Cybersécurité de l'informatique industrielle et des objets connectés industriels (IIoT) : SystemX lance le projet IO4

Ce nouveau projet de R&D concourt au développement de la souveraineté numérique relative aux enjeux de cybersécurité pour l'Usine du Futur et l'Internet des Objets Industriels (IIoT). Ces travaux visent à lever les verrous existants pour proposer une architecture de déploiement de dispositifs IIoT sécurisée de bout en bout, qui tient compte des spécificités et contraintes imposées par le matériel. Ils seront validés par des tests physiques et numériques, notamment sur la plateforme d'expérimentation en cybersécurité CHESS, développée avec le soutien de l'ANSSI.

Palaiseau, le 23 août 2018 – SystemX, unique IRT dédié à l'ingénierie numérique des systèmes du futur, lance le projet IO4 (« Industrial IIoT 4 Secure Manufacturing ») qui vise à concevoir des approches innovantes en matière de cybersécurité pour l'IIoT et l'Usine du Futur. Rassemblant Assystem, CyberTestSystem, ENGIE, IOTify, Pertimm, SIGFOX et le CEA, le projet fédère des travaux académiques, des technologies émergentes et produits/solutions de sécurité en développement, autour d'une méthodologie qui repose sur les principes de co-création et d'expérimentation des usages de l'IIoT dans des environnements réels.

« La cybersécurité est un des enjeux majeurs de l'industrie du futur et de la ville numérique. Ces nouveaux systèmes reposent sur une utilisation massive des objets connectés, augmentant la surface d'attaque pour des acteurs malveillants. La sécurisation de ces sites nécessite tout d'abord une connaissance précise de l'environnement de déploiement mais également et surtout une bonne compréhension des nouvelles menaces. C'est là tout l'enjeu du projet IO4, lancé par SystemX dans la continuité des travaux menés dans le cadre du programme « Internet de Confiance », explique Reda Yaich, chef de projet IO4 chez SystemX.

Le projet IO4 en quelques mots

- **Programme :** Internet de Confiance
- **Durée** : 48 mois
- **Effort total** : 21 ETP

Partenaires industriels : Assystem, Cyber Test System, ENGIE, IoTify, Pertimm et SIGFOX
Partenaire académique : CEA

Objectifs du projet :
- développer, dans le cadre de l'Usine du Futur, une architecture de déploiement de dispositifs IIoT sécurisée pour garantir la collecte et la gestion des données de bout en bout
- proposer des mécanismes de gestion sécurisée du cycle de vie des dispositifs IIoT.

Deux cas d'usage :
- Usine du Futur
- Ville numérique

Le projet IO4 adresse les enjeux de cybersécurité de l'Usine du Futur et des objets industriels connectés. Il sert deux objectifs principaux :

- Développer une architecture de déploiement de dispositifs IIoT qui garantira la sécurisation de la collecte, la remontée et le stockage des données, tout en tenant compte des contraintes imposées par le matériel (autonomie, mémoire, bande passante, etc.)
- Proposer une architecture de sécurité intégrale couvrant chaque étape du cycle de vie des dispositifs IIoT (enrôlement, mise à jour, maintien en condition de sécurité, maintien en condition opérationnelle, etc.).

Deux cas d'usages

Le projet IO4 traitera les verrous scientifiques et technologiques de la cybersécurité appliquée à deux cas d'usage distincts :

- **Usine du Futur : Maintenance industrielle prédictive sécurisée.** Dans ce cas d'usage, le projet permettra à un fournisseur d'énergie d'anticiper les aléas et d'assurer la continuité du service grâce à la collecte sécurisée des données sur le terrain par les IIoT.
- **Ville Numérique : Maintien en condition de sécurité des IIoT en environnement Urbain.** Il s'agit dans ce cas d'usage d'adresser le besoin de maintien dans le temps du niveau de conformité avec les exigences de sécurité. Pour cela, il est impératif à la fois de sécuriser le processus permettant d'accéder à distance aux dispositifs IIoT pour leur mise à jour mais également de réduire le coût d'une telle opération (autonomie, communication, etc.).

Pour tester et valider l'ensemble des travaux de R&D et en faciliter le transfert technologique, le projet IO4 disposera de deux nouveaux environnements d'expérimentation :

- **Une infrastructure d'expérimentation et de validation grandeur nature** : la plateforme comportera 1000 dispositifs IIoT répartis sur différents sites industriels et urbains présents sur plusieurs continents.

- **Une « CyberRange »** de simulation avancée et de génération de trafics (12 000 IIoT) qui viendra enrichir **CHESS, plateforme d'intégration et d'expérimentation en cybersécurité** développée avec le soutien de l'ANSSI et sur laquelle l'IRT SystemX mutualise ses travaux (évaluation des performances, de la robustesse, du passage à l'échelle, etc.))

À propos de l'IRT SystemX

Basé sur le plateau de Paris-Saclay, l'IRT SystemX se positionne comme un accélérateur de la transformation numérique. Centrés sur l'ingénierie numérique des systèmes du futur, ses projets de recherche couvrent les enjeux scientifiques et technologiques des filières industrielles transport et mobilité, énergie, sécurité numérique et communications. Ils répondent aux défis que rencontrent les industriels dans les phases de conception, de modélisation, de simulation et d'expérimentation des produits et services futurs, intégrant de plus en plus de technologies numériques.

L'évolution des technologies et la nécessité de leur intégration impliquent en effet de tenir compte du nouveau paradigme « Digitalisation » par une approche « systèmes » voire « systèmes de systèmes ». La feuille de route 2016-2020 de l'IRT s'articule autour de 4 programmes : l'industrie agile, les transports autonomes, les territoires intelligents et l'internet de confiance. Aujourd'hui, SystemX, ce sont 31 projets lancés (dont 20 en cours), impliquant 83 partenaires industriels et 24 laboratoires académiques, et 265 collaborateurs dont 130 ressources propres.

Contacts presse
Marion Molina – Claire Flin
Tél. 06 29 11 52 08 / 06 95 41 95 90
marionmolinapro@gmail.com / clairefline@gmail.com