Cybersécurité industrielle : d'un monde cloisonné vers l'industrie 4.0 : état des lieux d'un monde qui se révolutionne

Loïs Samain - Responsable de la Sécurité des Systèmes d'Information (RSSI) Groupe Adjoint – EDF Renouvelables

19/11/2019 @Mine2Rien

Qui suis-je ?

RSSI adjoint du groupe EDF Renouvelables & Membre du CESIN

Cette présentation représente **ma propre vision de la cybersécurité industrielle aujourd'hui**.
Les opinions exprimées ici sont **uniquement personnelles**.

Le Système d'Information Industriel

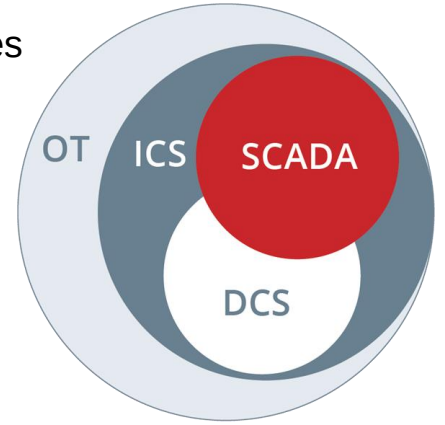
Qu’est ce qu’un système industriel ?

Selon l’**ANSSI** (*Agence Nationale de la Sécurité des Systèmes d’Information*) :

Un **système automatisé de contrôle des procédés industriels** (ou, plus brièvement, système industriel) désigne un ensemble de **moyens humains et matériels ayant pour finalité de contrôler** ou **commander des installations techniques** (composées d’un **ensemble de capteurs et d’actionneurs**)

Différentes définitions dans le monde du SI Industriel

- **OT** (*Operational Technology*) : englobe les systèmes informatiques qui gèrent les opérations industrielles. Cela comprend la surveillance du pétrole et du gaz, du réseau des services publics d'électricité, des activités de fabrication, etc. En opposition direct avec l'IT.

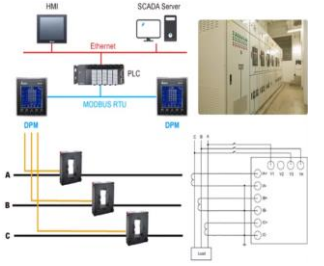


- **ICS** (*Industrial Control System*) : systèmes contrôlés par ordinateur qui surveillent et contrôlent les processus industriels qui existent dans le monde physique. Englobe le SCADA & DCS.

- **PLC** (*Programmable Logic Controller*) : dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. Les automates programmables sont programmés dans un langage spécialisé qui imite la logique de relais et fournit également des fonctions de contrôle automatisé pour gérer la pression, le débit, la température, le contrôle du mouvement et toutes les variables de processus.

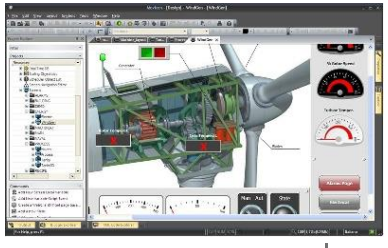
Différentes définitions dans le monde du SI Industriel

- **SCADA** (*Supervisory Control and Data Acquisition*) : logiciel utilisé pour surveiller les équipements de processus à l'aide de PLC / DCS et de tout autre automate. L'objectif principal du SCADA est l'acquisition de données : les réseaux se composent de plusieurs unités de terminaux distants (RTU) qui sont utilisées pour collecter les données au centre de commande central, où elles peuvent être utilisées pour prendre des décisions de haut niveau. Un système SCADA est piloté par les événements et est orienté pour la collecte de données.

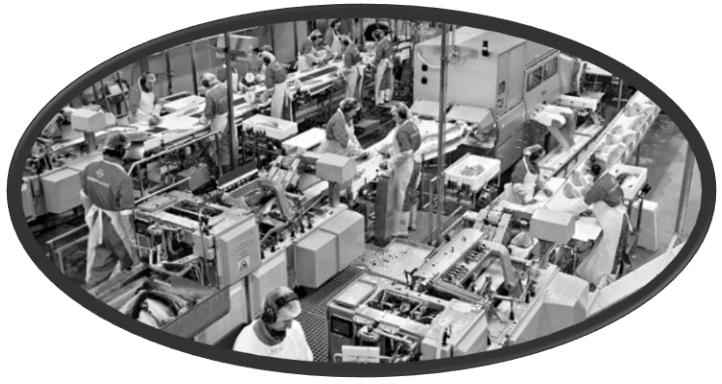


- **DCS** (*Distributed Control System*) : système de contrôle informatisé qui est réparti en niveaux de contrôle. DCS contrôle le paramètre du processus en envoyant le signal à l'actionneur de l'usine, à la vanne de régulation, à l'électrovanne et à de nombreux autres équipements de contrôle. Un DCS est piloté par l'état et est orienté par les processus.

