Les défis posés par la sécurisation de l'I-IOT

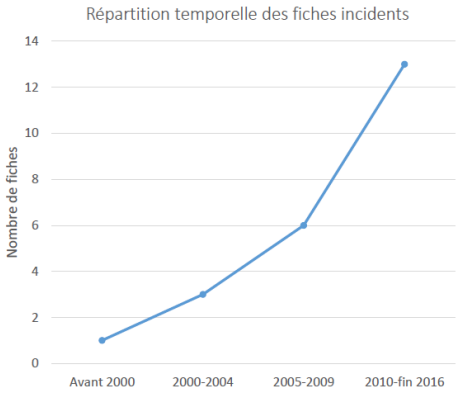
15/05/2019

Maxime Puys, CEA-Leti
Pierre-Henri Thevenon , CEA-Leti

Cybersecurity Institute
Univ. Grenoble Alpes

Contexte

- Augmentation croissante des incidents de sécurité dans les entreprises mondiales
- Complexité de sécurisation d'un système industriel
- Vuln. importantes des installations legacy ou non sécurisées
- Une majorité des attaques sur SO
- Réglementations française (LPM) et européenne (Cyberact) imposant:
  - Qualification des dispositifs et des installations
  - Transparence en termes d'attaques subies
- Prise en compte de la cybersécurité à différents niveaux:
  - Des normes de sécurité de plus en plus précises
  - Des fournisseurs de solutions
  - Forte progression des solutions de surveillance réseau

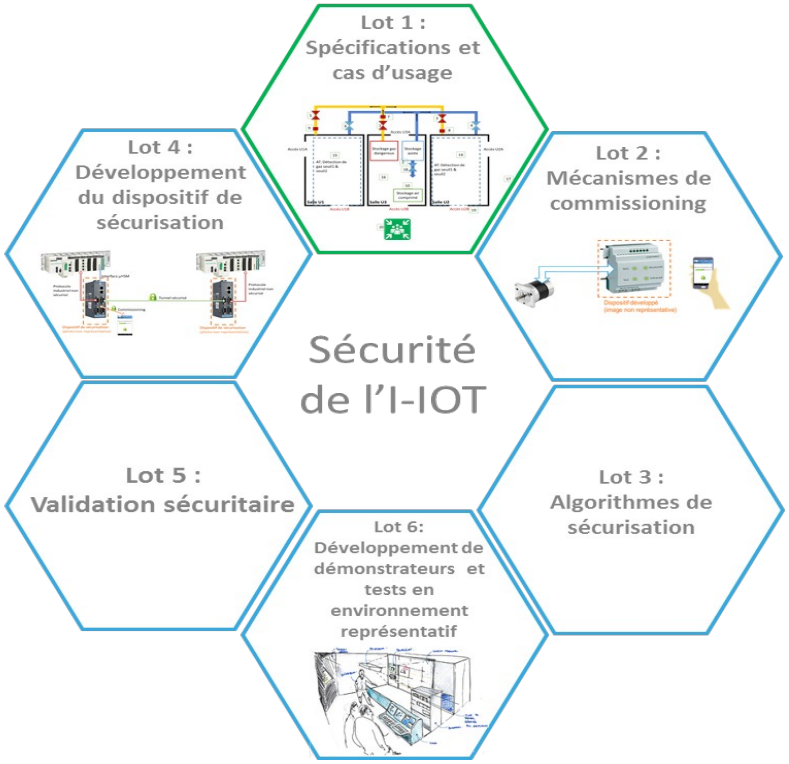


[Figure 1] Fiches Incidents Cyber SI Industriels, CLUSIF –Groupe de Travail SCADA, 2017
[Figure 2] Common Cybersecurity Vulnerabilities in Industrial Control Systems; Homeland Security,

Objectifs du projet

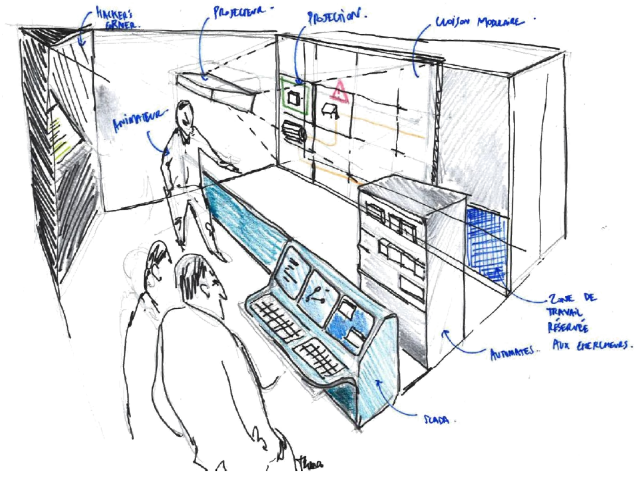
- Des partenaires académiques et industriels
  - CEA
  - Univ. Grenoble Alpes/ENSIMAG (VERIMAG, LIG, Institut Fourier)
  - Schneider Electrics, ST Microelectronics

