

Poste à pourvoir : Doctorat en Génie Électrique/Informatique

- **Titre :** Intelligence artificielle et jumeaux numériques pour la sécurité des systèmes de contrôle industriel
- **Lieu de travail :** Département de Génie Électrique et de Génie Informatique, Faculté de Génie, UdeS
- **Date de début :** Été 2025
- **Direction de recherche :** Prof Aref Meddeb
- **Organisme de financement :** CNC : *Consortium National pour la Cybersécurité*
- **Projets de recherche et développement** – Science / technologie relative à la protection des infrastructures critiques.
- **Financement :** Bourse de \$30 000 par année

Contexte

Dans le paysage technologique actuel, la cybersécurité des systèmes de contrôle industriels (ICS) devient une préoccupation majeure, notamment en raison de l'augmentation des cyberattaques visant les infrastructures critiques. Le projet de recherche vise à évaluer la cybersécurité des ICS en développant des solutions robustes permettant d'évaluer et renforcer la sécurité des ICS avant leur mise en œuvre 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 projet vise à utiliser l'IA pour étudier les cyberattaques dans un environnement d'émulation, reproduisant fidèlement les architectures des ICS ciblés, tout en conservant les approches spécifiques 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.

L'innovation de ce projet réside également dans son approche holistique de la cybersécurité, qui prend en compte non seulement les aspects techniques des ICS, mais aussi les facteurs humains et les politiques de sécurité. En intégrant des attaques variées, ce projet cherche à évaluer la résilience des systèmes face à un large éventail de vecteurs d'attaque. En outre, il propose des recommandations personnalisées pour renforcer les protocoles de sécurité, la formation des employés et les politiques de gestion de l'accès des partenaires au projet.

La collaboration avec l'industrie est également un aspect crucial de ce projet. En travaillant directement avec des entreprises actives dans divers secteurs industriels, la personne doctorante pourra affiner ses méthodes d'évaluation afin de refléter les défis spécifiques de chaque secteur. Cette approche collaborative garantit que les résultats du projet sont pertinents et applicables dans des contextes industriels réels.

Objectifs de recherche

1. Développer un outil basé sur l'IA et les jumeaux numériques pour simuler/émuler des environnements ICS.
2. Identifier des vulnérabilités inconnues : Nous visons à découvrir des vulnérabilités jusqu'alors inconnues dans les ICS testés. Grâce à l'utilisation avancée de techniques d'IA et de jumeaux numériques, nous pourrions simuler des attaques visant à révéler des faiblesses subtiles dans les logiciels et le matériel que des acteurs malveillants auraient pu exploiter.
3. Évaluer la résilience des ICS : Les simulations d'attaques seront utilisées pour évaluer la résilience des systèmes face à différents types de menaces, fournissant ainsi une mesure quantifiable de la robustesse des systèmes industriels. Cette évaluation devra aider les entreprises à comprendre les niveaux de risque associés à leurs infrastructures.

Quelques conseils :

- Vous présenter en quelques lignes (formation antérieure, vos champs d'intérêt)

- Envoyer votre curriculum vitae, vos relevés de notes et démontrer votre expérience de recherche
- Si vous avez contribué à des publications, envoyer un lien ou un document

Si vous avez besoin d'information complémentaire ou pour déposer votre candidature, faites parvenir un courriel à l'adresse aref.meddeb@usherbrooke.ca