueur (env. 560€/mois). Possibilité de prise en charge partielle des frais de transport.

financed by IDEX Université Grenoble Alpes