La sécurité des systèmes d'information dans le domaine industriel.

Particularités
Les réponses possibles, bonnes pratiques

Philippe Hofmann
philippehofmann@netscape.net

Séance Grifes,
3 Mai 2005, Cern

A quoi va-t-on s'intéresser.

- **A la gestion de la sécurité logique**
- **Dans les entreprises dont le métier consiste (entre autre) à produire des biens tangibles:**
  - ⇨ processus physiques, avec des 'machines' et des 'usines'
  - ⇨ Par opposition aux entreprises qui produisent essentiellement des services: banques, administrations, etc…
- **NB:La frontière n'est pas aussi nette que cela…**
  - ⇨ "Utilities": énergie, eau,etc.
  - ⇨ Le CERN
  - ⇨ Les entreprises industrielles produisent aussi des 'services'…

Une entreprise industrielle

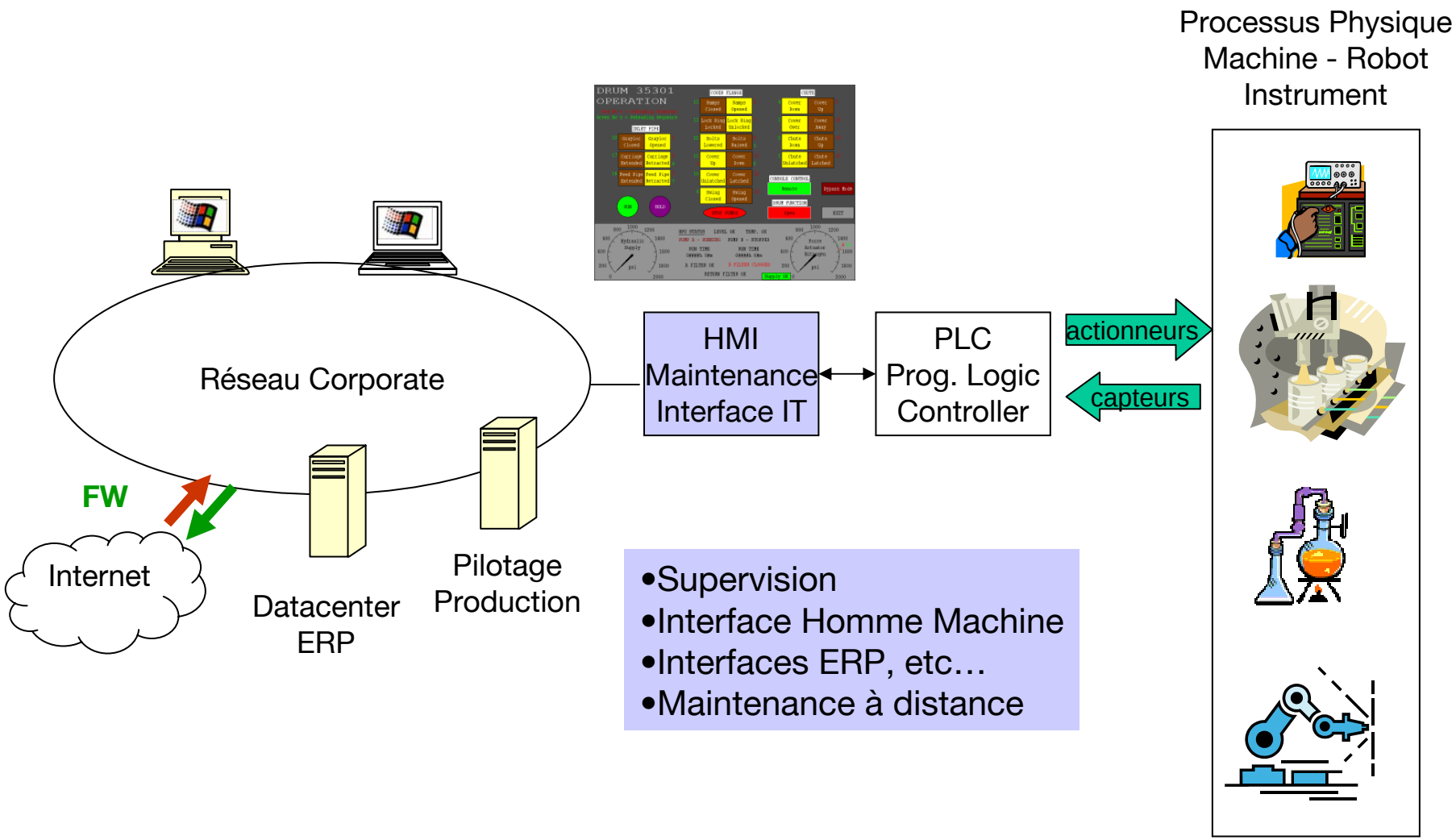
- **Des Services**
  - ⇨ Finance, RH, Communication, Marketing
  - ⇨ Ventes, études, développement
  - ⇨ Supply chain, Internet, B2B, B2c
  - ⇨ Etc.
- **Production**
  - ⇨ Usines, ateliers, centrales, laboratoires, etc.