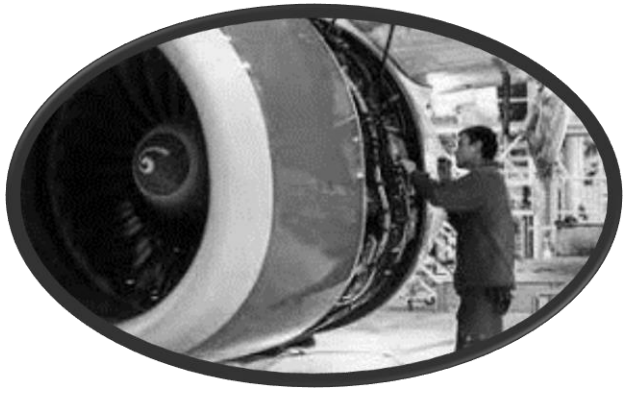
- **IHM** (*Interface Homme-Machine*): interface entre le process et les opérateurs – par essence même le tableau de bord des opérateurs. C'est le principal outil au travers duquel les opérateurs et superviseurs de lignes coordonnent et supervisent les processus industriels et manufacturiers dans les usines. L'affichage à proximité de l'information opérationnelle en temps réel est le domaine de l'IHM.

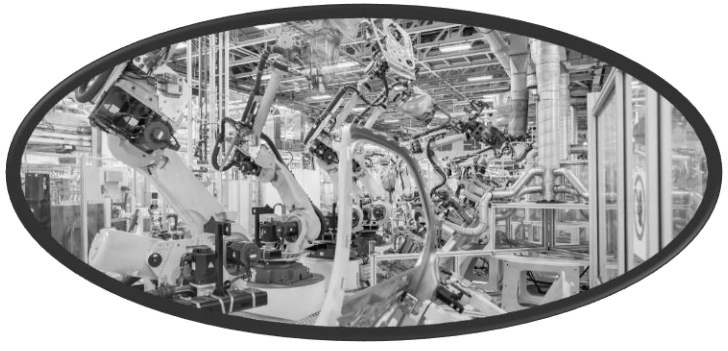


Ou trouve-t-on ces systèmes industriels ?



Partout…



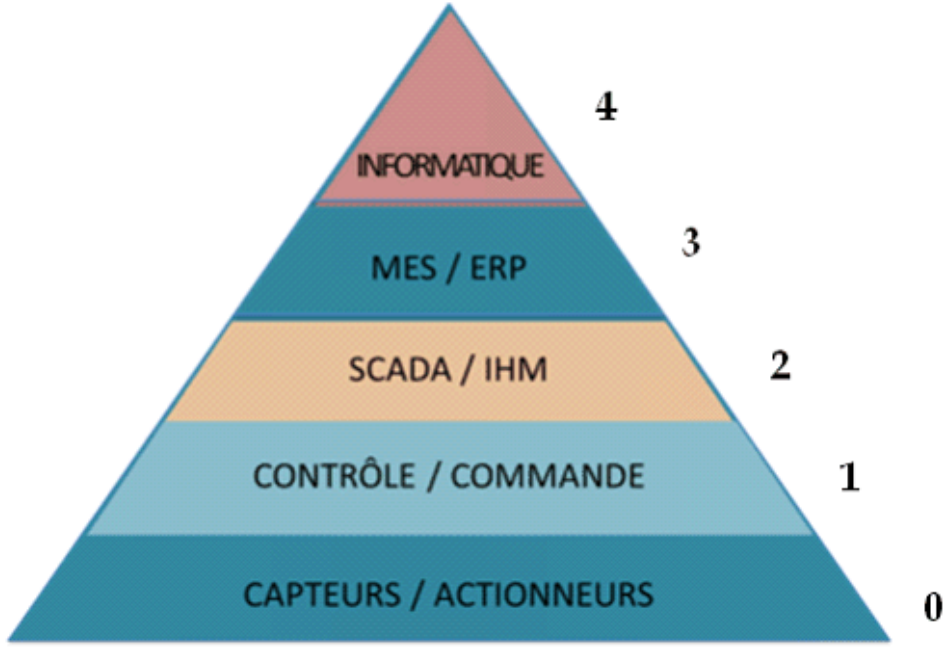


Une évolution des systèmes d'information industriels … et des risques

On peut observer différentes évolutions technologiques sur les SI Industriels :

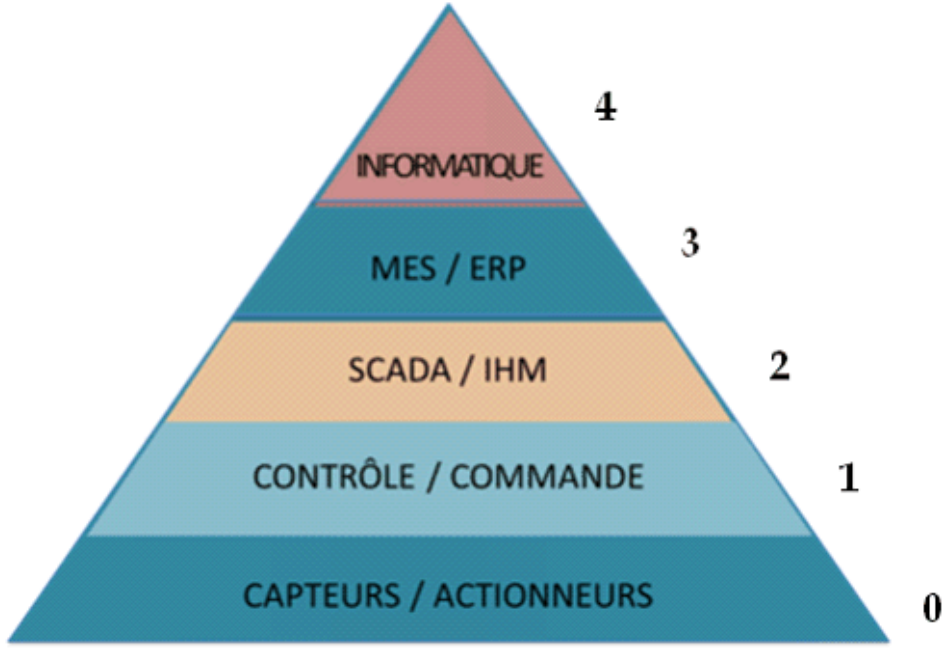
- Apparition des **signaux électriques** entre les actionneurs & les PLC (uniquement par contrôle pneumatique avant) ;
- Apparition des **DCS** & des **IHM** permettant de **contrôler et communiquer** avec les systèmes industriels de manière **non manuelle ;**
- Apparition des systèmes de supervision **en local** des systèmes industriels et **interconnexion avec le SI de l'Entreprise ;**
- Apparition des systèmes de supervision déportés **hors du SI de l'Entreprise** (télémaintenance par exemple).

