CYBERSÉCURITÉ INDUSTRIELLE

Yann Cochard

CLERMONT’ECH - API Hour #40

2019-01-15

Sécurité ? Sûreté ? Cybersécurité ?

Sécurité : consiste à prévenir contre tout ce qui concerne les accidents, donc par définition **involontaire** (ex : sécurité routière).

Sûreté : consiste à prévenir tout ce qui est actes **volontaires**.

Cybersécurité : (Sécurité de l'information / SSI)

- Disponibilité
- Intégrité
- Confidentialité

} **des données**

/!\ faux amis en anglais :

- safety = sécurité
- security = sûreté
- cybersecurity = ~~sûreté numérique~~ cybersécurité ¯_(ツ)_/¯

Industrie

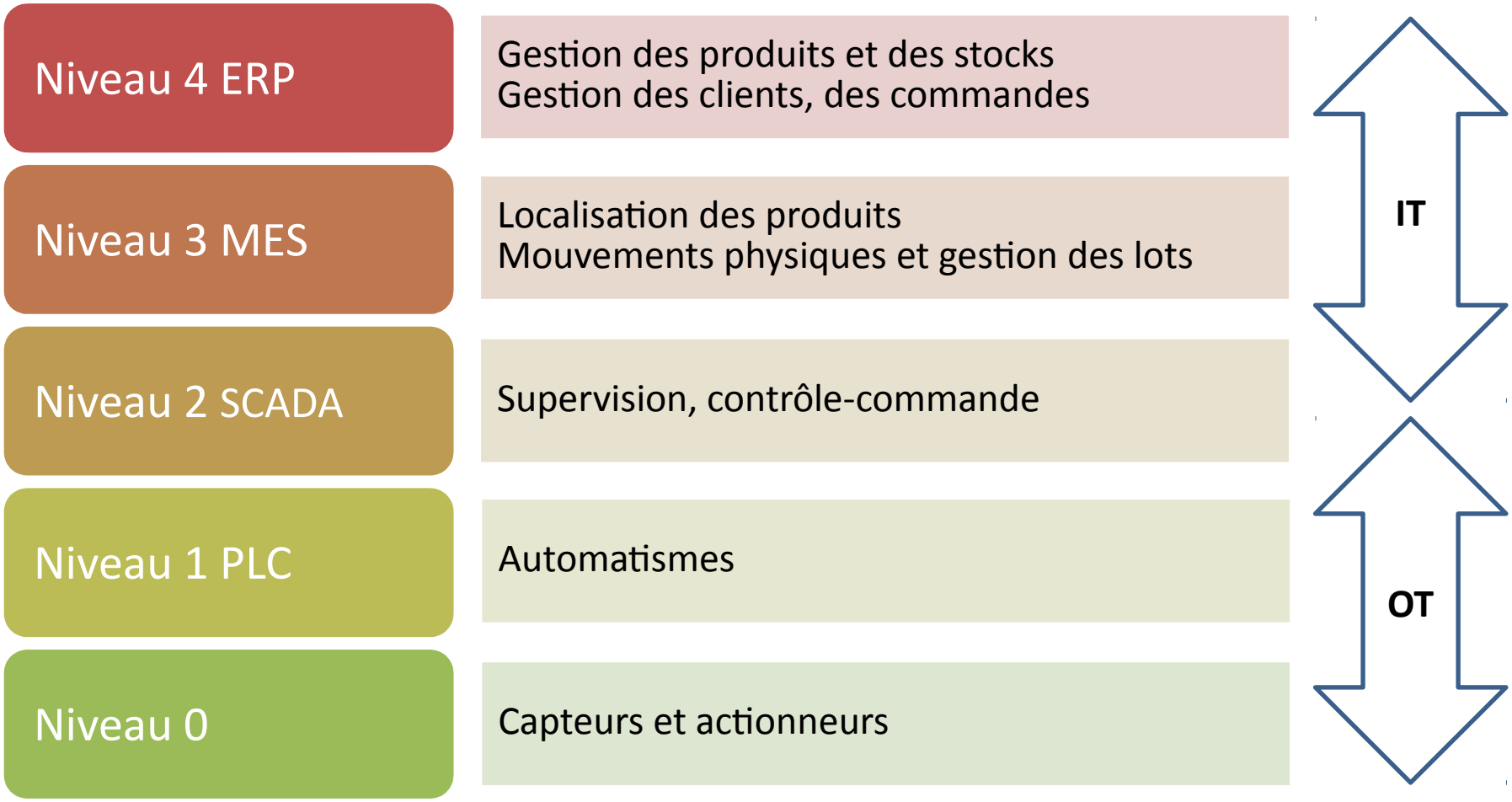
Eau
Énergie
Production
Transport
Agroalimentaire
etc

Machines
Centrales
Barrages
Aiguillages
Vannes
etc

Tout ce qui agit sur notre environnement, le physique

Architecture

(PERA - Purdue Enterprise Reference Architecture)