- **Informatique**
  - ⇨ **Services**: ERP, bureautique, mail, applications métier, réseaux,etc.
  - ⇨ **Production**: automatisation au sens large:
    - systèmes de pilotage, systèmes de contrôle, machines

Pour se comprendre: quelques termes

- **« Corporate IT »:**
  - ⇨ l'ERP, la bureautique, la messagerie, les applications métiers, Internet, le B2B/B2C, etc…
  - ⇨ Gérée par "l'informatique"
- **Informatique industrielle:**
  - ⇨ Technologies IT utilisées dans des système de production (machines, robot, supervision, mesure,etc….)
  - ⇨ Généralement gérée par les spécialistes processus
- **Systèmes de contrôle de processus:** systèmes d'automatisation.
- **Usine:** laboratoires, ateliers, usines
  - ⇨ par extension, le lieu ou il y a des 'machines' et de l'informatique industrielle
- **Sécurité physique:** accès, sûreté, santé, environnement
- **Sécurité logique:** Information/IT/Cyber/Network Security

Les systèmes de contrôle: vue d'ensemble



Particularités
systèmes de contrôle de processus.

- **L'utilisation massive de technologies IT dans les processus de production**
  - ⇨ PCs, Réseau, Internet, Wireless, Accès à distance (télé-maintenance)
- **La très grande créativité des ingénieurs qui développent les systèmes de production.**
  - ⇨ 'early adopters' de nouvelles technologies IT
- **Les technologies IT sont 'embarquées' dans les systèmes**
  - ⇨ Managés par les spécialistes processus, ou par les fournisseurs
  - ⇨ Équipes IT pas systématiquement impliquées

Particularité, suite
Beaucoup de systèmes spécialisés, ‘clé en main’

- **Machines, robots, instrumentation, impression**
- **Saisie:** terminaux spéciaux, scanner code bar RF
- **Gestion** énergies, climatisation, alarmes, caméra, sûreté, etc…

- **Des systèmes très intégrés,** avec des composants IT souvent ‘exotiques’
- **Durée de vie:** proche de celle de l’outil de production
- **Des contraintes ‘légales’:**
  - ⇨ Validation FDA, pour les pharma
  - ⇨ Normes de sûreté
  - ⇨ Engagement de la responsabilité du fournisseur

Particularités, suite
Organisation du travail

- **Sûreté et efficacité priment sur la sécurité logique**
- **Utilisateurs pas nécessairement identifiés individuellement**
  - ⇨ Pas enregistrés comme utilisateurs informatiques
  - ⇨ Succession rapide de personnes sur un poste informatique
  - ⇨ Mouvement du personnel: remplacement, etc.
- **Contraintes liés au temps de travail et au planning**
  - ⇨ 7x24, arrêts pour maintenance planifiés a long terme
  - ⇨ Autonomie électrique du matériel mobile
- **Conséquences:**
  - ⇨ Gestion des accès: la règle « un utilisateur une session» ne fonctionne pas
  - ⇨ Mesures standards souvent inapplicables: screenlock, changement de mot de passe (pas de clavier…), MS Patch Wednesday, WEP/WPA
  - ⇨ Standards InfoSec incompatibles avec la production
- **Mais niveau de sécurité physique élevé: badges, garde, etc.**