Modèle d'architecture d'un système industriel

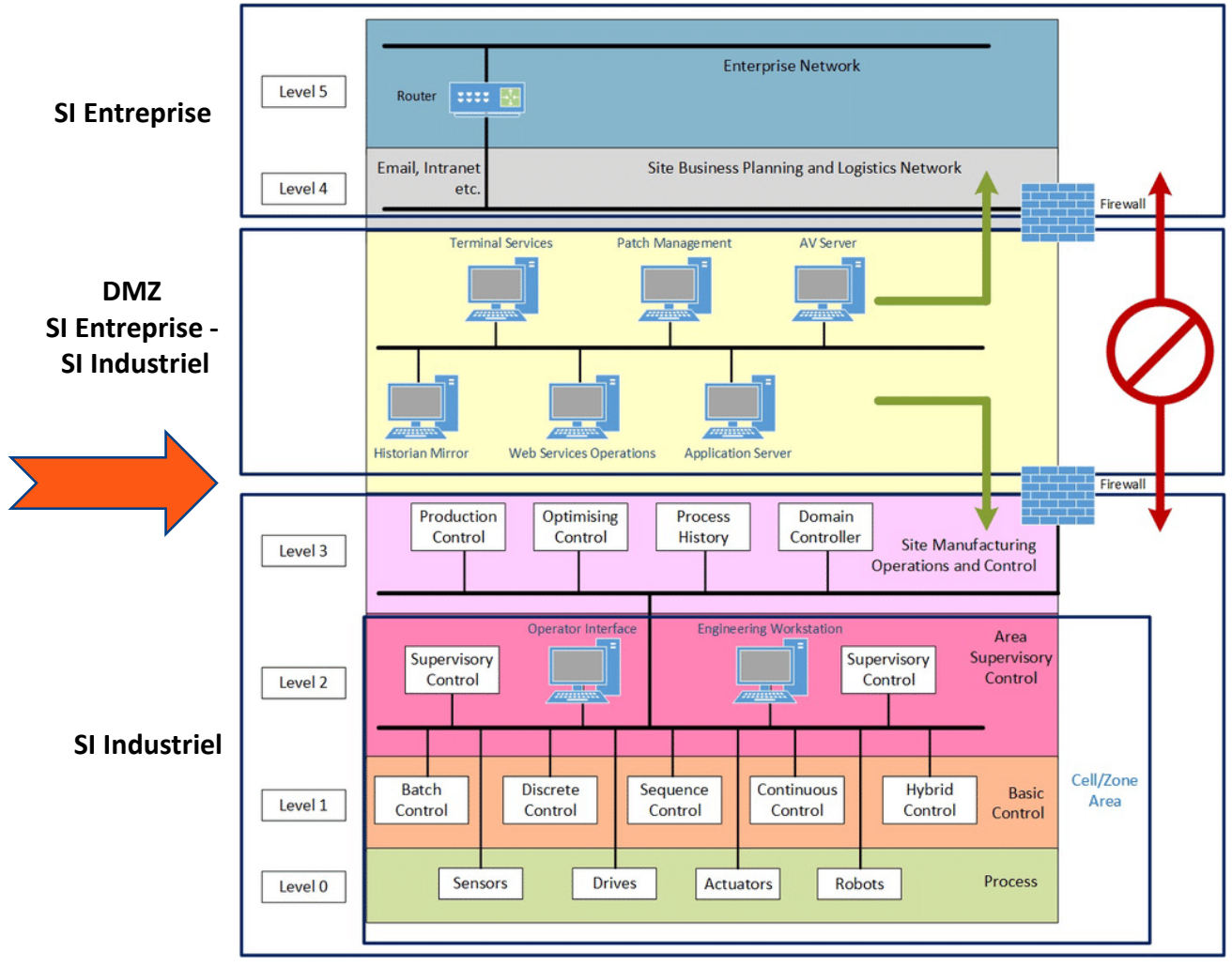


Modèle de référence CIM des processus industriels en vue de leur automatisation

Modèle d'architecture d'un système industriel



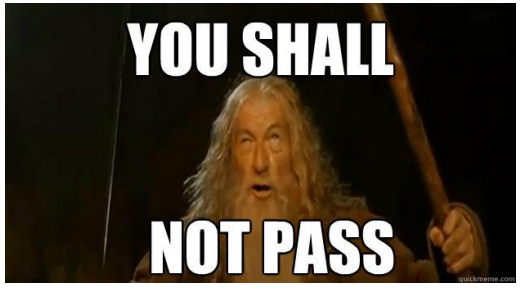
Modèle de référence CIM des processus industriels en vue de leur automatisation



