(Pas de) Sécurité des systèmes de contrôle !?

…concernant le besoin d'une sécurité industrielle

Dr. Stefan Lüders (CERN IT/CO)

Les Séances de Groupe Information et Sécurité (GRIFES)

6 Mars 2007


Contenu

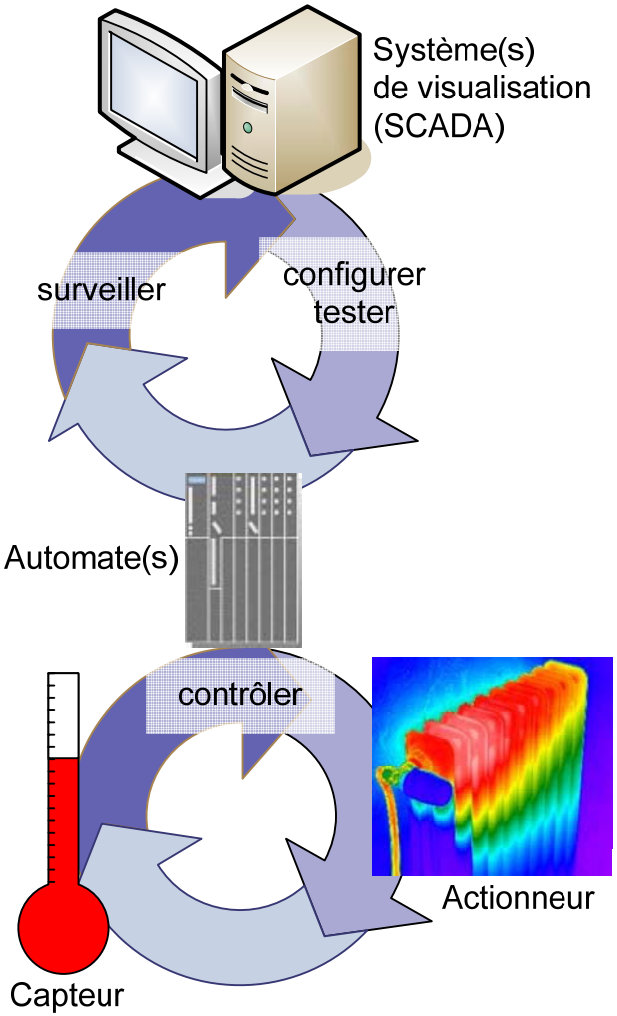
Le Passé:
La (r)évolution des systèmes de contrôle

Le Présent:
Pas de Sécurité !?

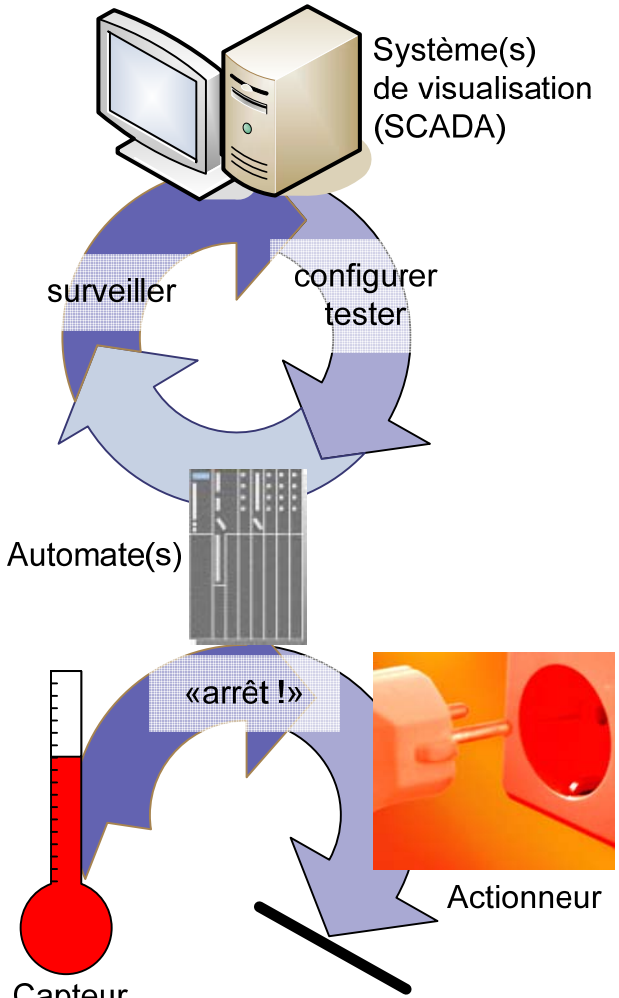
Le Future (!):
Une solution c'est «Defence-In-Depth»