IT = Information Technology - OT = Operational Technology

Informatique industrielle : IT vs OT

OT

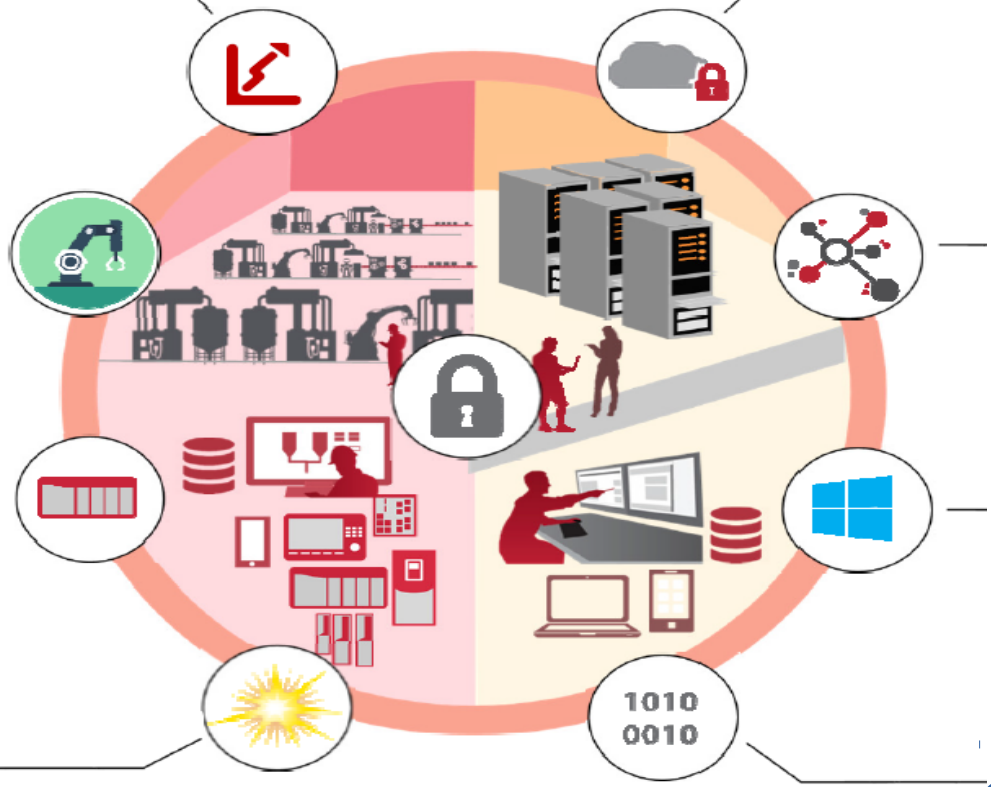
Operationnal Technology

Priorité : fiabilité et intégrité du système. Haute disponibilité.

Architectures propriétaires et dédiées à une tâche spécifique. Systèmes isolés.

Interfaces hétérogènes, spécifiques, à longue durée de vie

Production physique



IT

Information Technology

Priorité : disponibilité et confidentialité des données.

Architectures omniprésentes, sur plusieurs niveaux (tiers) pour une large accessibilité

Interfaces homogènes, à usages multiples et courte durée de vie

Production numérique

Un peu d'histoire - attaques ciblées

STUXNET (2010)
Impact : centrifugeuses du programme nucléaire iranien.
Usage de 4 failles 0-day. Automates Siemens.

HAVEX (2013, EnergeticBear / Dragonfly)
Spearphishing. Espionnage, aucun impact.
Scan OPC (Siemens, Rockwell). Espionnage (US, EU).

BLACKENERGY 2 (déc 2015 - Sandworm team)
Espionnage, impact 700 000 foyers coupés en Ukraine.
Fichier ms-office avec macros.

CRASHOVERRIDE/Industroyer (déc 2016)
1er malware dédié à l'attaque de réseaux électriques.
Décembre 2016 : Kiev (Ukraine) : impact = plus de 225 000 foyers sans électricité.

Un peu d’histoire - attaques « aveugles »

Dégâts collatéraux par des ransomwares.

WANNACRY (2017)

- Cyberattaque mondiale. Renault.

NOTPETYA (2017)

- Saint-Gobain (220 M€).
- Merck (500 M$ à 1 Md$) / 6 mois pour redémarrer.

=> Prise de conscience

Protection

Cloisonner et filtrer les réseaux industriels

Installer les mises à jours

Former les personnes

Renforcer les systèmes (hardening)

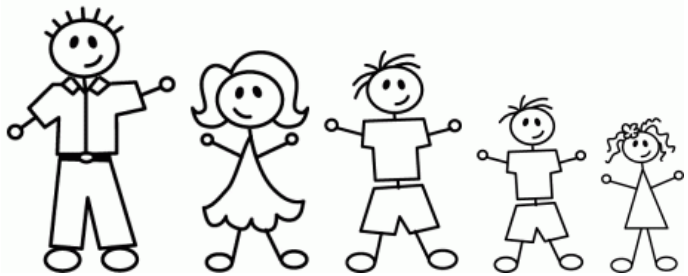
Renforcer les contrôles d’accès

Mettre en place de systèmes de détection

Inventaire par analyse réseau passive

Merci

Kaella



IFMA

yanncochard.com