Introduction

SECURITES DES RESEAUX INDUSTRIELS

M2I 3 ème année

Guillaume PETIT

Tables des matières :

Historique des modifications :

Date	Version	Évolution du document	Auteur
18/11/2020	1	Création du document	Guillaume PETIT

Documents liés :

N°	Date	Nom	Sujet

Références :

N°	Lien

1 Terminologies :

1.1 ICPE :

Installation Classées pour la Protection de l'Environnent

L'**ICPE** c'est une norme Française L4ICPE date des année 60.

"usines, ateliers, dépôts, chantiers, installations exploitées ou détenues par toute personne physique ou morale publique ou privé, pouvant présenter des dangers ou des inconvénients pour le voisinage, pour la santé, la sécurité, la salubrité publique, l'agriculture, la nature, la conservation des sites et des monuments du patrimoine archéologique",

1.2 Installation industrielle :

Pour l'Etat Français C'est un système technologique délimité par un périmètre (ex : un site), qui peut être :

- Un site fixe (lieu de stockage, un lieu d'approvisionnement, une usine, une raffinerie, un réseau de transport, aéroport, port maritime)
- Un site mobile : Pétrolier, croiseur, plateforme pétrolière, stellite….
  La configuration du site peut être de deux formes :
  - Monolithique : un endroit unique (site) ou tout est centralisé,
  - Réseau hybride : champs éolien, smartgrid (réseau électrique intelligent), gazoduc, distribution d'eau

2 Historique de la SSI sur les réseau Industriels :

Travaux du passé sur la sécurité des réseau industriels et installations industrielles :

Début de l'ère industrielle -> concentrés les efforts d'ingénierie sur des méthodes permettant d'optimiser les processus de fabrication (redondance des équipements -> problème financer, ne pas perdre de l'argent à cause d'une production défaillante -> résilience industrielle). Optimisation des méthodes stockage des matières premières ou produits finis (flux tendus),

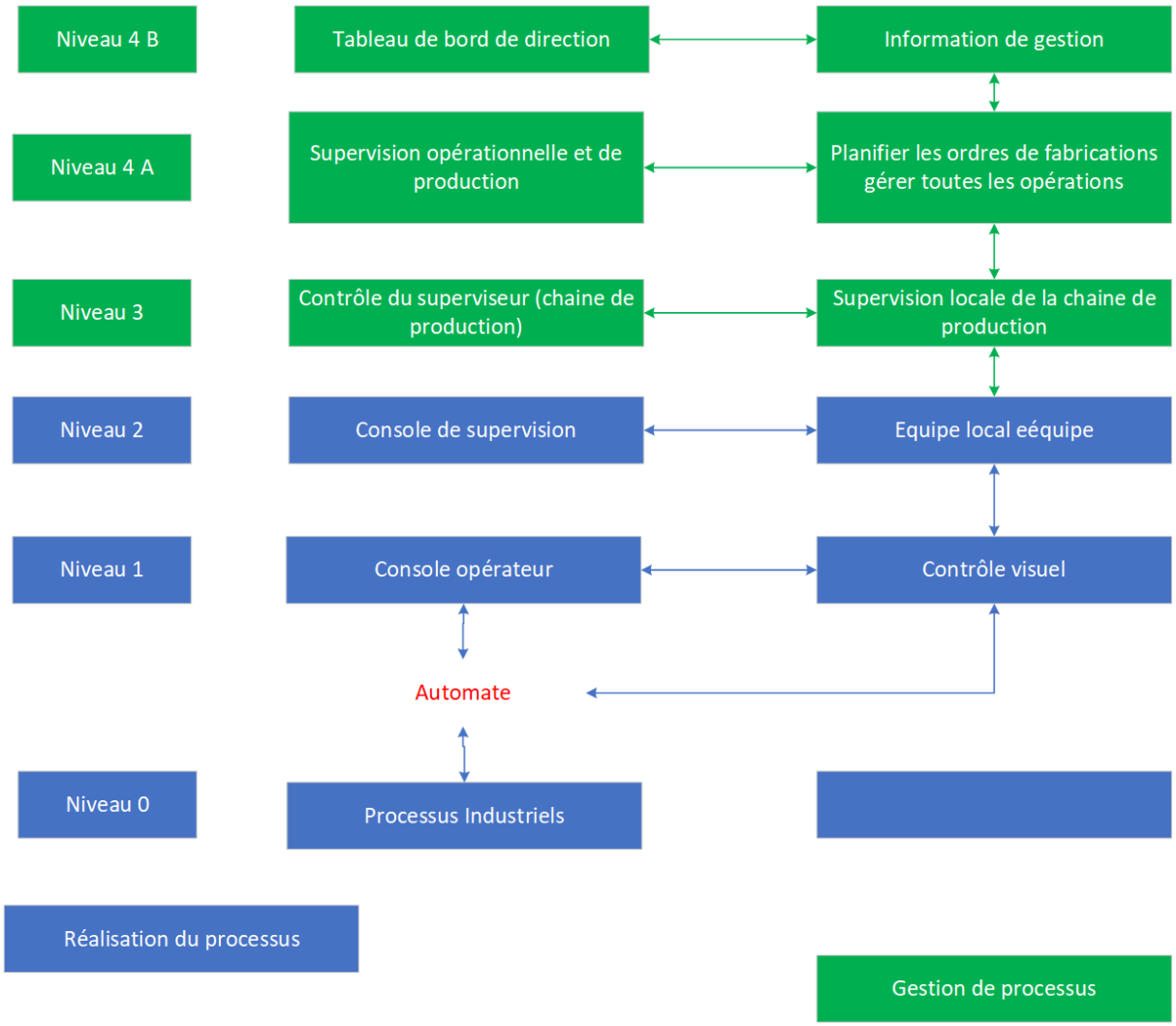
Début 1900 -> première norme environnementales : crash pétrolier -> réfléchir à modifier l'approche purement optimisation économique dans la conception des usines (installation industrielles) -> arrivé de l'informatique.