- Sécurisation des systèmes et des installations industrielles legacy ou non sécurisées



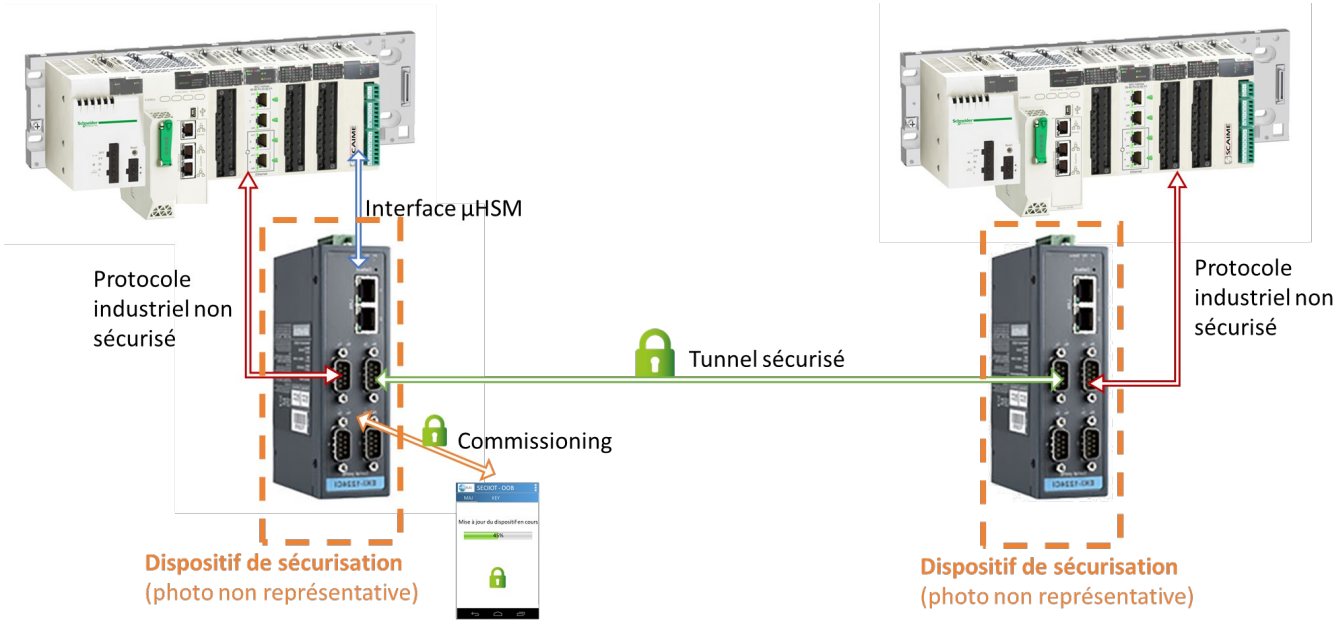
Plateforme de tests

- Objectifs de la plateforme:
  - Vitrine technologique pour l'IRT
    - Présentation de plusieurs scénarios d'usage
    - Présentation des faiblesses d'un système industriel en terme de cybersécurité
    - Présentation des solutions développées par l'IRT ou ces partenaires
  - Plateforme de tests
    - Mise en place d'attaques
    - Intégration de contre-mesures et autres solutions



Dispositif de sécurisation - objectifs

- Définition fonctionnelle du dispositif de sécurisation



- 3 fonctions principales:

Proxy de sécurisation
- Sécuriser l'interface de comm (MODBUS)
- Filtrage

Fonction µHSM
- Génération et stockage de clés
- Chiffrement et signature

Fonction commissioning
- Administration / config
- Mise à jour logicielle
- Provisioning de clé

Dispositif de sécurisation - verrous technologiques

- Travaux sur des bus de communication terrains non TCP/IP
  - Dispositif transparent
  - Contraintes temps réelles fortes (latence < 10 ms)
    - Optimisation à tous les niveaux tout en garantissant une sécurité importante du système

- Gestion du cycle de vie du dispositif
  - Interface de commissioning sécurisée
  - Gestion des droits pour les différents utilisateurs du système (prestataire de maintenance, intégrateur et fournisseur de solutions, exploitant, …)
  - Fin de vie (destruction clés, logs, etc)

- Prise en compte de la sécurité à tous les niveaux :
  - Protocoles de communication utilisés
  - Architecture HW/SW, composants utilisés
  - Tests de pénétration dans le cadre de l'intégration continue

Conclusion

- Début et fin du projet: Janvier 2018 – Décembre 2020

- Travaux en cours :
  - Implémentation et sécurisation du dispositif (briques fonctionnelles et composants de sécurité HW/SW)
  - Réalisation de la plateforme

- Etat de l'art :
  - Plusieurs travaux en lien [Cox ; Cardenas ; Chen ; Badrignan]
  - Plusieurs filtrent à postériori et utilisent du machine learning

- Nouveauté :
  - Positionnement sur bus de terrain (RS485)
  - Interface de commissioning

Maxime.Puys@cea.fr
Pierre-Henri.Thevenon@cea.fr

Merci de votre attention