Purdue Model – ISA-99.03.03 (IEC 62443)

Cloisonnement des réseaux industriels – de la théorie à la réalité du terrain

- Des interconnexions entre le SI Industriel et le SI de l'Entreprise difficile à couper avec **des flux traversants la DMZ** (partage des données des historian, CCTV, accès à des pages Internet légitimes, etc.)
- Une évolution de l'architecture qui peut être **complexe** à mettre en place (couts trop importante, refus du changement, etc.)
- Difficultés de la prise en compte du **cloisonnement horizontal** : risques de propagation entre zones de même niveau (l'interconnexion entre les différents sites industriels par exemple)
- De plus en plus de **flux externes nécessaires pour le business** : de plus en plus de métiers sur le SI de l'Entreprise ont besoin d'avoir accès à des données, télémaintenance



Quelques différences par rapport au SI de l'Entreprise

- **Des systèmes avec de longues durées de vie**
  - Des durées de vie en plusieurs dizaines d'années pour les systèmes industriels
  - Fin de support de ces systèmes (OS, drivers, etc.)
  - Maintien en Condition de Sécurité qui peut aller jusqu'au cout de rachat complet (SCADA)
  - Hétérogénéité des parcs (modèles & technologies différentes)

Quelques différences par rapport au SI de l'Entreprise

- **Des systèmes avec de longues durées de vie**

- **Des correctifs difficilement applicables**
  - Déploiement des correctifs durant les périodes de maintenance définies (où vous n'êtes pas la priorité)
  - Redémarrage pour application des patchs parfois impossible
  - Des infrastructures parfois difficilement accessibles physiquement et avec un faible débit

Quelques différences par rapport au SI de l'Entreprise

- **Des systèmes avec de longues durées de vie**
- **Des correctifs difficilement applicables**

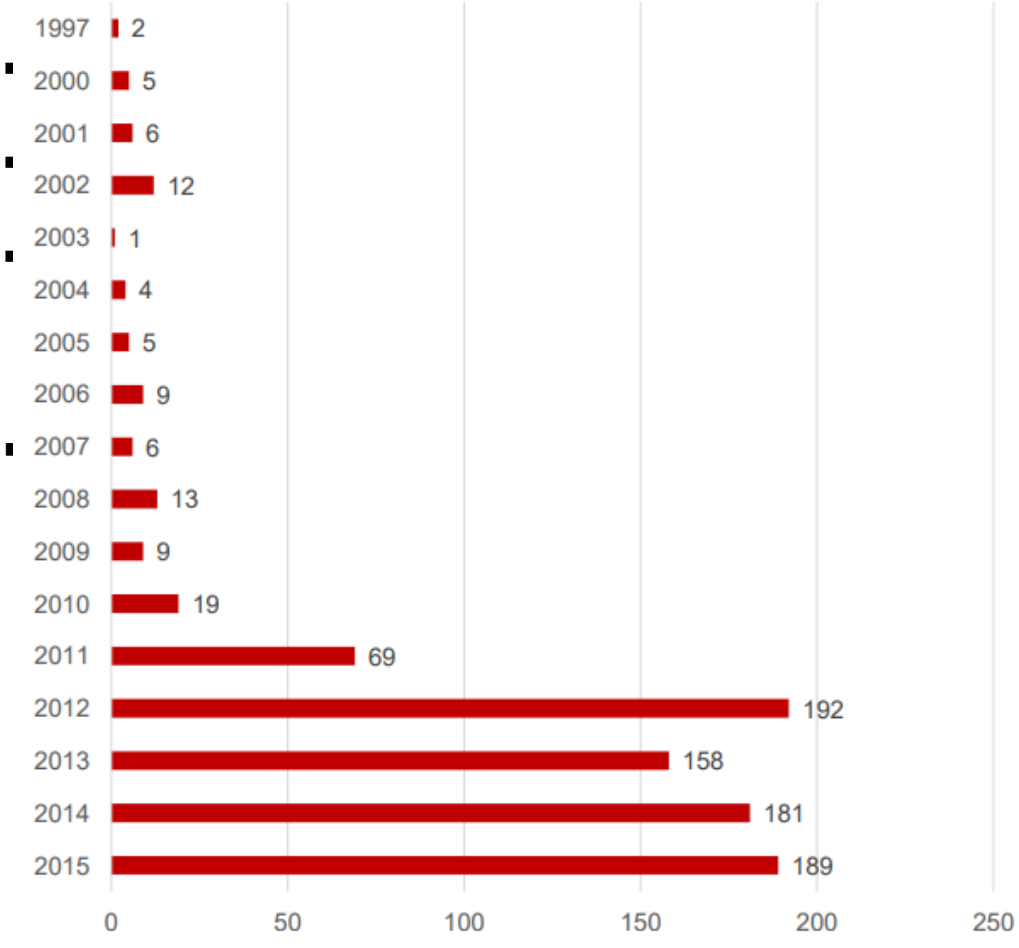
- **Des systèmes qui ne sont pas prévus pour échanger avec l'extérieur du SI Industriel**
  - Télémaintenance, accès à distance, etc. sont de plus en plus demandés par les fournisseurs
  - Même l'Entreprise a besoin de plus en plus de données venant de ces systèmes industriels (Cloud, Datalake, etc.) : le contenu des données industrielles est de plus en plus important dans la stratégie de l'Entreprise