Particularités, suite
sensibilité aux risques élevée, mais différente

- **En général, très grande sensibilité aux risques ‘tangibles’:**
  - ⇨ Sûreté, environnement, santé, fiabilité, accès physique
  - ⇨ Doubler/tripler un équipement, ou un contrôle est naturel.
- **Moindre sensibilité aux risques IT dans l’environnement ‘usine’**
  - ⇨ Les risques IT ont des impacts sur les usines que depuis peu.
  - ⇨ Le réseau, c’est un câble comme une autre (pas de danger…)
  - ⇨ Mettre un firewall dans une usine n’est pas encore naturel…
- **Souvent des équipes / langages / cultures différents**
  - ⇨ **Spécialiste process**: fiabilité, PLC, machines, analogique, capteurs,
  - ⇨ **Spécialiste IT**: réseau, PC, TCP/IP, firewall, virus, etc…
  - ⇨ Siemens/Rockwell/Johnson Control versus Microsoft/Cisco/IBM/HP …

Similitudes: gestion de la sécurité « corporate IT »

- **Les priorités dépendent du profil de risque de l'entreprise.**
  - ⇨ Propre à chaque entreprise.
  - ⇨ **Indépendamment de son secteur économique** (secondaire ou tertiaire).

  - ⇨ Infrastructure, données, applications, systèmes, internet, B2B, B2C, etc…

  - ⇨ **Confidentialité**: propriété intellectuelle, données clients,…
  - ⇨ **Intégrité**: conformité des données, non altération,…
  - ⇨ **Disponibilité**: fiabilisation, plan de secours, sauvegardes, etc…

- ***Note: Je ne suis pas d'accord avec l'affirmation généralement admise:***
  - ⇨ *La Confidentialité est plus importante pour le tertiaire*
  - ⇨ *La Disponibilité et l'Intégrité sont plus importante dans le secondaire.*

