Sécurité Informatique des systèmes industriels en 2016

OSSIR
Paris, 12 janvier 2016

Christophe Renard <Christophe.Renard@hsc.fr>

Plan

- Généralités sur les SI industriels
- Les menaces
- Evolution des risques
- Cadre réglementaire et légal
- Constats
- Sécurisation : par où commencer ?
- Conclusions

Généralités sur les SII

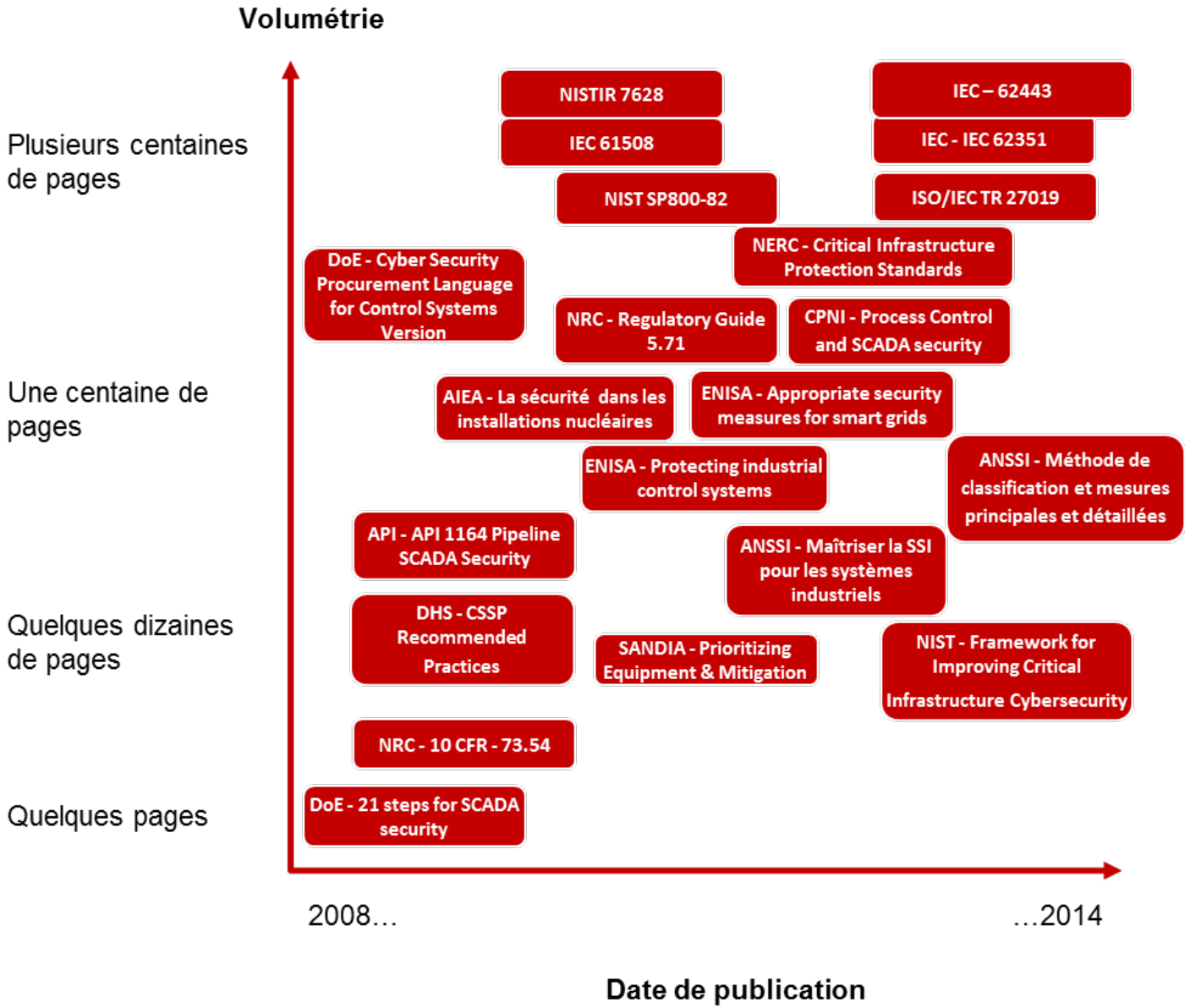
De quoi parle-t-on ?

- Un vocabulaire confus : SCADA, ICS, DCS...
  - Rigoureusement :
    - **ICS** « *Industrial Control Systems* » / Systèmes de contrôle industriel
      - Terme général rencontré dans la littérature technique
    - **SCADA** : uniquement la supervision, l'acquisition de données
      - Terme sorti du pur domaine technique
    - **DCS** « *Distributed Control Systems* »
      - ICS décentralisés, couvrent la plupart des systèmes modernes
  - SCADA domine
    - Devenu synonyme de ICS dans les médias
    - Par abus de langage désigne souvent tous les systèmes industriels
  - Beaucoup de définitions sont propres à un métier/secteur