Quelques différences par rapport au SI de l'Entreprise

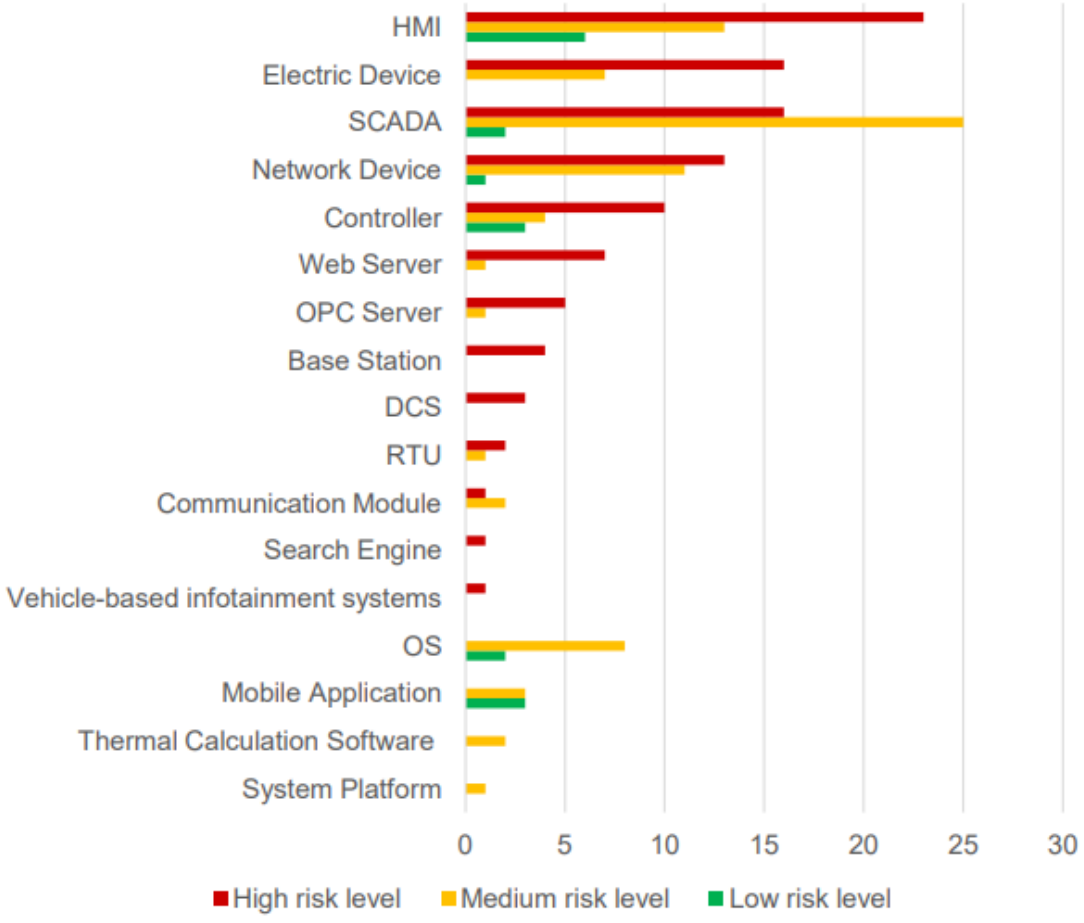
- **Des systèmes avec de longues durées de vie**
- **Des correctifs difficilement applicables**
- **Des systèmes qui ne sont pas prévus pour échanger avec l'extérieur du SI Industriel**

- **La cybersécurité n'a pas beaucoup été pris en compte sur ces systèmes**
  - Gérer l'existant où la sécurité n'a jamais été prise en compte
  - Apparition de la technologie IP en remplacement du série qui amène de nouvelles problématiques

Quelques différences par rapport au SI de l'Entreprise



Vulnérabilités ICS par année
Source : Kaspersky



Nombre de vulnérabilités ICS par type
Source : Kaspersky

Quelques différences par rapport au SI de l'Entreprise

- **Des systèmes avec de longues durées de vie**
- **Des correctifs difficilement applicables**
- **Des systèmes qui ne sont pas prévus pour échanger avec l'extérieur du SI Industriel**
- **La cybersécurité n'a pas beaucoup été pris en compte sur ces systèmes**

- **Les critères de sécurité DICT qui n'ont pas la même hiérarchie**
  - La **C**onfidentialité n'est pas le critère de sécurité n°1
  - La **D**isponibilité est le critère essentiel au sein des SI Industriels, suivi par l'**I**ntégrité

Quelques différences par rapport au SI de l'Entreprise

- **Des systèmes avec de longues durées de vie**
- **Des correctifs difficilement applicables**
- **Des systèmes qui ne sont pas prévus pour échanger avec l'extérieur du SI Industriel**
- **La cybersécurité n'a pas beaucoup été pris en compte sur ces systèmes**
- **Les critères de sécurité DICT qui n'ont pas la même hiérarchie**

- **Des impacts suite à une compromission souvent bien supérieurs à ceux du SI de l'Entreprise**
  - ➢ Un incident sur le SI industriel peut avoir des conséquences directes et fatales sur les hommes et l'environnement !