Les systèmes de contrôle de processus
Évolution, nouveaux risques

Évolution des systèmes de contrôle et de supervision de processus

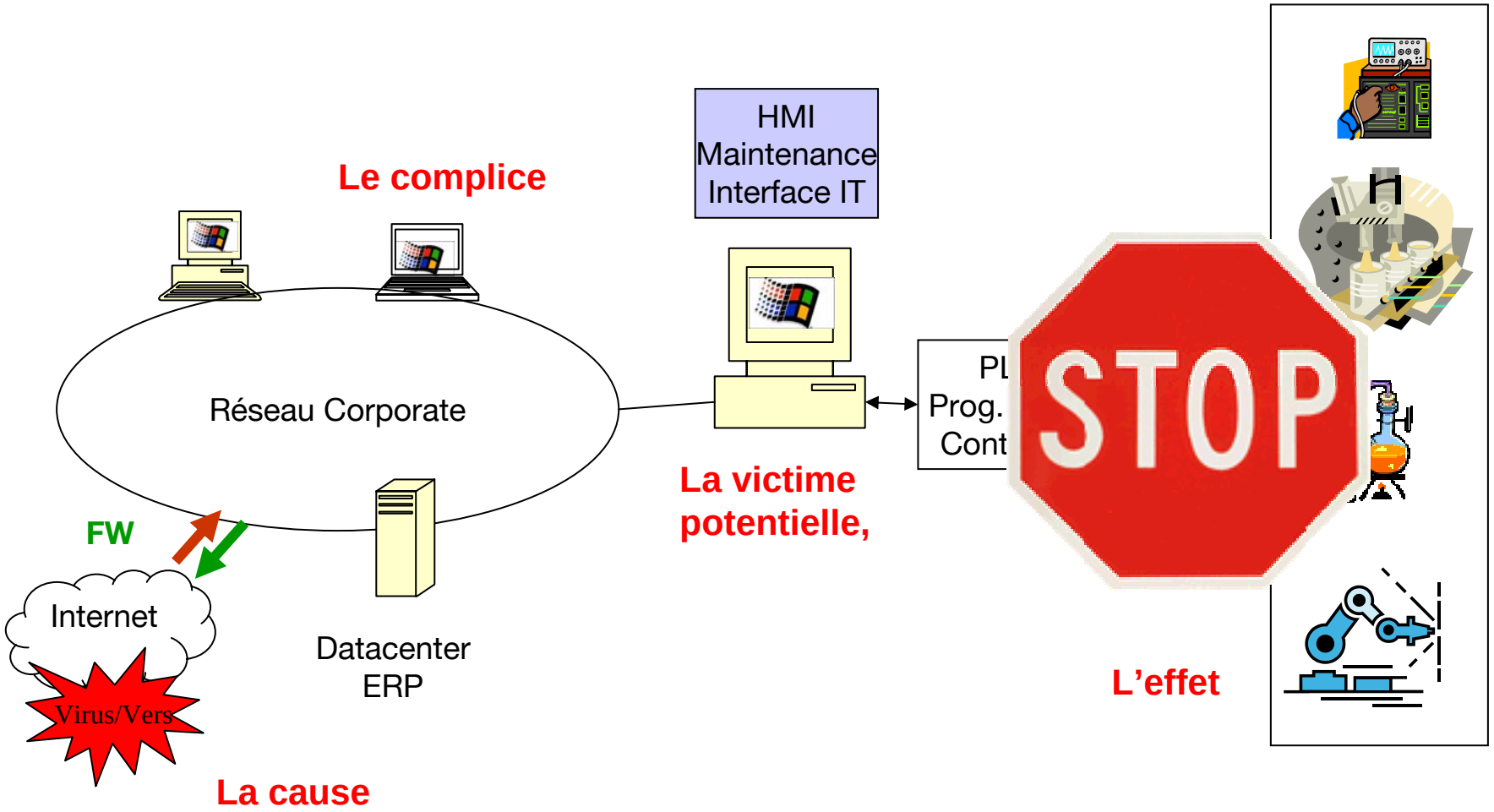
Historiquement

- **Standalone ou réseau séparé**
- **Hardware propriétaire**
- **Syst. expl. Propriétaire**
- **DOS / Windows 3 / NT4**
- **Réseaux propriétaires**
- **Système ‘fermé’**
- **Maintenance par modem en mode terminal**
- **Fiable par design**

Aujourd’hui

- **Échange des données avec IT**
- **PC (standard ou exotique)**
- **Microsoft**
- **Windows 2000, XP**
- **TCP/IP Ethernet Wired/Wireless**
- **Système ‘ouvert’**
- **Remote access par réseau (tout est possible…)**
- **Fiabilisation par modification de la configuration logicielle.**

Système de contrôle
Les risques: technologies ‘virus compatibles’



Les nouvelles menaces

- **Depuis 2003: le ‘Grid’ des virus….**
  - ⇨ Windows 2000, XP
  - ⇨ Blaster, Welchia, etc…
  - ⇨ ADSL, 100 millions de PC domestiques ‘virus compatibles’ en ligne
  - ⇨ Fulgurance des ‘attaques’
- **Effet boule de neige**
  - ⇨ Il suffit d’un seul PC infecté dans un bureau
    - Un consultant, un visiteur, un fournisseur, avec un pc portable
  - ⇨ Le pc portable infecté va silencieusement scanner le réseau.
  - ⇨ Dès que plusieurs autres PC vulnérables sont infectés, cela va très vite….
  - ⇨ Conséquences diverses et souvent sérieuses:
    - Inondation réseau, applicatifs en panne, perturbation de la production.