Début 1970, première version livrée et exploitée : 1980. Ce sont les Américains qui créer le modèle Purdue "Purdue Laboratory for Applied Industrial Control". Organisation dot l'objet principal a été créer une organisation des installation industrielles compatibles avec les critères "CIM" Computer Integrated Manufacturing. Ce modèle a évolué et est devenu le modèle CIM89 (revalidé/modifié en 1989).

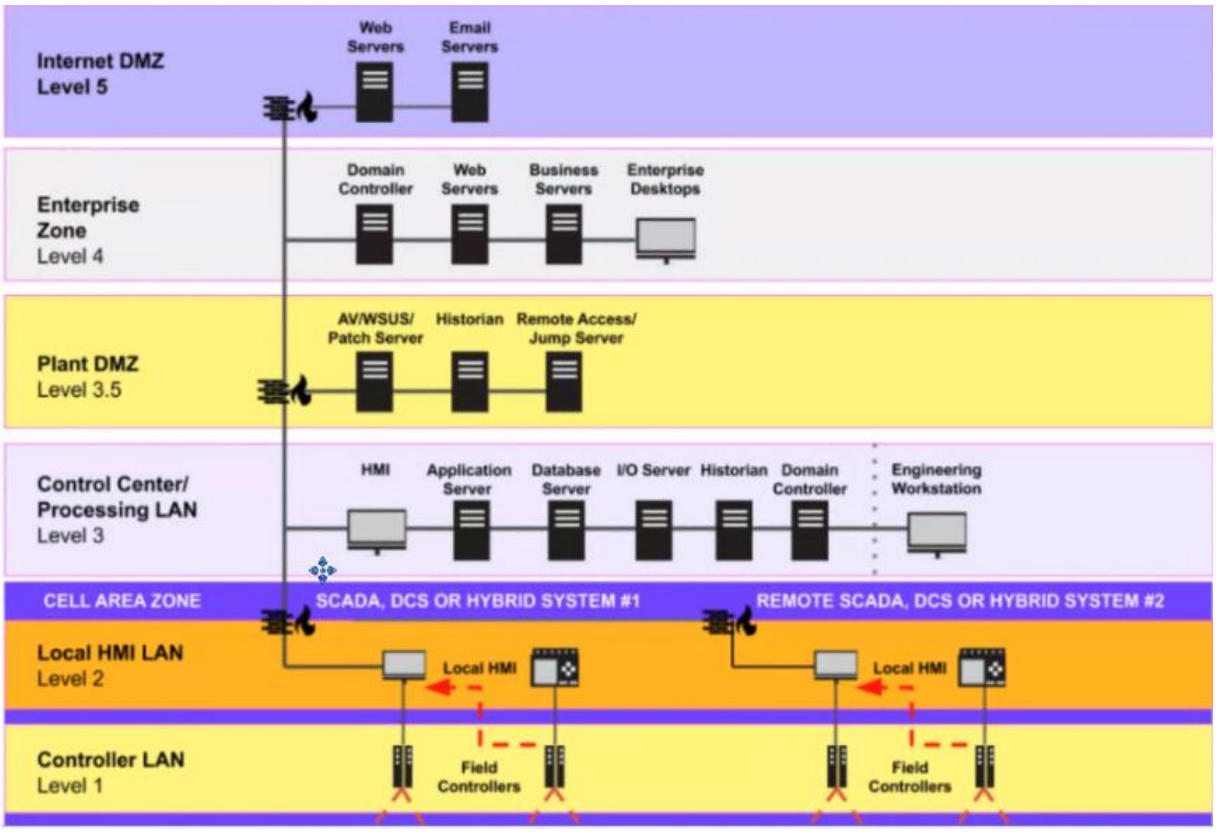
Tout le monde appelé CIM89 ou CIM, le modèle PURDUE
Tous les industriels du monde entier connaissent ce modèle.
Ce modèle catalogue les activités, les tâches et le processus à opérer et hiérarchise le contrôle entre les niveaux.