Un domaine très morcelé

- Beaucoup de producteurs de référentiels, normes ou standards
  - **ISO** (Organisation Internationale de Normalisation)
  - **IEC** (Commission Electrotechnique Internationale)
  - **ANSI** (*American National Standards Institute*)
  - **NIST** (*National Institute of Standards and Technology*)
  - **NRC** (*Nuclear Regulatory Commission*), **IAEA** (*International Atomic Energy Agency*)
  - **ENISA** (Agence Européenne chargée de la sécurité des réseaux et de l'information)
  - **NERC** (*North American Electric Reliability Corporation*) **CIP** (*Critical Infrastructure Protection*)
  - **CFATS** (*Chemical Anti-Terrorism Standards*)
  - **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information)
  - **ISA** (*The International Society of Automation*)
  - Etc

Littérature abondante



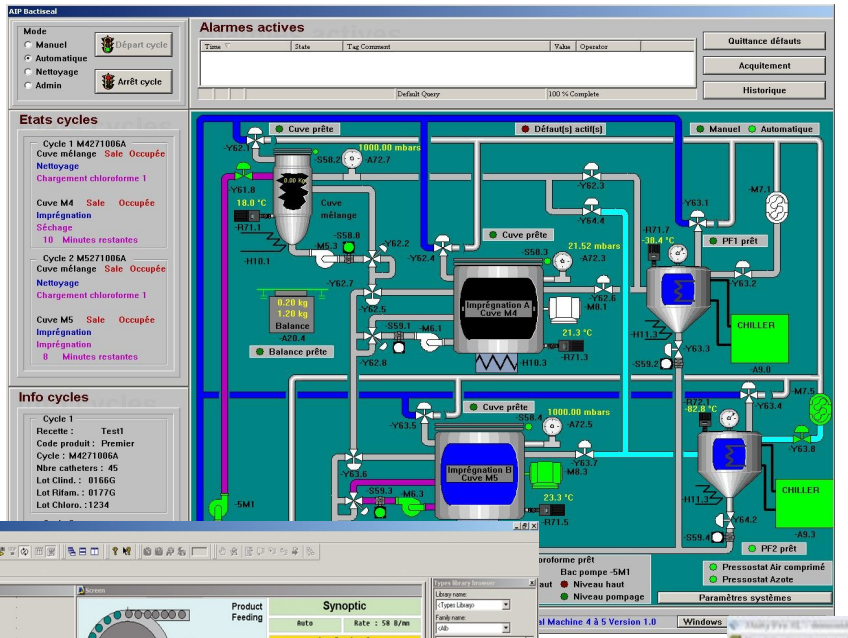
Evolution des systèmes industriels

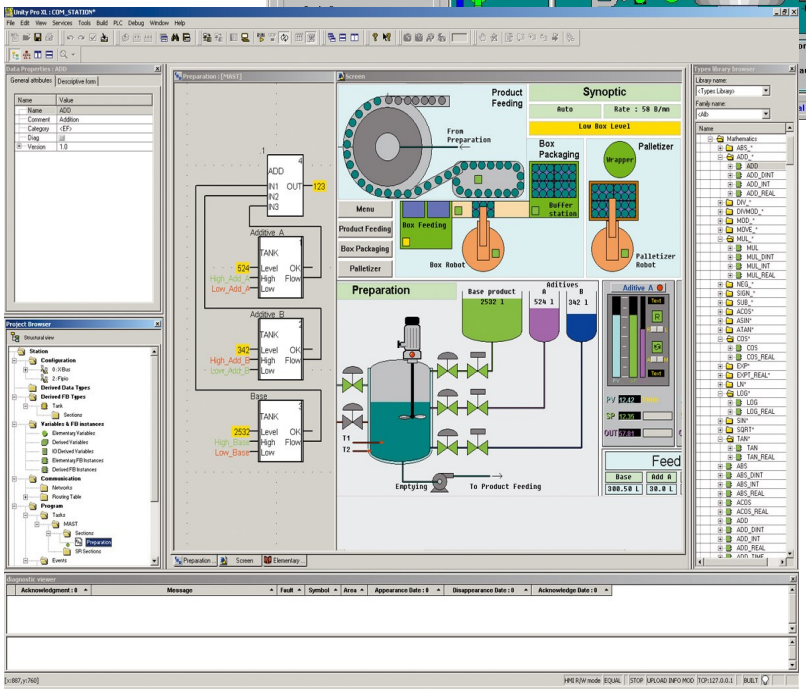
- Initialement des systèmes *adhoc* et propriétaires
  - Connexion directe PC/automate : connexion série
  - Dans quelque cas : un réseau local
    - Très peu de systèmes étendus
  - Pas de standard du marché
  - Accès distant par modem
- Evolution moderne
  - Standardisation
    - Des systèmes sous Ms Windows
    - Des protocoles : Ethernet, Modbus, TCP/IP
  - Connectivité
    - Extension des zones couvertes
    - Connectivité des sites distants via Internet
    - Raccordement au réseau de zones peu protégées (shelters, sous-stations ...)