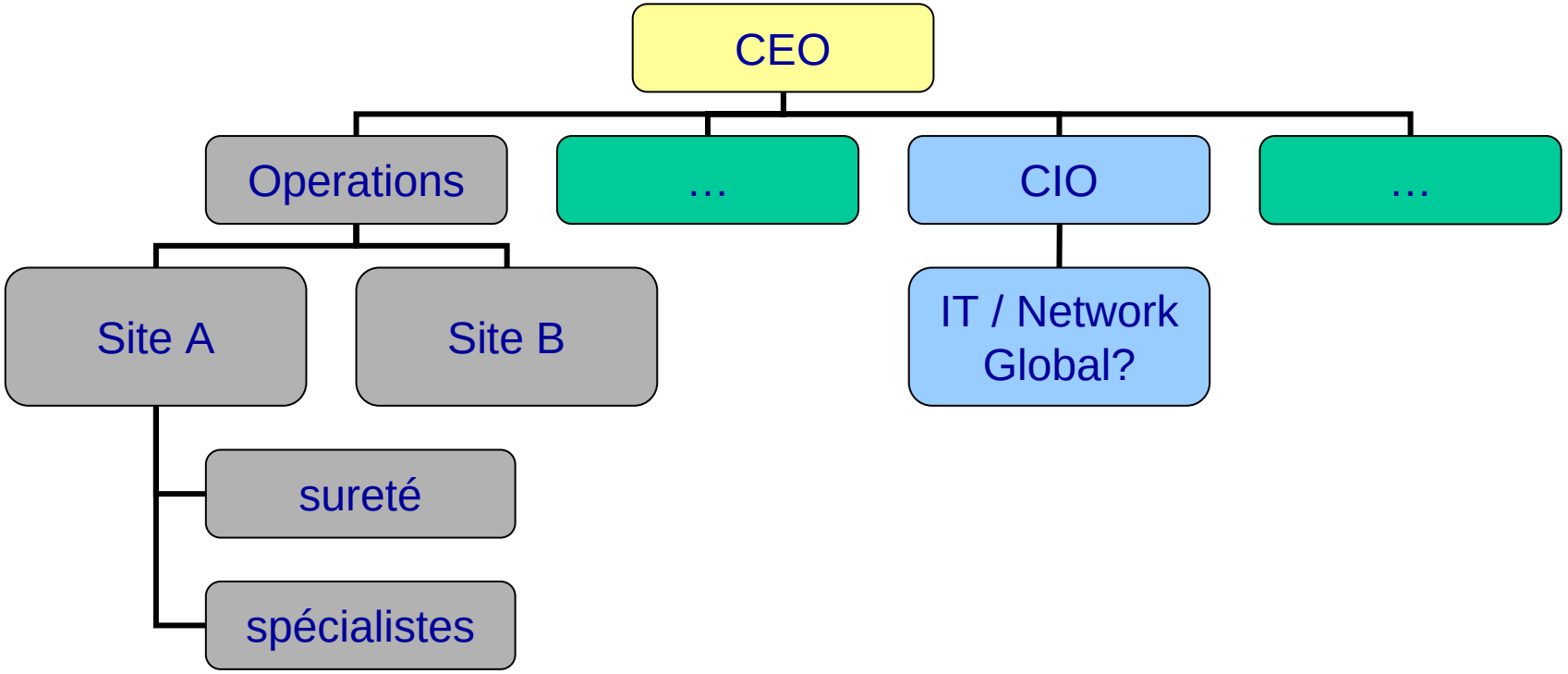
Les défis de la sécurité dans le milieu industriel: En résumé

- **Des technologies IT utilisés dans les 'usines'**
  - ⇨ Mêmes vulnérabilités que dans le « Corporate IT »
- **Des contraintes fortes**
  - ⇨ Systèmes clés en main
  - ⇨ L'organisation du travail
- **Une culture différente.**
  - ⇨ Des équipes différentes.
- **En plus des défis liés à la sécurité « Corporate IT », communs à toutes les entreprises….**

Les solutions sécurité ‘corporate IT’ sont-elle applicables?

	« Corporate IT »	Contrôle de processus.
Protection: Anti-virus/ firewall / etc…	Utilisé	Souvent difficile à utiliser
patching	Possible/fréquent	Rare, sous contrôle du fournisseur
Durée de vie	3-5 ans	5 - 10 ans et plus.
Arrêt pour Maintenance	Possible/quotidien.	Difficile/Rare
Scanning de vulnérabilité	Utilisable	Dangereux
Responsables	Convaincus	Moins convaincus… Autres priorités

Organisation



Que faire?

- **Les menaces liées au réseau ont un impact potentiel sur l'informatique industrielle**

- **Les pratiques et solutions de sécurité qui s'appliquent bien dans le domaine 'corporate IT' ne sont pas toujours adaptées**

Réponses possibles.

Principes généraux

- **Les technologies de sécurité ne vont pas tout résoudre**
  - ⇨ Sensibilisation, inventaire, directives, procédures,
  - ⇨ Les technologies doivent aussi s'adapter
- **Il faut travailler ensemble: IT & spécialistes processus.**
- **Support du management de la production**
  - ⇨ Parler en terme de risques 'production', pas en terme IT.
- **Pragmatisme**
  - ⇨ Favoriser les solutions **simples**.
  - ⇨ Favoriser les '**Quick-Wins**'
  - ⇨ Surfer sur les 'petits incidents', vous avez ***6 mois***…

Principes généraux, suite
Attention aux particularités de l'informatique industrielle.

