Soumission d'une présentation de fin de projet de recherche pour RESSI 2022

Nom du projet : PULSE - Cybersécurité des systèmes industriels **Porteur :** Vincent Cachard (CEA-Leti)

Consortium : CEA-Leti (porteur), Université Grenoble Alpes, Schneider Electric, et STMicroelectronics.

Organe de financement : IRT-Nanoelec (ANR-10-AIRT-05)[1]

Début et fin de projet : 2018 – 2021 **Plage de TRL :** TRL 4-5

Les systèmes de contrôle industriel (ICS) sont utilisés pour surveiller et contrôler des procédés physiques industriels. La cybersécurité des ICS est devenue un domaine de recherche à la croissance très rapide après l'attaque Stuxnet en 2010. Les conséquences des cyberattaques sur les ICS sont très coûteuses d'un point de vue économique mais aussi pour l'environnement et l'intégrité des citoyens. Cela a contraint les agences gouvernementales, les fabricants de matériel et les chercheurs à développer des mesures de cybersécurité. Cependant, la cybersécurité des ICS pose deux principaux verrous scientifiques et techniques : (i) les systèmes industriels sont un monde propriétaire ; (ii) l'impact d'une cyberattaque sur le procédé physique est très difficilement prédictible due à l'explosion combinatoire engendrée par le nombre d'états possibles.

Contributions : Pour pallier ces défis, le projet Cybersécurité des Systèmes Industriels lancé en 2018 dans le cadre de l'IRT Nanoelec / PULSE présente deux objectifs principaux. Le premier vise la mise en place d'un démonstrateur de système industriel afin de pouvoir conduire des tests de sécurité et des attaques sur ses sous-systèmes et valider des outils de cybersécurité. Le second objectif est le prototypage d'un dispositif électronique permettant de mettre en place des politiques de sécurité dans des systèmes industriels initialement non sécurisés. Les développements menés dans le cadre du projet ont conduit à sept communications scientifiques dans des conférences nationales, internationales et ouvrages de vulgarisation. Nous faisons ici un résumé des résultats du projet et donnons les perspectives sur les travaux futurs.

WonderICS : La plateforme WonderICS (présentée en Figure 1) est un environnement de co-simulation matériel-logiciel (Hardware-In-The-Loop) principalement dédié à la sensibilisation aux problèmes de cybersécurité dans les ICS et à l'expérimentation de solutions de sécurité innovantes. Régulièrement utilisée pour des démonstrations à des acteurs clés du domaine (plusieurs dizaines par an), la plateforme intègre et fait communiquer plusieurs composants pour assurer une représentation d'un système industriel à la fois réaliste, flexible et attaquable à de multiples niveaux :

- Une reproduction d'un système industriel comprenant plusieurs dispositifs industriels réels (automates programmables, disjoncteurs, relai de protection électrique, écran de visualisation, etc.). Ces équipements communiquent, d'une part, avec un logiciel de supervision permettant de piloter l'installation (SCADA) et, d'autre part, avec un simulateur de procédé physique. Ce simulateur permet d'opérer des cyberattaques sans risque des procédés industriels critiques. Trois scénarios sont actuellement implémentés au sein de la plateforme : (i) une centrale hydroélectrique, (ii) une usine impliquant des gaz dangereux et (iii) l'usine chimique basée sur le procédé Tennessee-Eastman. Ce simulateur est également connecté à une représentation en 2,5D du procédé physique choisi (tous deux développés dans le cadre du projet et présentés en Figure 2), afin d'exposer l'état réel du procédé (potentiellement différent de l'état visualisé sur l'écran de supervision lors d'attaques).
- Un poste opérateur vulnérable, basé sur une infrastructure de machines virtuelles, constituant la porte d'entrée pour des attaques invasives et pouvant être facilement restauré à l'identique.
- Un poste attaquant intégrant plusieurs cyberattaques développées dans le cadre du projet. Elles vont d'attaques simples et visuelles (clé USB corrompue, *ransomware*), à des attaques furtives de type *Advanced Persistance Threat* (*remote access trojan*, *phishing*, etc). Ces attaques peuvent conduire jusqu'au sabotage du procédé industriel, visible grâce aux diverses représentations.

[1] Ce travail a été financé par le programme national français Programme d'Investissements d'Avenir, IRT Nanoelec ANR-10-AIRT-05.

Figure 1. Plateforme WonderICS

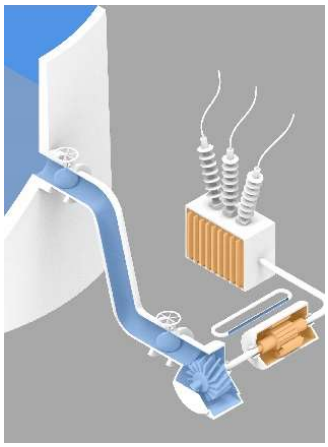

Figure 2. Exemple de vue 2,5D

Proxy de sécurisation : Le dispositif électronique développé vise à mettre en place un canal de communication sécurisé (à l'instar d'un VPN) entre plusieurs dispositifs industriels dits traditionnels (legacy). Parfois installés depuis plusieurs dizaines d'années, ces dispositifs , n'ont pas été conçus pour être sécurisés. Le proxy de sécurisation permet d'analyser et de chiffrer les communications émises sur un bus de terrain tout en respectant les contraintes de latence imposées par le procédé physique opéré. Par ailleurs, il offre des capacités similaires à celles d'un module matériel de sécurité (*Hardware Security Module*) et permet donc de mettre en place des fonctions cryptographiques dans des dispositifs industriels n'embarquant pas de sécurité. Enfin, une interface Bluetooth Low Energy, dite de commissioning facilite le déploiement de ces proxys dans les architectures industrielles en permettant la mise à jour et la configuration des fonctions de sécurité. A l'issue des développements, la maturité des proxys correspond à celle d'un prototype industriel (TRL 4 à 6). Ces développements ont abouti à la réalisation d'un démonstrateur portatif présenté au FIC 2020 (Figure 3). Ce démonstrateur illustre la possibilité d'attaques par injection de trames malicieuses sur la communication entre un automate et des relais de protection électrique via le protocole MODBUS/RTU. Les proxys de sécurisation viennent alors se placer en avant de chaque dispositif afin de chiffrer et signer les trames émises pour protéger les échanges de données.

Lors du prototypage et du développement, dans la perspective d'un transfert technologique, la sécurité intrinsèque des proxys de sécurisation a été prise en compte dans toutes les phases du cycle de développement. Une analyse de risque, intégrant 70 exigences de sécurité issues des normes IEC 62443 et IoT-SF ont permis d'atteindre un haut niveau de sécurité dans un environnement industriel. Par ailleurs, un banc de test incluant des outils d'intégration continue a permis de réaliser aussi bien des tests de sécurité que de non-régression tout au long des développements.

Figure 3. Démonstrateur présenté au FIC 2020