«Contrôle» & « Sûreté»

Système de Contrôle



Système de Sûreté




Systèmes de contrôle…

Systèmes de contrôle utilisés partout:

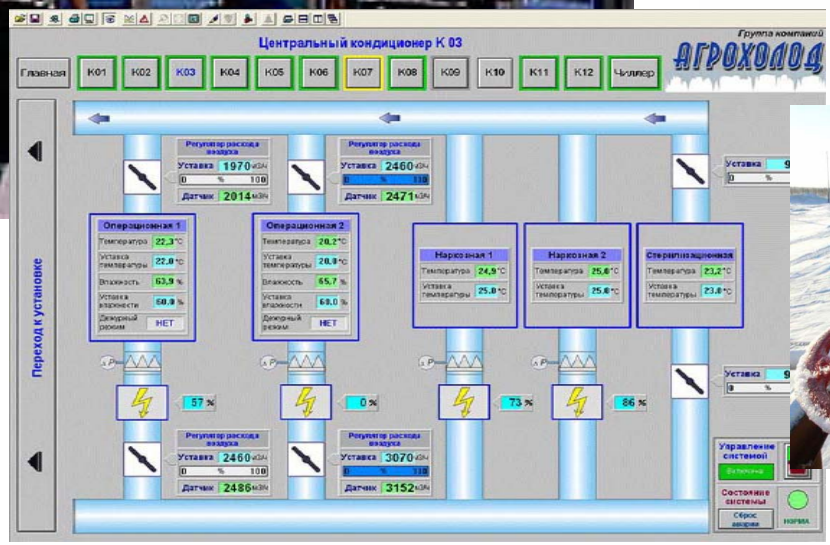
- Dans les secteurs
  électricité, transport, fioul & gaz, pharmaceutique, production…
- Dans la production
  automobiles, avions, vêtements, …
- Dans les supermarchés (p.ex. balances)
- Pour le gestion des bâtiments (électricité, distribution d'eau, d'air, …)

Aujourd'hui la perte de contrôle pourrais devenir critique:

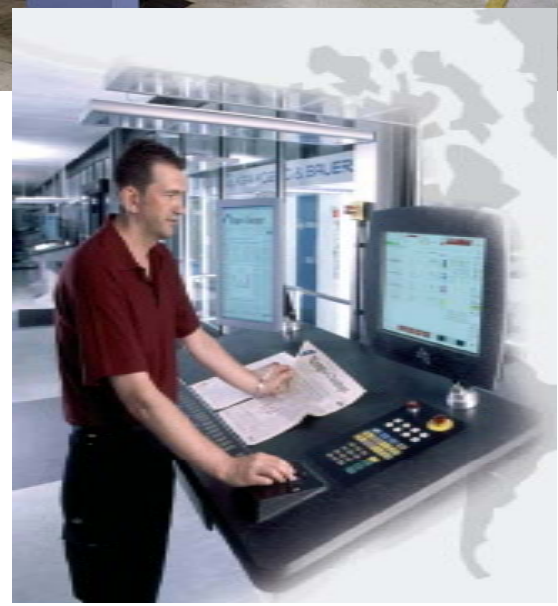
- Cause des perturbations significatives dans ces secteurs…
- Traitement spécial par les instances officielles

Critical Infrastructure Protection (CIP)

