MÉTHODOLOGIE DISTRIBUÉE DE DÉTECTION DES ATTAQUES CIBLANT LE PROCESSUS PHYSIQUE DANS LES SYSTÈMES DE CONTRÔLE-COMMANDE INDUSTRIELS

Estelle HOTELLIER Naval GROUP, Naval Cyber Laboratory – INRIA – LIG – Grenoble-INP – UGA
Franck SICARD Naval GROUP, Naval Cyber Laboratory
Julien FRANCQ Naval GROUP, Naval Cyber Laboratory
Stéphane MOCANU INRIA – LIG – Grenoble-INP – UGA

CONTEXTE

Modèle de Purdue

Niveau 4 et 5 : Gestion des ressources et Direction générale

Niveau 3 : MES – Pilotage de la production

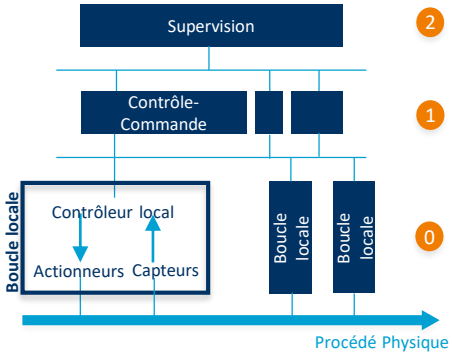
Niveau 2 : Système SCADA - Supervision

Niveau 1 : API (Automates Programmables Industriels)

Niveau 0 : Capteurs et actionneurs

ICS = entité ayant de larges surfaces d'attaque pouvant être exploitées par des attaquants

Typologie du système étudié



APPROCHE

IDS – Intrusion Detection System

- Approche comportementale
- Network IDS
- Attaques orientées procédé
- Localisation au niveau supervision - niveau 2 du modèle de Purdue

Challenges

- Détection distribuée dans un environnement temps réel
- Cohérence des données en entrée et sortie d'un équipement
- Normalisation des données des trames
- Observabilité partielle du trafic

Formalisme

- Automates finis, Réseaux de Pétri, Logique Temporelle (LTL, MTL et STL : Linear, Metric and Signal Temporal Logic), Réseaux Bayésiens, IA

ETUDE DE CAS [G-ICS Industrial Cybersecurity Lab]