- **Exemples**
  - ⇨ Antivirus:
    - Quand, le scan hebdomadaire.
    - Silencieux, la fenêtre d'alerte ne peut pas être réduite (pas de souris…)
  - ⇨ Le WIFI:
    - WEP/WPA/802.x n'est pas forcement disponible sur les équipements
    - Consommation électrique des équipements mobiles, pas de standby.
  - ⇨ Mot de passe: et si il n'y a pas de clavier?
- **Ne pas imposer les politiques/standards sécurité IT aveuglement.**
  - ⇨ Étudier le risque réel
- **Concevoir ensemble des solutions simples, en 'couche'.**
  - ⇨ Accepter l'imperfection… (difficile pour des ingénieurs…)

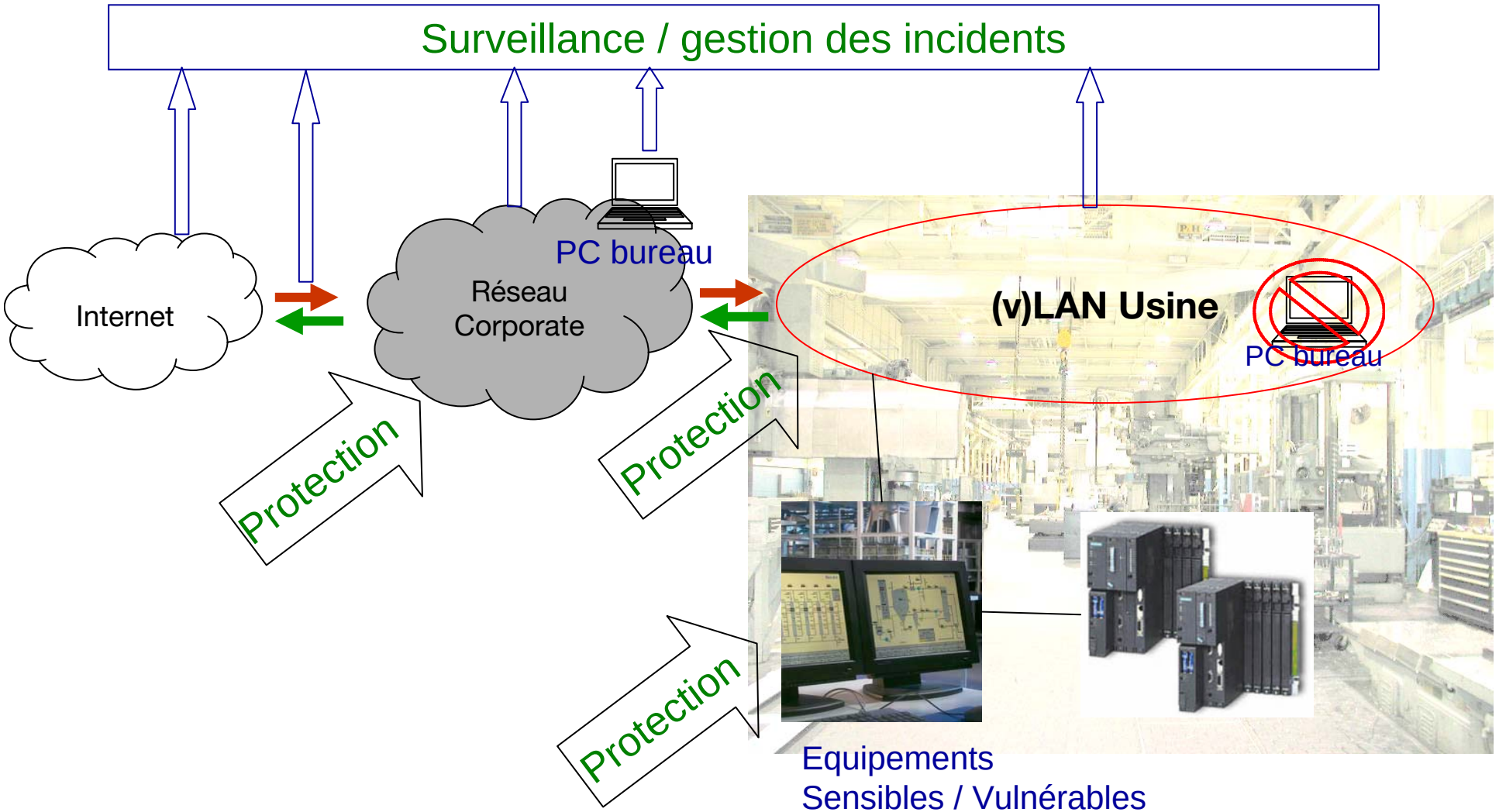
Principe généraux, suite

- **Etre ‘flexible’…**
  - ⇨ Politiques de mots de passe, timeout session, de userID, doivent être adaptées à l’organisation du travail.
  - ⇨ Accès à distance: respecter des contraintes.
- **Sinon,**
  - ⇨ Les règles seront contournées
  - ⇨ Le RSSI perd sa crédibilité…
- **Mais aussi proposer des ‘contreparties’ pour réduire le risque.**
  - ⇨ Spécialiser les postes: une seule application.
    - Pas de bureautique (IE, Office, Outlook) si poste non ‘conforme’
  - ⇨ Restreindre les UserID ‘anonymes’ à un poste.
  - ⇨ Allumage manuel d’un modem…
  - ⇨ Autre exemple: WIFI ouvert, mais 1 port seulement, FW ou ACL sur le switch, monitoring, sensibiliser aux risques.

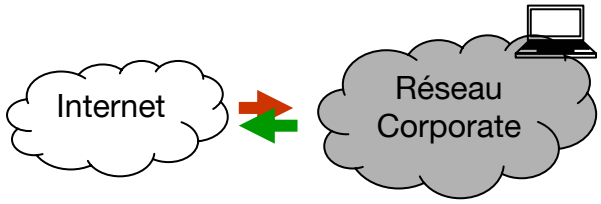
Sécuriser les systèmes de contrôle de processus: « *Defense in depth* », une sécurité en couche.