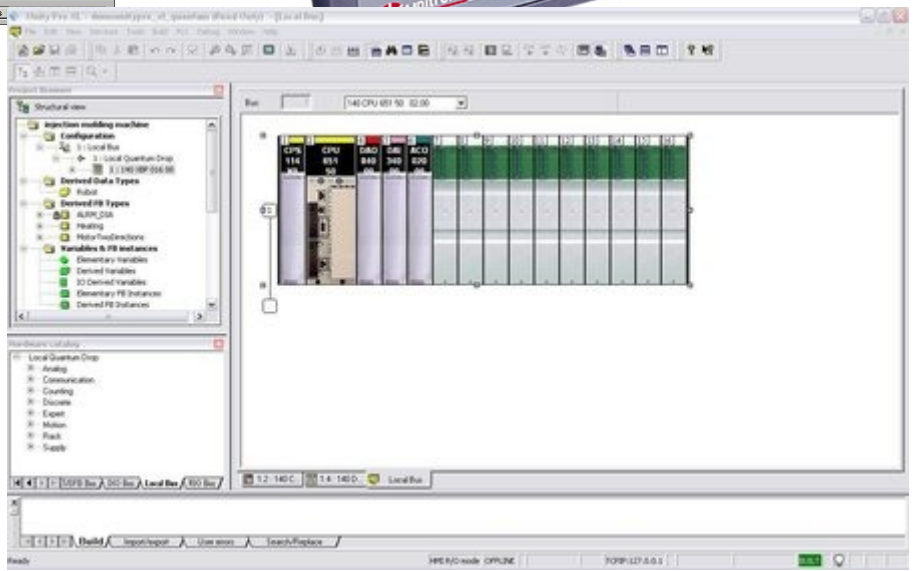
Actionneurs et automates

- Dispositifs télécommandés
  - « Simple » dispositif mécanique lié à une commande électrique télécommandable
- Automates
  - Schneider
  - Emerson
  - Siemens
  - Honeywell
  - Rockwell Automation / Allen-Bradley
  - Yokogawa
  - ABB
  - Wago
  - Etc.

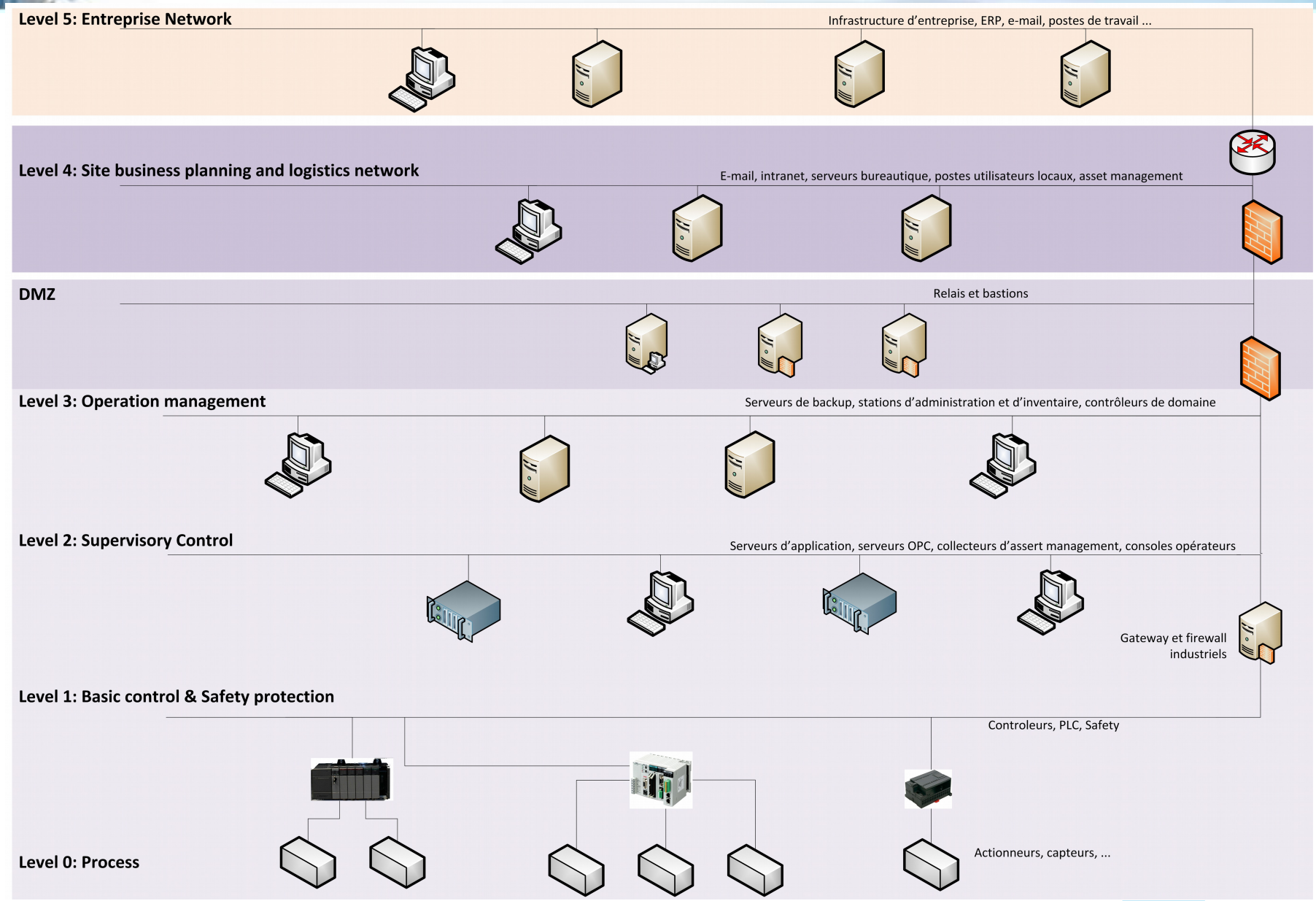
IHM (Interface Homme-Machine)