La cybersécurité industrielle

Des SI Industriels non cloisonnés : des impacts lors de cyberattaques sur le SI de l'Entreprise

- Mai 2017 : **Renault** (Wannacry) : chaines de production paralysées en Europe suite à la contamination de Renault pendant un week end

- Fin juin 2017 : **Saint Gobain** (NotPetya) : contamination par ransomware du SI de Gestion & SI Industriel avec un impact financier qui approche les 250 millions d'euros sur ses ventes et 80 millions d'euros sur son résultat d'exploitation

- Mars 2019 : **Norsk Hydro** (LockerGoga) : chaines de production paralysées dans le monde avec un impact financier de 40 millions de dollars en perte de revenue et des coûts de services informatiques supplémentaires pour la remise en marche du SI pendant deux semaines

Focus sur des cyberattaques qui ont fait prendre conscience du sujet

Le premier qui a fait bougé les choses : **STUXNET**

- Avant 2010, « impossible d'avoir des attaques SCADA » - « FUD »
- En Juin 2010, découverte par un éditeur biélorusse d'antivirus VirusBlokAda(VBA32) travaillant avec l'Iran
    - Cible les équipements SIEMENS
        - Automate PLC et IHM
            - WinCC Simatic & Step 7
            - MC7
        - 4 zero days ont été découvertes dans l'analyse
        - Mots de passe hardcodés dans les systèmes

- Environ 1000 centrifugeuses d'enrichissement en Uranium détruites => impact sur le programme d'enrichissement nucléaire iranien situé à Natanz
- **Un véritable avant/après dans la prise en compte du risque cyber sur les systèmes industriels**

Focus sur des cyberattaques qui ont fait prendre conscience du sujet

Un impact visible et durable : **BlackEnergy**

- Fin décembre 2015 : cyberattaque du réseau électrique de Prykarpattya Oblenergo (Ukraine)

  sur 3 centres de distribution électrique en simultanée (environ 50 sous-stations électriques)

  - Tout a commencé par la compromission du SI de Gestion à travers une campagne de phishing avec un Word compromis (ces joyeuses macros).
  - Compromission de l'Active Directory et modification des credentials pour des collaborateurs ayant des comptes VPN pour gérer à distance des SCADA
  - Reprogrammation des UPS et des systèmes industriels
  - Désactivation des sous-stations électriques avec en parallèle du TDoS sur les call-center
  - Destruction du MBR et système à travers le malware *KillDisk* sur les postes opérateurs

- **Impact : pas d'électricité pour 1,4 millions d'habitants (environ 250.000 foyers) dans l'ouest de l'Ukraine durant 3 à 6 heures**

Focus sur des cyberattaques qui ont fait prendre conscience du sujet

La première cyberattaque sur les systèmes instrumentés de sureté (SIS): **Triton**

- Fin d'année 2017 : découverte d'une cyberattaque sur le SIS Triconex de Schneider Electric en Arabie Saoudite
  - SIS ? Système visant à mettre un procédé en position de repli de sécurité (c'est-à-dire un état stable ne présentant pas de risque pour l'environnement et les personnes), lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement
  - Contamination d'un poste opérateur permettant le contrôle et la programmation des automates du SIS
  - Exploitation d'une vulnérabilité zero-day sur le SIS pour écrire dans la zone mémoire système et réécrire les automates avec déploiement d'un RAT pour garder le contrôle à distance
  - Plusieurs arrêts du processus industriel du SIS dû (surement) à des erreurs des attaquants qui mettent la puce à l'oreille aux exploitants
- **Impact : Sabotage et endommagement des systèmes. Un niveau au dessus de Stuxnet : Triton permet une communication totale et à distance entre l'attaquant et les automates du système instrumenté de sureté**

Point de situation de la cybersécurité industrielle

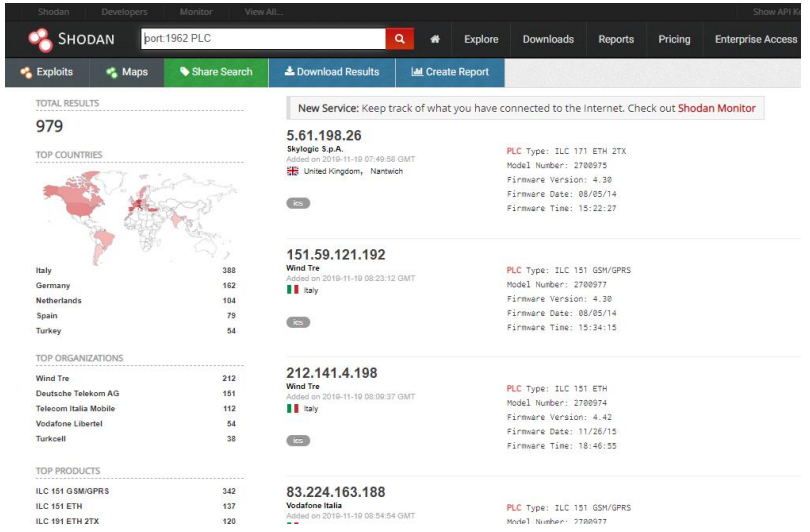
Aujourd'hui, à part quelques exceptions, on a aujourd'hui plusieurs années de retard par rapport au niveau que l'on devrait avoir.

