THALES

Sécuriser la transformation numérique des industries

Quels enjeux ?

Jean-Marie Letort
VP Technology and Cybersecurity Consulting
Thales

Transformation numérique ? Non, Révolution industrielle ! (1/2)

Une très forte montée en puissance des technologies numériques au sein du secteur industriel

Des technologies désormais incontournables

- IIoT (Industrial Internet of Things)
- Big Data Analytics
- Cloud Computing & SaaS

Etre capable de mesurer factuellement la performance des processus industriels critiques

THALES

Transformation numérique ? Non, Révolution industrielle ! (2/2)

4 principales familles de bénéfices pour les industriels

- Optimisation des processus de gestion
- Maîtrise / Réduction des coûts de production
- Nouveaux produits et services
- Nouveaux modèles économiques

- Passer à un modèle d'offre de services à la demande vs vente de produits
- Modèle économique de souscription
- Enjeu de réactivité et disponibilité et d'engagement (SLA)

THALES

Quelques exemples de transformation numérique d'acteurs industriels

ENERGIE

- Programme « Engie Digital »

AUTOMOBILE / EQUIPEMENTIER

- Déploiement d'IIoT et de solution de Smart data Analytics pour optimiser les coûts logistiques, et offrir de la maintenance préventive
- Voiture autonome et « car sharing » (GM / Maven)

ESPACE

- Solution de Réalité Virtuelle Augmentée pour Thales Alenia Space

THALES

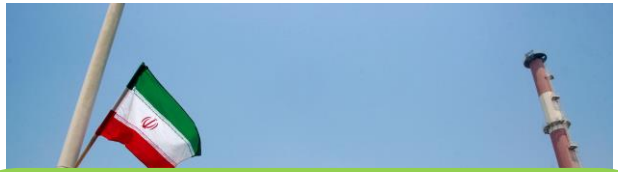
« Industrie 4.0 » rime aussi avec exposition à de nouveaux risques

De nouvelles vulnérabilités dues au « tout connecté », en particulier via…

- … l'objet connecté industriel : nativement peu sécurisé (arbitrage compétitivité / sécurité)
- … la collecte, le transport et le stockage des données

Des exemple notables de cyberattaques industrielles

- Stuxnet 2010 – Attaque sur une centrale nucléaire iranienne
- Black Energy 2015 - Coupure d'électricité en Ukraine



Les principales menaces :

- **Cyber espionnage** : vol de secrets industriels et de données confidentielles (IP, données de production, etc.)
- **Corruption de données et Cyber sabotage** d'un outil industriel (prise de contrôle ou corruption du fonctionnement)

THALES

Comment cybersécuriser l'innovation digitale dans l'industrie ?

Corriger

- **Travailler sur le parc existant** (recherche de vulnérabilités / mesures d'impacts) : **secured by service**

Superviser

- Mettre en place des **centres opérationnels de cybersécurité (CSOC) pour les OT** en extension de ce qui existe pour les SI critiques

Anticiper

- Prévoir le futur en intégrant la cybersécurité dès la conception : **secured by design**
- Travailler avec les constructeurs de SCADA, capteurs, etc. sur les roadmaps du futur

Se préparer

- **Plan de Continuité d'Activité - Offre de Cyber-résilience**

THALES

Protéger les assets les plus critiques : les données, or noir du XXIème siècle

Protéger la donnée tout au long de son cheminement, du capteur au datalake

- Acquisition de la donnée par IIOT : sécuriser les accès et durcissement software et hardware
- Transport de la donnée vers le datalake : authentifier et chiffrer les connexions
- Stockage de la donnée dans un datalake : sécuriser l'accès aux données, voire à chaque donnée

Garantir la protection et l'intégrité des données est vital pour le succès de l'industrie 4.0

THALES

Cybersécurité et innovation technologique maitrisée, les clefs de voûte de la transformation numérique des industries

- Etre conscient des risques et des obligations (LPM, RGPD)
- Mettre en place des solutions permettant de « dérisquer l'innovation technologique »
- Associer un acteur industriel de la cybersécurité tout au long du programme de transformation numérique

Le rôle de la cybersécurité : rendre possible la transformation digitale des industriels

THALES