Évaluation de la cybersécurité de modèles prédéploiement de systèmes industriels

Record number : OPR-1325

Overview

RESEARCH DIRECTION

Pierre Martin Tardif, Directeur de département - Department of Information Systems and Quantitative Management Methods

INFORMATION

pierre-martin.tardif@usherbrooke.ca

RESEARCH CO-DIRECTION

Aref Meddeb, Directeur de département - Department of Electrical and Computer Engineering

INFORMATION

aref.meddeb@usherbrooke.ca

ADMINISTRATIVE UNIT(S)

École de gestion
Département des systèmes d'information et méthodes quantitatives de gestion
Faculté des sciences
Faculté de génie

LEVEL(S)

2e cycle
3e cycle

LOCATION(S)

Université de Sherbrooke, campus principal

Project Description

Dans le paysage technologique actuel, la cybersécurité des systèmes industriels devient une préoccupation majeure, notamment en raison de l'augmentation des cyberattaques visant les infrastructures critiques. Un projet de recherche innovant visant à évaluer la cybersécurité des modèles de systèmes industriels avant leur déploiement est une initiative cruciale pour anticiper et contrer ces menaces. À l'intersection de la cybersécurité, de l'intelligence artificielle (IA) et des systèmes de contrôle industriel (ICS), ce projet vise à développer une méthodologie robuste pour évaluer et renforcer la sécurité des systèmes industriels avant leur mise en oeuvre effective. Cette approche repose sur un environnement d'émulation, ou Cyber Range avec certains équipements physiques, dans lequel un ICS réel qui sera bientôt mis en production est déployé d'une façon anonymisée.Le coeur de ce projet utilise des techniques d'IA avancées pour simuler des cyberattaques dans un environnement d'émulation, reproduisant fidèlement les architectures des ICS ciblés tout en conservant les approches spécifiques (p.ex. recette de peinture) anonymes. Le projet utilise des modèles de menace basés sur l'IA pour identifier les vulnérabilités potentielles des systèmes de contrôle industriels et des réseaux de communication. Ces modèles de menace évoluent et s'adaptent aux nouvelles techniques d'attaque, garantissant ainsi une évaluation complète et actualisée de la sécurité.

Discipline(s) by sector

Sciences naturelles et génie

Génie informatique et génie logiciel, Informatique

Funding offered

To be discussed

Partner(s)

Centris Technologies, Productique Québec, NeverHack

The last update was on 22 June 2026. The University reserves the right to modify its projects without notice.