L'avantage d'avoir des systèmes industriels isolés **se retournent contre nous aujourd'hui** : pas ou peu de prises en compte de la sécurité sur ces systèmes qui sont en train d'être interconnectés avec des systèmes d'information « extérieurs » (de l'entreprise ou même hors de l'entreprise) ;

Quelques mesures de sécurité qui doivent venir des basiques :

- Avoir un **inventaire fiable** de ces systèmes (+ veille vulnérabilité) ;
- Déploiement de **correctifs** (OS, applicatifs, etc.) dans des environnements complexes ;
- Mise en place d'exigences cybersécurité dans les **contrats** avec des fournisseurs historiques ;
- **Gouvernance** (Recrutement de ressources dédiées compétentes, sensibilisation) ;
- **Cloisonnement des réseaux** SI Industriels / SI de l'Entreprise tout en prenant en compte les besoins métiers (données production, télémaintenance, Cloud, etc.) ;
- **Surveillance** « cyber » des SI Industriels pour détecter au plus tôt les évènements de sécurité

Les différents vecteurs d'intrusions les plus courants



- Des SI Industriels **connectés à Internet** (merci **Shodan**)
- Des **accès tiers** non surveillés ou managés
- Des **vulnérabilités récurrentes** sur les PLC et les IHM :
  - Services accessibles (FTP, Telnet, Web, Modbus SNMP)
  - Credentials codés en dur
  - Vulnérabilités applicatives classiques (injection SQL, authentification, XSS, etc.)
- Des **accès directs** sur les systèmes industriels (clé USB d'un opérateur contaminé par exemple)
- Les SI Industriel **accessibles librement** à travers le SI de l'Entreprise

Mais un monde qui s’organise autour de tout ça

En France, à travers des lois et des stratégies :

- **Livre blanc sur la défense et la sécurité nationale**
  - Focus sur la Cybersécurité.
  - La protection des États et des OIV : une priorité nationale
- Loi de programmation militaire : **cadre juridique à respecter pour les OIV**
  - Mise en place des dispositions réglementaires relatives à la sécurité des systèmes d'information des opérateurs d'importance vitale (OIV) avec des décrets par secteurs
- Des **plans d’investissements**, comme le pacte Défense cyber en 2014 par exemle
  - Budget annoncé d’un milliard d’euros : renforcement de la cybersécurité des installations militaires; augmentation de l'effort de recherche et développement de nouvelles armes.
  - renforcement de la SSI de l’État, développement d’une industrie cybersécurité, effort sur formation

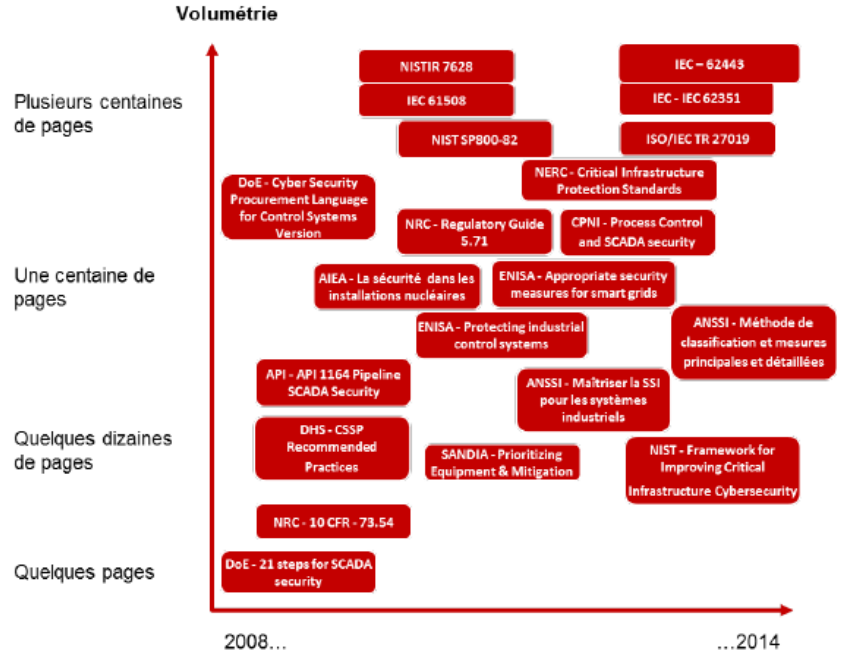
Et l’Europe n’est pas en reste, avec l’ENISA et ses groupes de travail ou les travaux de la Commission Européenne

Source : étude CLUSIF 2015

Mais un monde qui s'organise autour de tout ça

A travers des référentiels :

- Une littérature abondante
- Certains spécifiques à des secteurs d'activité
- Pour tout public : Filière SSI, Conception / Intégration / Maintenance, Filière SII