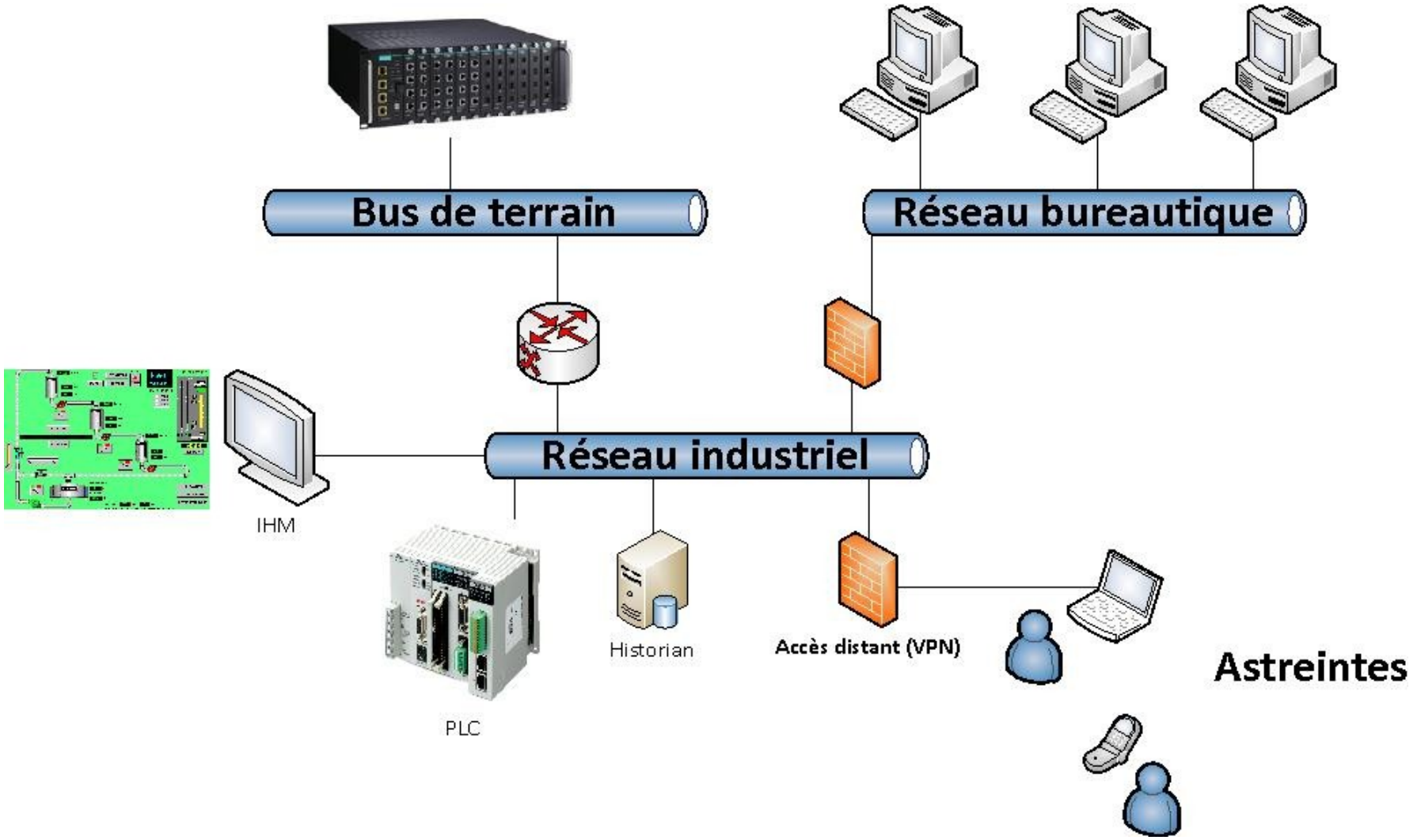




Architecture par couches(ISA95)



Système industriel réaliste



Les menaces

13 Usines de montage automobiles aux USA

- Année 2005
  - Attaque non ciblée :
    - Mais dégâts à grande échelle
  - Ver Zotob
    - Le ver s'est propagé dans tout le réseau bureautique
      - Puis industriel
      - Une fois dans le réseau industriel
        - Propagation horizontale d'usine en usine
        - 13 usines impactées
    - Impacts
      - 50000 travailleurs à la chaîne de bloqués
      - Pertes estimées à 14 millions de dollars

Attaque sur une fonderie allemande

- Rapport publié en 2014 par le Bureau Fédéral de Sécurité Informatique Allemand
- Attaque de 2013
  - Peu de détails fournis
    - Entrée des attaquants par compromission de postes utilisateurs
    - sur le SIE, par courriels piégés
    - Dégâts estimés en millions d'euros
  - Première attaque documentée par des criminels sur infrastructure industrielle

