CYRUS

Plateforme de tests de cybersécurité pour systèmes cyber-physiques industriels

CYRUS est un projet de recherche industrielle dont l'objectif est de définir et développer un démonstrateur de plateforme de tests de cybersécurité pour des systèmes cyber-physiques industriels, avec une priorité marquée pour les systèmes critiques en termes de sûreté de fonctionnement.

Contexte et Objectifs

CYRUS est un projet de recherche industrielle dont l'objectif est de définir et développer un **démonstrateur de plateforme de tests de cybersécurité pour des systèmes cyber-physiques industriels**, avec une priorité marquée pour les systèmes critiques en termes de sûreté de fonctionnement. Le projet est motivé par la connectivité croissante (5G prochainement) de ces systèmes industriels, qui les rend plus vulnérables aux menaces de cyberattaques. Il prendra en compte l'**évolution du contexte régulatoire** (règlement européen Cybersecurity Act) **et normatif** en cybersécurité. Il constitue la première phase d'un projet ambitieux visant à développer et à mettre en place, en Wallonie, un laboratoire de tests en cybersécurité dédié à ce type de systèmes et ce dans une large gamme de domaines industriels.

Les systèmes cyber-physiques (Cyber Physical Systems ou CPS en anglais), en particulier industriels, présentent des **défis spécifiques en termes de cybersécurité par rapport aux systèmes IT traditionnels**, et ce en raison de leurs caractéristiques propres :

- combinaison de composants physiques, réseaux et logiciels inter-connectés,
- caractère distribué et hétérogène, d'un point de vue technologique et en termes de ressources disponibles, de ces composants, protocoles et technologies de communication divers (filaires, sans fil, parfois non standards/propriétaires)
- fonctionnement en temps réel avec des interactions sur le monde physique induisant des contraintes fortes en termes de sûreté de fonctionnement.

AGORIA Cenaero Multitel INNOVATION CENTRE LOGISTICS IN WALLONIA
European Digital Innovation Hub – WalHub Project 101083685
Co-funded by the European Union
sirris Ocetic Your Connection to ICT Research IDELUX PÔLE MECATECH Agence du Numérique
Avec le soutien de la Wallonie

En raison de ces caractéristiques, les méthodes de tests de cybersécurité pour les logiciels traditionnels ne peuvent pas être appliquées telles quelles aux CPS et doivent dès lors être significativement adaptées.

Le projet CYRUS vise, pour ce type de système, à **définir une procédure et une architecture de test de sécurité** ainsi que sélectionner, intégrer et mettre en œuvre des **outils de tests** appropriés pour cette architecture au sein d'un démonstrateur, en visant un framework outillé cohérent et productif, qui permette autant que possible l'automatisation et la répétabilité des activités de test. Le démonstrateur permettra la réalisation de plusieurs types de tests : **tests de sécurité fonctionnels, tests de fuzzing, tests de pénétration**. Il sera **validé sur trois études de cas de systèmes industriels connectés** fournis par les partenaires, dans des domaines d'application différents (cfr ci-dessous).

Le projet produira également des **recommandations** et une **roadmap** pour la suite des développements et l'évolution de ce laboratoire de test.

Partenariat et rôle du CETIC

La recherche sera effectuée par GUARDIS, le CETIC et UCLouvain sur base des besoins et cas d'étude fournis par ALSTOM (domaine ferroviaire), AISIN (domaine automobile) et ALX Systems (domaine des drones).

Le CETIC apporte son expertise en ingénierie logicielle et de sécurité, en particulier son expertise en tests logiciels, en développement de plateformes de génie logiciel et ses connaissances des normes de cybersécurité et du contexte de certification en évolution au niveau européen (projet SPARTA).

Le CETIC joue un rôle transverse dans ce projet : il participe à l'état de l'art, à l'élaboration de la plateforme et de la procédure globale de test et à la réalisation du démonstrateur. Il s'implique dans la dimension opérationnelle des tests pour les trois études de cas du projet. Il s'intéresse de près aux questions de recherche et aux défis scientifiques et techniques entourant ce projet.

Le CETIC avec GUARDIS souhaitent se positionner comme acteurs-clé en vue de l'**industrialisation du démonstrateur** et la création à terme du centre wallon de tests de cybersécurité pour CPS.

Valeur ajoutée par les entreprises wallonnes

Comme déjà expliqué plus haut, le projet CYRUS constitue la première phase d'un projet ambitieux visant à développer et à mettre en place, en Wallonie, un **laboratoire de test en cybersécurité pour les Systèmes Cyber-Physiques (CPS)** qui se développent et se déploient dans tous les domaines industriels.

Un **Advisory Board (Comité Consultatif)** sera constitué afin d'impliquer dans cette recherche d'autres acteurs wallons concernés par la problématique.

Ce projet s'inscrit par ailleurs dans la stratégie de la **plateforme d'innovation CPSET** dédiée aux Systèmes Cyber-Physiques dans les domaines de la conversion d'Énergie et du Transport. Cette plateforme a pour objectif de consolider et pérenniser un nouvel éco-système R&D en Wallonie centré sur les systèmes cyber-physiques et ce autour de plusieurs axes thématiques d'intérêt commun. Elle a été fondée mi-2018 par plusieurs grands industriels wallons (dont ALSTOM et AISIN) et 2 centres de recherche (dont le CETIC). Elle se veut ouverte, au-delà de ses membres fondateurs, aux acteurs wallons (industriels, centres de recherche, académiques) concernés par les systèmes cyber-physiques, en particulier aux PMEs. Elle vise entre autres à favoriser le dépôt de projets de recherche collaboratifs associant ces différents acteurs.

L'exploitation envisagée pour les résultats dépasse les frontières wallonnes. **Le marché visé est en effet international et multi-domaines** : l'ensemble des entreprises produisant ou utilisant des CPS ont des besoins croissants en test de cybersécurité. Les principales raisons sont la connectivité croissante de ces systèmes (avec bientôt la 5G aussi), le contexte régulatoire et normatif en pleine évolution sur la cybersécurité de ces systèmes (y compris en termes de certification) et aussi les demandes des clients de ces entreprises. De plus en plus, ces derniers formulent des exigences de sécurité au niveau des cahiers de charge telles que la compliance à ces nouvelles normes, la mise à disposition d'informations précises et de preuves sur le niveau de protection et le risque encouru par ces systèmes. Ils exigent aussi que des tests de cybersécurité soient réalisés par des organismes indépendants des fournisseurs de CPS afin de vérifier et assurer le niveau de protection des CPS proposés.