Intelligence artificielle et industrie du futur

Grenoble mardi 5 et mercredi 6 février 2019

L'IA pour la détection d'intrusion pour les systèmes de commande industriel : apport et difficultés par rapport aux approches classiques

Jean-Marie FLAUS

Professeur, G-SCOP

46 avenue Félix Viallet, 38000 Grenoble

jean-marie.flaus@grenoble-inp.fr

Mots clés : Cybersécurité, Intrusion Detection System (IDS), Système cyber-physique, machine learning

Résumé :

La cybersécurité des installations industrielles est une question qui préoccupe fortement les pouvoirs publics. De nouvelles réglementations et guides ont été proposés ces dernières années pour mettre en place une démarche de défense en profondeur permettant de maîtriser le cyber-risque.

Dans le cadre de cette démarche, les systèmes de détection d'intrusion constituent un élément important. Ils ont pour objectif d'alerter en cas d'intrusion et toute la difficulté est d'avoir un bon taux de détection sauf pour autant générer de fausses alertes.

La plupart des approches de détection d'intrusion pour les systèmes industriels se distinguent des approches classiques par le fait qu'elles utilisent un modèle dynamique du système piloté, en boucle ouverte ou en boucle fermée. L'algorithme de détection d'appuie sur des techniques de détection d'anomalie, assez proches de celles utilisées depuis de nombreuses années en détection de fautes ou en diagnostic.

Cette présentation se propose de faire le lien entre la nouvelle problématique de la cybersécurité, les apports des idées du diagnostic et l'intérêt et les limites des méthodes d'apprentissage automatique.