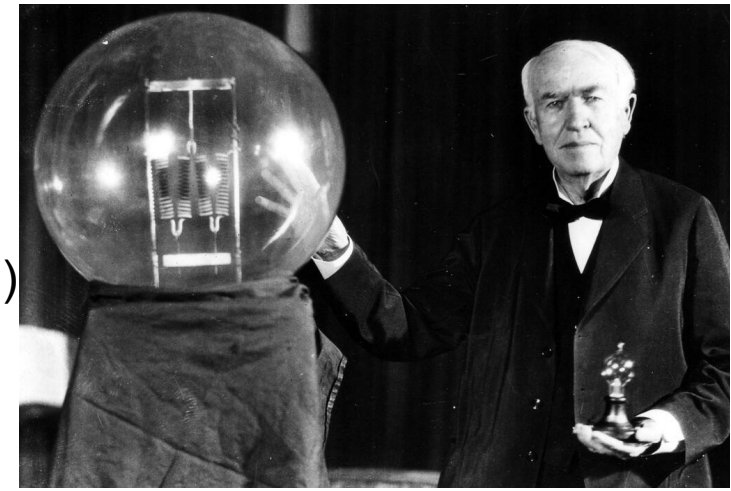
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

Sabotage de noël en Ukraine

- Décembre 2015, coupures de courant
  - =~ 80000 foyers affectés
  - Principalement le 23/12
  - Infection par un malware criminel russe connu :
    - BlackEnergy
    - A permis la diffusion d'un vecteur d'attaque ciblé
      - Malware non encore étudié publiquement
    - Nettoyage des traces par KillDisk
  - Des zones d'ombre
    - Attaque simultanée en déni de service sur les lignes de hotline des fournisseurs
      - Moyen non détaillé à ce jour.
    - Nature de la charge industrielle non détaillée à ce jour
  - Selon iSight attaque russe
    http://www.isightpartners.com/2016/01/ukraine-and-sandworm-team/
  - Synthèse par SANS
    https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
  - Alerte ICS Cert
    - https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

Tendances des attaques

- **Les attaques non ciblées sont un risque permanent**
  - Forte vulnérabilité des SII aux virus informatiques
  - Difficulté du maintien à jour : correctifs, bases antivirales



- **Les attaques criminelles sont probables**
  - Manipulation de marché (production, matières premières)
  - « Prise en otage » d'usine (exemple des *crypto-lockers*)
- **Sabotage informatique gouvernemental**
  - Partie standard de l'arsenal des nations
  - Rôle classique des forces et services spéciaux
  - Peu différent du sabotage traditionnel
  - Mais moins coûteux
- **Le terrorisme par voie informatique, un risque de second rang ?**
  - Difficulté à revendiquer un incident industriel de façon crédible
  - Complexité de la planification de l'aspect industriel de l'incident
  - Mais récurrent dans les médias (*« American Blackout »* ...)
  - Faible risque pour l'attaquant, mais forte technicité(métier) requise

Evolution des risques

Attentes des entreprises

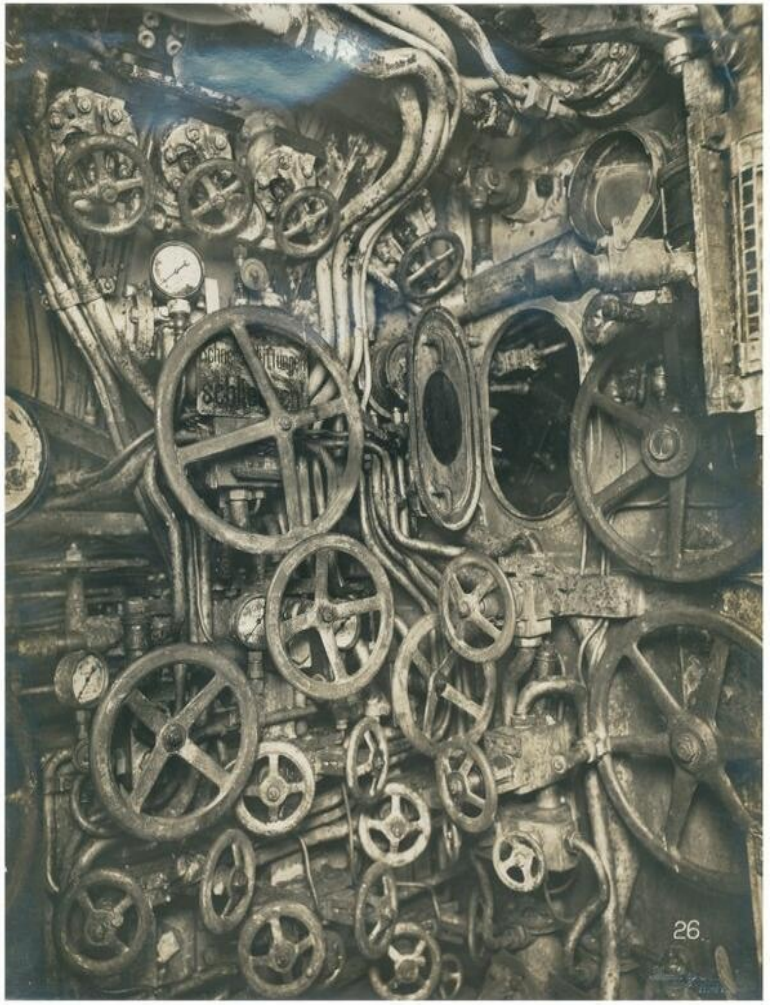
- **Diminuer les coûts**
  - Moins de personnel
  - Plus d'automatisation
  - Factorisation des fonctions support SII/SIE
  - Accès aux données et diagnostiques partout
    - Réalité augmentée : *« Virtual X-Ray »*
    - Terminaux portables
- **Optimiser les processus**
  - *« Analytics »* → méga-données
  - Services tiers d'optimisation *« factory in the cloud »*
  - Boucles de *reporting* courtes
- **Réactivité**
  - Production « à la demande »
    - Raccord du marché à la production → intégration SII/SIE
    - Raccourcissement de la chaine R&D / Production
      - Directement de la CAO vers la production
  - Suivi Temps réel
  - Sous-traitance de toutes fonctions non-essentielles