- **On peut/doit agir à plusieurs niveaux: 6 axes de défense.**
  - ⇨ Rendre le réseau corporate ‘moins’ dangereux, le rendre ‘étanche’
  - ⇨ Protection du équipements vulnérables (PC sous Windows…)
  - ⇨ Isolation/filtrage du réseau local ‘usine’
  - ⇨ Monitoring: détection rapide des menaces
  - ⇨ Gestion efficace des incidents
  - ⇨ Influencer le futur
- **Si chaque défense élimine 80% des risques (impact ou probabilité)**
  - ⇨ 1 couche: 20% de risque résiduel, 2 -> 4%, 3 -> 0.8%
- **Commencer par les Quick-wins, mêmes imparfaits.**

Dans un monde idéal…

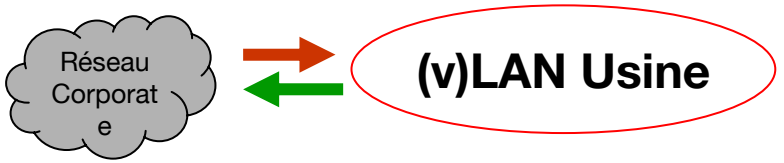


Le réseau Corporate



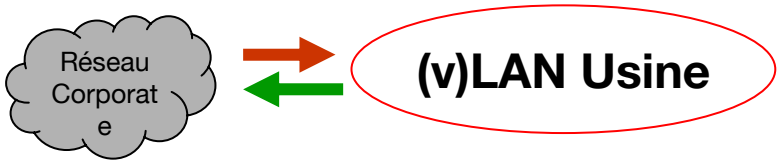
- **Objectif:** rendre le réseau ‘corporate’ étanche.
- **Selon l’organisation, les compétences, les moyens:**
  - ⇨ Contrôler les accès au réseau: 802.x, Mac @, vérification de Conformité
  - ⇨ Politique de correction de vulnérabilités, inventaire, scanneur de vulnérabilité
  - ⇨ Télédistribution: standardisation des configurations
  - ⇨ Élimination des logiciels ‘dangereux’/non standards: MSN, p2p, Outlook…
  - ⇨ Sensibilisation des utilisateurs.
- **Internet:**
  - ⇨ Filtrage Internet (contenu des flux 80…)
- **Les laptops:**
  - ⇨ **Politique *draconienne* si connectable sur Internet.**
  - ⇨ FW personnel, patch, Tunnels IPsec, configuration ‘fermée’
- **Et bientôt: les PDA, smartphones, etc…**

Protection du réseau Usine.