Source : étude CLUSIF 2015

De nombreux documents de références

- Guides ANSSI :
  - Maîtriser la SSI pour les systèmes industriels
  - Méthode de classification et mesures
- Norme IEC 62443
- ISO 27019
- NERC CIP
- NIST SP800-82

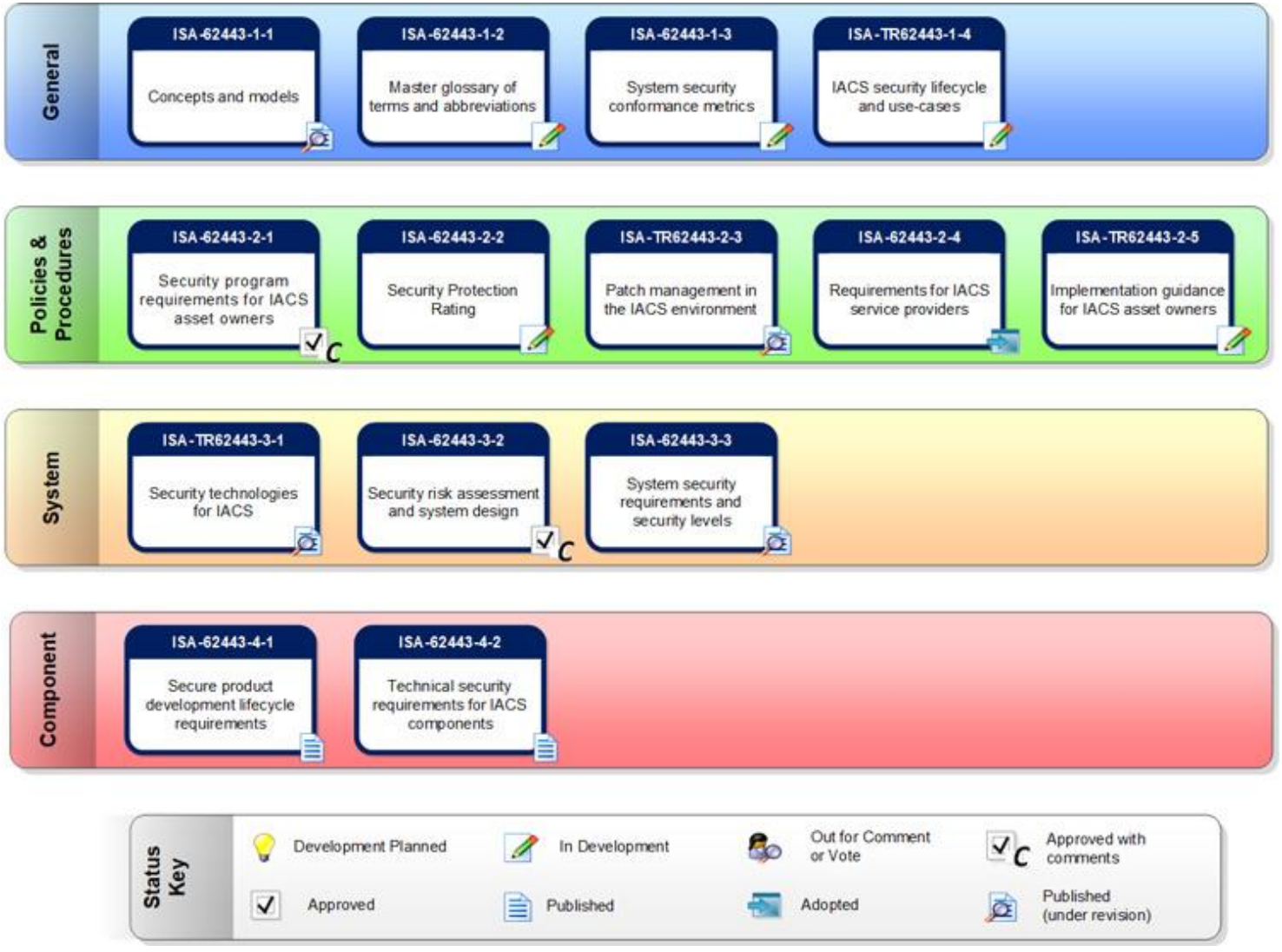
Mais un monde qui s'organise autour de tout ça

Des référentiels incontournables

Source : Etude CLUSIF 2015

Mais un monde qui s'organise autour de tout ça

Focus sur l'IEC 62443



Mais un monde qui s'organise autour de tout ça

A travers des recherches & conférences :

Juillet 2017

Présentation de plusieurs cyber-attaques contre des parcs éoliens ayant des impacts logiques et physiques, lors de BlackHat 2017

Aout 2017

Démonstration théorique et pratique de la façon dont un pirate informatique pourrait causer des pannes d'électricité locales et continentales sur des installations photovoltaïques lors de la conférence SHA2017

SA x20

IECON '18

The 44th Annual Conference of the IEEE Industrial Electronics Society

Washington D.C., USA | October 21-23, 2018

IEEE

ies

Et demain ?

- Des systèmes IT & OT **de plus en plus interconnectés** ;
- **Explosion des données** au sein de l'OT ;
- **Explosion des systèmes connectés** (OT / IoT) avec l'arrivée de la 5G, des véhicules connectés, etc. ;
- Réflexion pour la mise en place de **certifications** de ces solutions industrielles (IQS-Label, réflexion de la Commission Européenne, etc.)

Merci