3 Les modèles :

3.1 PURDUE CIM :



3.2 PURDUE CIM89 :



En 1989, les ingénieurs n'ont pas pris en charge **l'IoT** et la remonté des données dans le cloud. Mais c'est quand même bien pensé pour **1989**.

4 La règlementation :

ICPE : Nomenclature ; SEVESO : Classification
Ces deux éléments sont issus de la réglementation Française.

4.1 La nomenclature ICPE :

Nomenclature ICPE est une rubrique permettant de classer la nature du risque :

- Substance (toxique, comburants, explosivité, combustible, corrosion, réaction ou précipitation chimiques),
- Activités (Agriculture, Elevage, Agroalimentaire, textile, carton, minerai, chimie, plastique, déchets),
- Emission industrielle : En fonction des rejets, nécessité de recourir aux meilleures techniques existantes afin de prévenir toute pollution environnementale,

L'entreprise rempli un formulaire ICPE lorsqu'elle a une activité industrielle, ce formulaire est transmis au préfet. Le préfet transmet à l'Etat ce formulaire avec avis.
L'état qui donne l'autorisation d'exploiter, si les méthodes de dépollution permettent d'atteindre les VLE (Valeurs Limites d'Emission).

4.2 Les classements SEVESO :

Les classements SEVESO, il en existe plusieurs :

- **NC** (*Non Classé*) : Vos activités sont sous le seuil de la pollution de dangerosité de la nomenclature ICPE,

- **D** (*Déclaration*) : L'installation ICPE, doit faire l'objet d'une déclaration au préfet avant la mise en servie du site de production : le risque est acceptable l'entreprise suis les prescriptions nationales,

- **DC** (*Déclaration Contrôlée*) : Déclaratif au préfet et un contrôle et un audit régulier par un organisme,

- **E** (*Enregistrement*) : Avant mise en service, l'entreprise a monté un dossier SEVESO, ce status indique que le dossier est en cours de traitement par les services de l'état. Le Préfet demande un audit extérieur pour vérifier que le dossier respecte les préconisations nationales,

- **A** (*Autorisation*) : Le préfet a statué par arrêté préfectoral au cas par cas de l'autorisation SEVESO (faut pour les sites non classés),

- **AS** (*Autorisation et Servitudes*) : Risque technologiques élevés, qui s'approchent ou dépassent les seuils de dangerosité ou de rejet autorisés par l'état. Les seuils dépassés sont autorisés parce que le site de production est considéré d'utilité publique. Dans ce cas, il sera impossible d'installer d'autres sites industriels ou habitations personnelles à proximité,
  S'il y a déjà des habitations à côté d'un site SEVESO qui dépasse les normes alors l'état qualifie l'industrie d'utilité publique et « *on fait avec* ».

4.3 La LPM :

Entre 1993 et 2014, les état Européen ont mis en œuvre les **Lois de Programmation Militaire** (LPM). La **Loi de Programmation Militaire** précise les responsabilités des états de définir et s'assurer d'une cybersécurité suffisante des systèmes critiques des opérateurs d'importance vitales. Par extension, la responsabilité de définir les bonnes pratiques pour toutes entreprise opérant avec des **Systèmes d'Informations**.

Le secteur couvert par les LPM :

- **SAIV :** *Secteur d'Activité d'Importance Vitale*, *article R1332-2 LPM*
  - Armée, Police, Gendarmerie,
  - Vinci Autoroute,
  - Maintient du potentiel du défense du pays (Airbus, Thalès, etc.),
  - La sécurité de la nation,
  - La grande distribution,

  Chaque pays Européen peut déterminer ses SAIV c'est la seule liberté des états pour adapter la directive dans sa législation. C'est le premier ministre qui décide les domaines référencés dans les SAIV.