Le futur des systèmes industriels

- L'usine intégrée
  - Promue par les équipementiers
    - GE : *« Internet of Industrial Things »*
  - Fin de la séparation entre SI d'Entreprise et SI Industriel
  - Accès universel à l'information :
    - Captation d'incidents de production au niveau de la pièce
    - Tableau de bord temps réel de toute l'entreprise
    - L'ERP au cœur de toutes les activités
  - Flexibilité
    - Reprogrammation rapide des chaînes de production
    - Gestion des stocks au fil de l'eau
    - IHM Versatiles
- Toutes ces tendances rendent la sécurisation plus complexe

Fin de la défense périmétrique

- **Interconnexions omniprésentes**
  - SI d'entreprise
    - bases de données, ERP
    - Partage de ressources réseau et télécom
  - Accès partenaires
    - Maintenance tierce
    - Équipement en leasing
    - Systèmes logistiques, support
    - Cloud
  - Systèmes répartis et hétérogènes
    - Fusions acquisitions d'entreprises et groupes
    - Multi-sites : points d'entrées partout
      - du plus petit au plus énorme
    - Globalisation de l'Entreprise
- **Comment gérer de l'exposition**
  - Micro-périmètres ?
  - Sécurité des extrémités ?
  - Protection des flux ?



Cadre légal

Evolution de la perception des risques

- Les risques industriels sont pris en compte depuis longtemps
  - Mais moins les dimensions informatique et intentionnelles
- La perception du risque par le législateur a évolué
  - Avant 2001 : l'accidentel
    - Installations « Seveso »,
    - Informatique très critique : nucléaire, aérien, ferroviaire
  - 2001 : le terrorisme et les risques sur les populations
    - Attaque du 11/09/2001 et l'explosion de l'usine AZF
    - Création des Zones d'Importance Vitale
  - 2008-2013 : protection des fonctions vitales
    - 2008 - Livre blanc sur la défense et la sécurité nationale
    - 2009 - Création de l'ANSSI
    - 2013 - Politique de la France en matière de cyber-sécurité

Loi de programmation militaire 2014-2018

- LOI 2013-1168 du 18 décembre 2013, article 22
  - A modifié le Code de la Défense
  - Relative à la protection des infrastructures vitales contre la cyber-menace
  - Règles de sécurité fixées par le Premier Ministre
- Détection et gestion des incidents : systèmes et prestataires qualifiés
  - PDIS : prestataires de détection d'incidents de sécurité
  - PRIS : prestataires de réponse aux incidents de sécurité
- Obligation de remonter les incidents à l'ANSSI
- Contrôle d'évaluation du niveau de sécurité et du respect des règles : prestataires qualifiés
  - Extension du champ d'action des certifiés PASSI : Prestataires d'Audit de la Sécurité des Systèmes d'Information (issus du RGS)

Opérateurs d'Importance Vitale

- Un OIV opère des Points d'Importance Vitale (PIV)
  - Dans des Zones d'Importances Vitale (ZIV)
  - Avec des Systèmes d'Information d'Importances Vitale (SIIV)
- Désignés par le ministre coordonnateur du secteur d'activité
  - Sur avis de la Commission interministérielle de défense et de sécurité des SAIV (Secteurs d'Activité d'Importance Vitale)
  - Comprend des représentants de la Défense et de l'Économie
  - 218 OIV, liste réputée classifiée Confidentiel Défense
- Périmètre des SIIV
  - L'OIV propose
    - Sur la base du guide de sécurité des systèmes industriel de l'ANSSI
  - L'ANSSI commente (de façon directive)