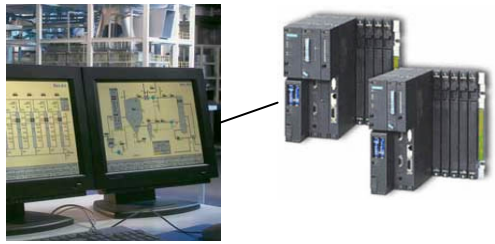
- **Objectif:** isoler les équipements sensibles sur un réseau séparé.
- **Les questions à se poser:**
  - ⇨ **Réseau Physique**: câblage, switchs, VLAN?
  - ⇨ **Protocoles?** Seulement TCP/IP?
  - ⇨ **Quels équipements sur le LAN usine**
    - Pas de bureautique et de PC ‘bureau’?
    - Seulement les PC impossibles à protéger?
  - ⇨ **Les flux entre les systèmes de contrôle et le « Corporate IT »**
    - Documentés?
    - Est-il concevable de les documenter, manuellement/automatiquement
    - Avez vous accès aux équipes qui développent

Protection du réseau Usine Suite



- **Le choix d'un mécanisme de filtrage / granularité du filtrage**
  - ⇨ ACL dans un switch/routeur, Firewall
  - ⇨ Intrusion Prevention System
    - Boite 'magique' qui analyse le trafic et qui 'bloque' les flux 'illégitimes'
    - Faux positifs….
- **Management:**
  - ⇨ Organisation/responsabilité: centrale, régionale, locale, nb de sites.
  - ⇨ Ressources/Compétences: qui sait faire – qui sait ce qu'il faut faire
  - ⇨ Gestion des changements
  - ⇨ Problème de la télémaintenance des équipements / Piquets
- **Conclusion:**
  - ⇨ La meilleure protection, mais la plus complexe à mettre en oeuvre sur un existant.
  - ⇨ Plus simple sur de nouvelles installations.

Protection des PC ’contrôle de processus’



- **Inventorier – catégoriser – décider - budgéter**
- **Mettre en conformité avec les standards sécurité quand c’est possible**
  - ⇨ AV, télédistribution, patching
  - ⇨ Montrer l’aspect réduction des coûts à moyen terme.
- **Pour les solutions ‘in-house’,** essayer de concevoir une configuration OS commune (master), avec la sécurité gérée (AV-pFW-Patches-Hardening).
- **Gérer les ‘exceptions’**
  - ⇨ Réseau ‘usine’
  - ⇨ Travail avec les fournisseurs
  - ⇨ Plus l’OS est vieux, mieux c’est. (Dos, Win3, Nt4 ~OK)
  - ⇨ Politique de sécurité: fixer des objectifs
  - ⇨ Prise en compte des maintenances OS dans les plans de maintenance usine

Monitoring activité réseau

- **Objectif: détecter au plus vite les ‘anomalies’**
- **Selon l’organisation, les compétences, la topologie du réseau, les moyens:**
  - ⇨ IDS ou « Intrusion Prevention System » en mode passif
  - ⇨ Solution de monitoring réseau avec analyse ‘layer 7’
    - Repérer les profils de trafic inhabituels
  - ⇨ Gestion des logs: efficace, mais peu de solution packagées.
    - Firewall Internet
    - Logs AntiVirus
    - Logs Netflow (CISCO)
- **Il faut faire quelque chose**
  - ⇨ Nécessaire en cas de problèmes

Gestion des incidents

- **Objectif: Protocole de gestion des incidents réseaux**
  - ⇨ Connu, personnel formé, autorité pour agir.
  - ⇨ La vitesse de réaction est critique.

- **Trouver:** identifier physiquement l'équipement.
- **Déconnecter:** manuellement ou automatiquement (pas facile…)
- **Analyser:** Que se passe-t-il
- **Corriger et vérifier**
- **Reconnecter**
- **Rapport:** essentiel pour identifier des scénarios nouveaux.

Influencer le futur

- **Objectif: faire prendre en compte les risques IT et les solutions par les équipes métier.**
- **Pistes possible:**
  - ⇨ Participer aux analyses de risque
  - ⇨ Architecture
  - ⇨ Travailler avec les achats techniques ou le département légal sur des clauses contractuelles avec les fournisseurs.
  - ⇨ Sensibiliser.
    - La commoditisation du hardware et du logiciel: des coûts cachés…

Une note personnelle

- **Attention à maintenir une “techno-diversité”**

  - ⇨ Tout IP?
  - ⇨ Tous connectés?
  - ⇨ Tout Microsoft?
  - ⇨ Une ‘masse critique’ qui peut ‘diverger’…

Conclusion

- **La différence majeure: l'informatique industrielle en plus**

- **Une approche différenciée, collaborative et pragmatique pour adresser la sécurité logique de l'informatique industrielle.**

Merci!