- **OIV :** *Opérateur d'Importance Vitale* (l'entreprise), article *R1331-1 LPM*
  Organisation qui exerce des activités comprises dans un secteur d'importance. Gère des établissements ou des ouvrages dont le dommage ou l'indisponibilité (ou la destruction) à la suite de malveillance, de sabotage, de terrorisme pourrait directement ou indirectement altérer gravement le potentiel de guerre économique, la sécurité ou la survie du pays, ou mettre gravement en danger la santé de la population. Les ministres vont fixer les OIV pour chaque ministère qu'il gère.

- **PIV :** *Point d'Importance Vitale* (site),
  Site ou installation dont le dysfonctionnement causerait les mêmes symptômes que ceux sur une OIV. Les PIV font l'objet d'audits constants Concernant la sécurité physique et la mise en ouvre de contre mesure à chaque risque potentiel évalué.

L'ANSSI a fait un effort de classification, qui sont des modèles complémentaires à SEVESO/OIV/PIV permettent de gérer ou planifier la sécurité d'une entreprise critique ou d'un secteur critique.

4.3.1 Type A1 :

Chaîne de procédé (atelier automatisé)

- PURDUE niveau 0 et 1,

Un seul site, créer son produit finit de bout en bout. L'accès aux système numériques de production (supervision, commande, maintenance) Implique un raccordement à des réseaux extérieur, ou un accès physique.

- Attention : Contrôle d'accès physique (traçabilité), tiers intervient, un contrôle spécifique. Recommande IDS pour les connexions réseaux. Mise à jour des firmware systématique, obligation de contrôler l'absence de malware,

4.3.2 Type A2 :

Site de maintenance d'équipement :

- PURDUE 0,1,2

Zone(s) de stockage de pièces détachées + une partie des sites A1, mises à jour de firmware, adaptation de certains équipements en fonction des conditions.
Recommandations : Accès physique / traçabilité des tiers, IDS, contrôle de la validité des firmwares + contrôle de l'absence de malwares

4.3.3 Super A :

Installation industriel distribuée à logistique semi automatisé

- PURDU 0 à 4

Production répartie sur plusieurs sites (plus ou moins distant), la logistique entre site est semi automatisée, contient des sites A1, des zones de stockage (produit intermédiaire) les sites A2.
Attention très forte nécessité de chiffrer intégralement tout le trafic entre les sites. Traçabilité des mouvements de produits entres sites IDS, contrôle et MAJ Firmware y compris de tous les IoT de la chaine de transport. Communication IoT et de reste des sites production est intégralement chiffré. Séparation des communications (VLANs, pas de communication autorisée entre site, sauf pour les besoins de la production de la chaine de l'IoT).

4.3.4 B1 – Bâtiment fixe :

Bâtiment nécessitant un approvisionnement en énergie disposant d'une évacuation de déchets, autonomie maximale recherchée (datacenter, défense nationale -> OIV),

Attention : Sécurité physique paranoïaque, surtout sur la partie industrielle.
Exemple : building avec des salariés. Ventilation, Climatisation, Eau potable, Ascenseur -> garantir le bon fonctionnement, la résilience de ces systèmes.

4.3.5 B2 – Bâtiment mobile :

Se déplace ou peux se déplacer plus ou moins rapidement et ce déplacement est nécessaire à sa mission.
La notion de sécurité des personnes est accrue -> sous-marin, le plus important sera d'évacuer les occupants en cas de cyberattaque paralysant les systèmes du sous-marin.
Le bâtiment mobile doit disposer en tout temps et toutes circonstance de moyens lui permettant de communiquer.

4.3.6 B3 – Bâtiment mobile reparti :

Comme B1, mais son périmètre et plus étendu qu'un bâtiment. Toute l'automatisation d'une ville (signalisation, caméras, éclairage publique, smartgrid, route à accès contrôlé – plots).
Relais télécommander, centre de contrôle (qui ne sont pas toujours les mêmes).

Attention hardening fort suer les communications sans fil ou à distance. Hardening des accès physiques aux relais télécommunication.

4.3.7 Super B :

Installation massivement répartie à l'échelle d'un pays, d'un continent par exemple le trafic aérien. Hardening des communications spécifiques (tour de contrôle).
Paranoïa sur les IDS

4.3.8 C1 – Equipement sans prépondérance logicielle mais à risque numérique :

- Fourniture de services à la population, exposé à un risque (s) numérique(s)
  Par exemple les centrales nucléaires,

- Sensibilisation aux risques informatiques, y compris les accès physiques, entraînement régulier (mise en situation, des salariés, équipe informatique : SOC/NOC/CSIRT),

Nouveauté, Mise en place de système de détection comportementale.

4.3.9 C2 – Réseau de distribution :

Achemine des fluides d'un point A à un point B, contrôlé par des systèmes numériques. Risque sur la chaîne de transport. Attention la sécurité est de ressort de l'ANSSI qui ne communique pas sur le sujet.