Calendrier

- Première liste des SAIV fixée par arrêté en juin 2006
  - 12 secteurs d'activité d'importance vitale
- Septembre 2008 : IGI 6600 (MàJ janvier 2014)
  - Objectif : anticiper et réagir à la menace terroriste
  - En particulier, menaces liées à la sécurité des systèmes d'information
- En 2014 : loi de programmation militaire
  - Une partie concerne directement la SSI des OIV
  - Pour les systèmes industriels :
    - Guide de cyber-sécurité des systèmes industriels (ANSSI)
- 2015 :
  - Mars : Sortie du décret d'application de l'article 22 de la LPM
  - Sortie de nouveaux référentiels : PRIS, PDIS, PASSI 2.1
  - Ateliers avec les OIV
  - Arrêtés sectoriels : *date mystère*

Perspectives d'évolution du paysage légal et réglementaire

- **La tendance est au durcissement légal et réglementaire**
  - Responsabilité de l'opérateur du système
  - Responsabilité des fournisseurs informatiques
  - Incorporation de la dimension informatique aux normes de sûreté
- Assurance des installations
  - Le risque informatique devra être couvert à terme
  - Va imposer exigences et points de contrôle
- Besoin de normes de sécurité des systèmes industriels européennes, voir mondiales sur lesquelles s'aligner

Constats

Une situation hétérogène

- La taille de l'organisation est importante
  - Ressources et taille des équipes
  - Complexité et connectivité des systèmes
- Mais d'autres facteurs comptent
  - Secteur d'activité
    - Critique ou pas
    - Marges disponibles
  - Ancienneté des installations
  - Exigences de sécurité des clients
  - Étendue géographique de l'activité et des sites

Dichotomie offre/réalité

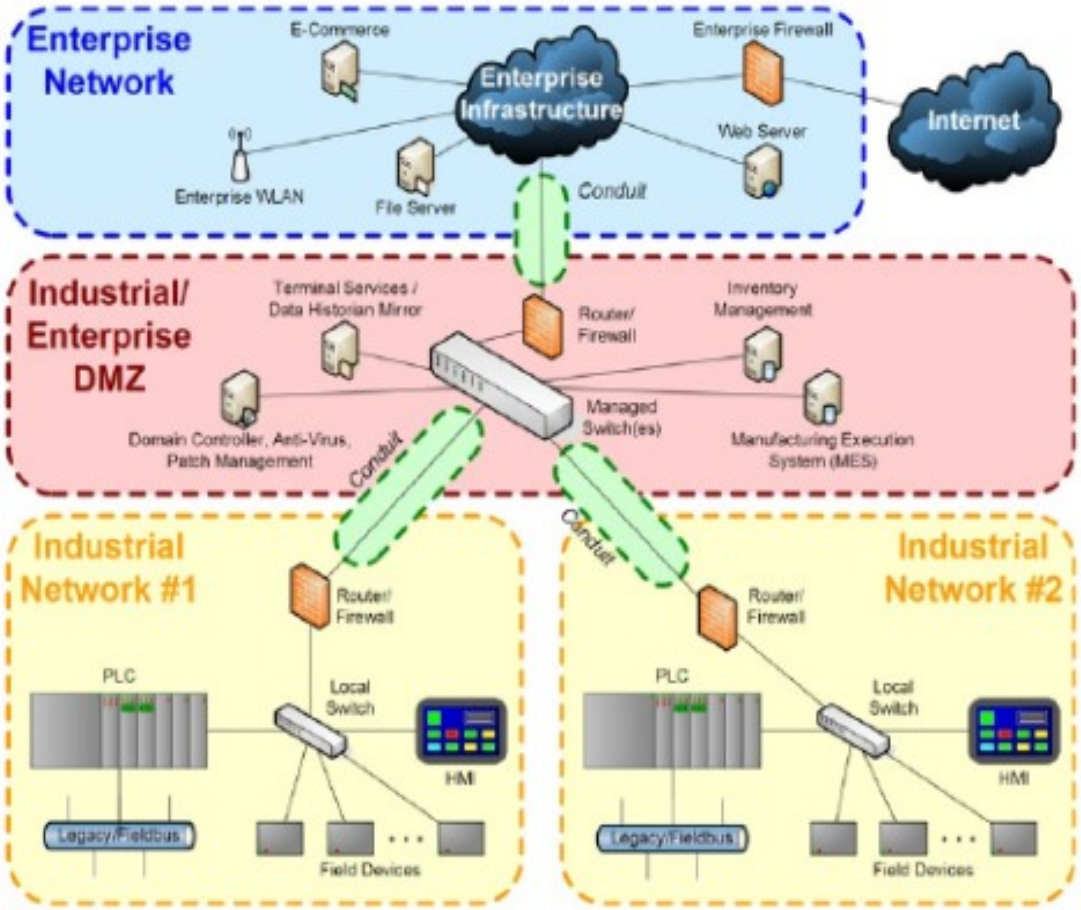
- Chez les équipementiers
  - Gammes intégrées
    - PLC / Logiciels / Protocoles de même génération
  - Sécurisation active et gérée
- Dans la réalité
  - Panachage de générations
    - Alignement sur le moins-disant → protocoles non sécurisés
  - Options par défaut
    - Comptes et mots de passe par défaut ou triviaux
  - Priorité à la disponibilité
    - Crainte d'auto-déni de service
      - Expirations de certificats
      - Composants ne fonctionnant qu'avec des valeurs par défaut

Sécurisation : par où commencer ?

Segmenter : Défense en profondeur

- *Zones and conduits* – ISA-99.03.03 (IEC 62443)

- **Zones**
  - Groupe d'actifs logiques ou physiques qui partagent les mêmes exigences de sécurité
- **Conduits**
  - Chaque communication entre zones est effectuée par un conduit



Gérer les accès aux systèmes

- Salle de contrôle
  - Typiquement de multiples systèmes
  - Contrôle par accès physique
  - Besoins d'authentification:
    - Rapide et simple (carte à puce ?)
    - Centralisée pour N systèmes
    - Produits du monde « bureautique » inadaptés
  - Systèmes répartis
    - Contrôle physique complexe (*shelters* et boitiers en extérieur)
    - Utilisation du callback : y compris sur 3G
    - Séparation de niveau type MLS (diode …)
      - Accessible physiquement → c'est une zone de faible protection
      - Cloisonnement horizontal : entre points de même niveau

Politique de mots de passe

- Politique de mots de passe sur tous les nœuds
  - Serveurs, stations, IHM, équipements réseau, automates, modems, VPN, bases de données, etc.
    - Modifier tous les mots de passe par défaut
    - Éradiquer les *backdoors* constructeurs
      - Compte *factory* sur les switches GarretCom, etc.

  - Éviter les mots de passe administrateurs connus et partagés par 100 personnes
  - Les mots de passe des IHM sont souvent partagés
    - On sait qui opère une console du fait des rotations de personnel
    - Mais les mots de passe système devraient être individuels et forts

Besoin de renforcement des authentification applicatives

Accès distants

- Interdire **impérativement** les IHM / automates connectés sur Internet
- Chiffrement et authentification forte sur les accès distants
  - VPN
    - Utilisateurs mobiles
    - Sites industriels satellites connectés avec un site principal
    - Sondes en sortie
    - Problème des certificats :
      - Expiration → déni de service
      - A quand un « Let's encrypt » industriel ?
  - Bastions
  - Sondes
  - Interdire sur les routeurs d'accès tout trafic hors VPN
    - **Dans les deux sens !**

- Attention aux supervisions « dans le cloud »
  - Compromission du NOC Telvent en 2012

Sécurisation des machines

- Les extrémités des réseaux sont l'ultime point de sécurisation
- On va rencontrer 3 types de systèmes
  - Automates
  - Systèmes informatiques classiques (Windows, UNIX)
  - Appareils réseau et de sécurité
- La sécurisation des automates est mal documenté
- Mais l'usage de postes « classiques » en milieu industriel a des impacts
  - Gestion des mises à jour
  - Risque de perturbation par les antivirus
  - Postes « console » sans authentification

Gestion des mises à jour

SII → Interruptions interdites

- Garder les systèmes à jour est la base
  - Bases de détection et filtrage : empreintes réseau et antivirales
  - Mises à jour système, et applicatives
  - Mises à jour de firmware réseau, automates…
  - **De plus en plus complexe : Internet requis par les produits…**
- Validation des non régressions
  - Fréquente limitations en version des OS par les équipementiers
  - Nécessite un environnement de test
  - **Rarement fait sur les équipements et logiciels anciens, voir récents.**
- Remplacement ou des technologies « mortes »
  - En particulier : Windows XP et Windows 2003 serveur
- Transfert entre les environnements
  - Nécessite des serveurs de transfert en DMZ

Stratégie de sécurisation

- Penser les mesures en fonction des menaces
  - Solutions sur l'étagère : rarement satisfaisantes
  - Exiger des vendeurs ;
    - Qu'ils démontrent l'efficacité de leurs solutions,
    - Le support sur la durée de vie des systèmes (MCO/MCS).
- **Prototyper !**
  - Monter des maquettes pour valider les choix technologiques,
  - En particulier l'interopérabilité et les impacts performance,
  - Attention aux impacts métier.
- *Basics* : les mesures d'hygiène de base
  - Établir/mettre à jour les plans d'architecture et matrices de flux
  - Durcir des systèmes et applications
  - Collecte des traces
  - Gestion les changements des mots passe
  - Restriction des sources de connexion

Conclusion

Conclusion

- Un niveau de risque élevé
  - Réalisation forte des pouvoirs publics
  - Mais évolutions rapides vers une plus forte exposition
- Pas de solution magique
  - Les solutions efficaces ne peuvent être ponctuelles
  - Adaptation nécessaire des outils du monde du SIE
    - Opportunités pour de nouveaux produits.
- Pas de raisons de baisser les bras
  - Des mesures simples peuvent drastiquement améliorer la situation
  - Les entreprises doivent demander des comptes à leurs équipementiers
- Il est urgent d'adopter une vision stratégique de la sécurité des SI industriels

Conclusion (OIV)

- Les mesures de la LPM se mettent en place
  - Plus de place laissée à la concertation qu'initialement redouté
  - Les arrêtés sectoriels devraient être issus des ateliers de concertation

- Restent de grosses inconnues
  - Calendrier de mise en conformité ?
  - Quels produits certifiés pour les OIV ?
  - Jusqu'où s'étendra le classifié de défense ?
  - Le coût de la sécurisation est-il supportable pour tous les OIV ?

Questions ?