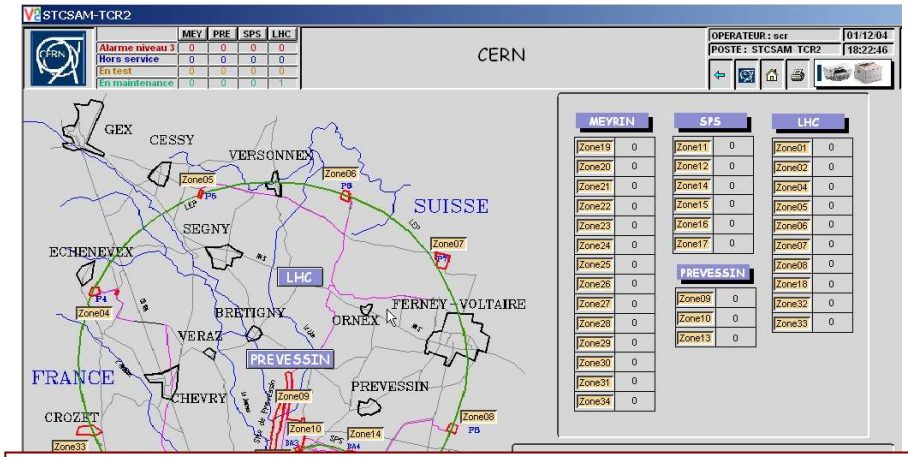
…dans l'energie

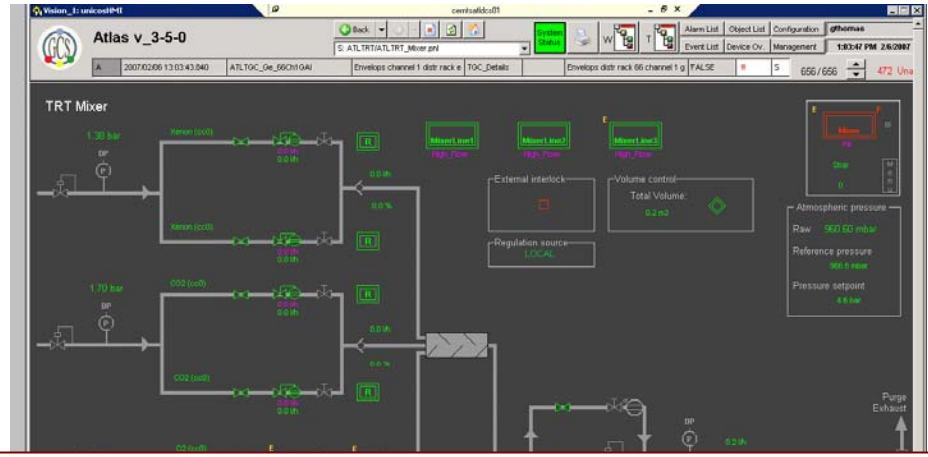


…à l'imprimerie

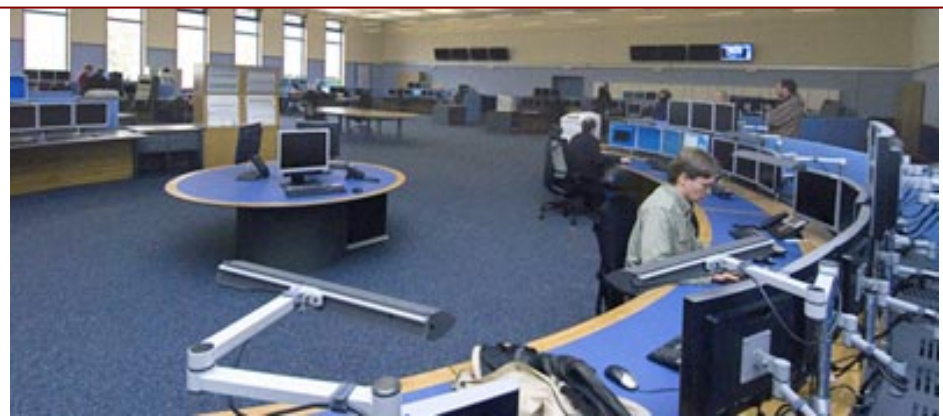


…au CERN

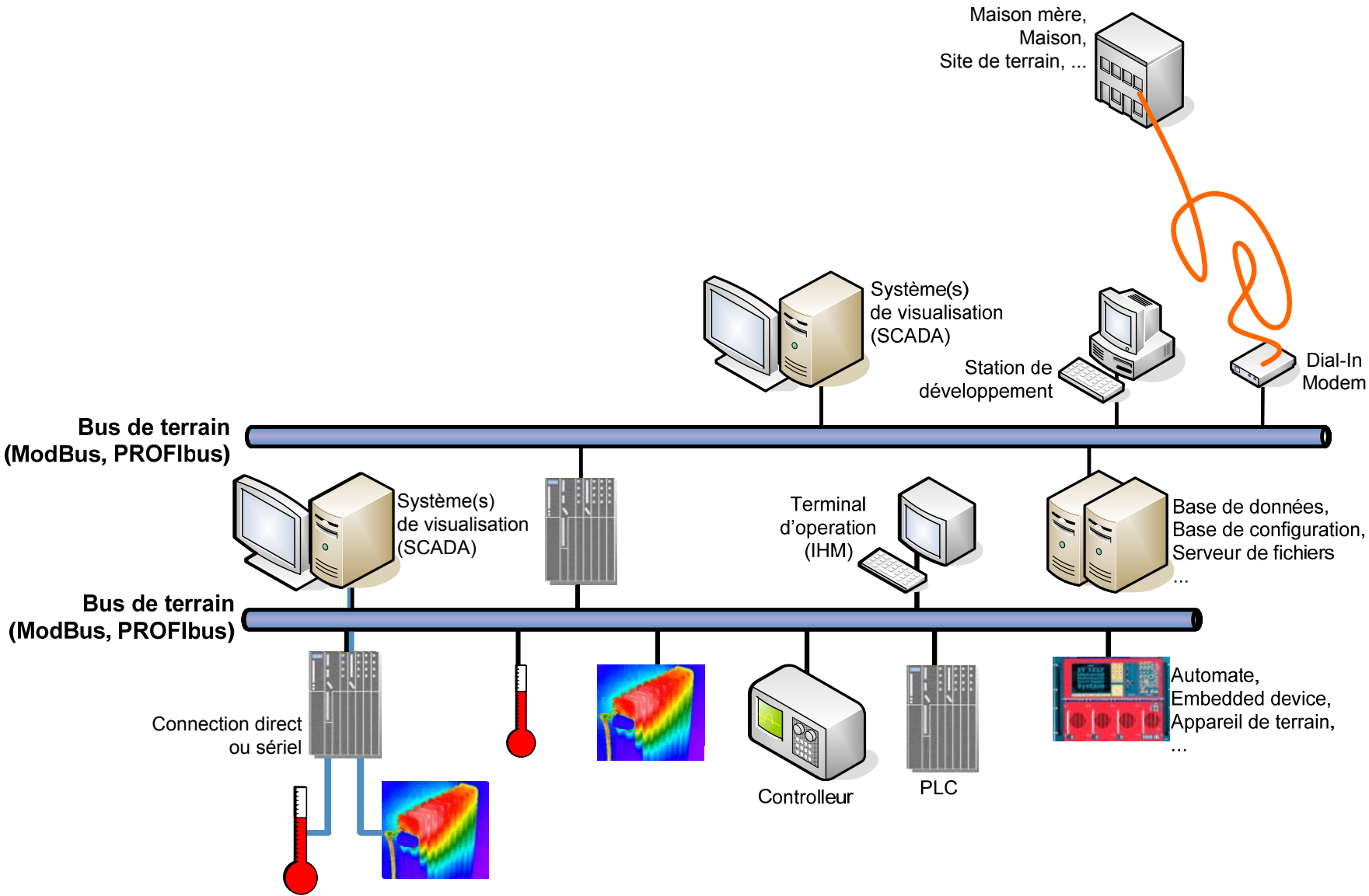




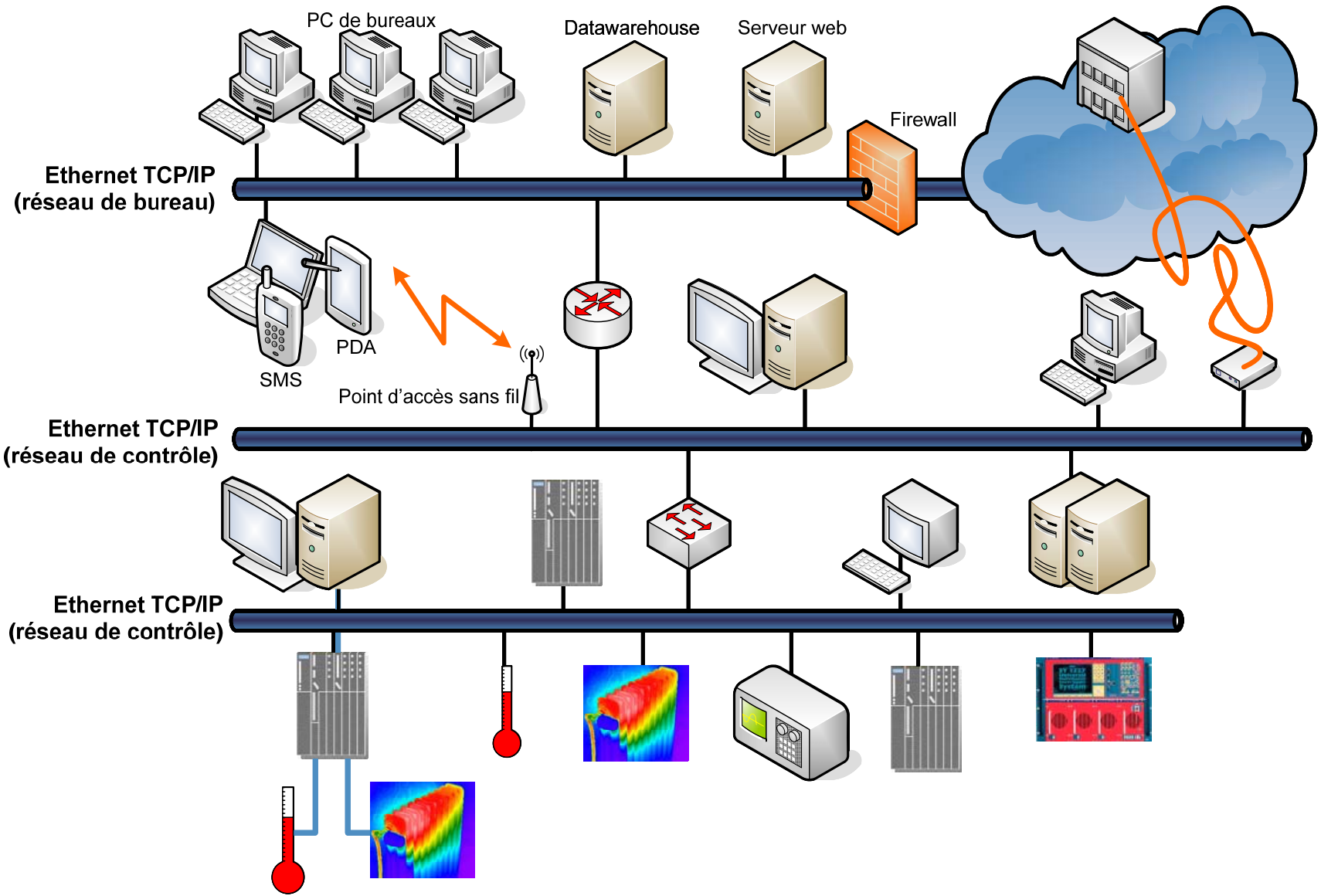
Il y a env. 120 systèmes de contrôle au CERN.




(R)Evolution: Le passé




(R)Evolution: Le présent




«Contrôles» fusionnent avec l'IT

Réseaux de contrôle fusionnent avec ces de business

- Bus de terrain propriétaire remplacés par Ethernet & TCP/IP
- Équipements connectés directement sur Ethernet & TCP/IP
- Applications en temps réel basées sur TCP/IP
- Connections VPN à partir de l'extérieur sur le réseau de contrôle

Utilisation des protocoles IT et de gadgets

- SNMP, SMTP, FTP, Telnet, HTTP (serveur web), WWW, …
- Points d'accès sans fil & transmission de données sans fil
- Ordinateurs portables, clé USB, cameras web, …

Migration sur une plateforme Windows de Microsoft

- MS Windows n'est pas fait pour les systèmes industriels / de contrôle
- OPC/DCOM utilise le port 135 (utilisé également pour RPC)


«Contrôles» ce n'est pas IT ! (1)

	«IT de bureau»	«Contrôles»
Temps cycle de système	3 – 5 ans	5 – 20 ans
Disponibilité	interruptions planifiées OK	24 / 7 / 365
Confidentialité	élevée	basse
Temps critique	retards tolérés	critique
Changements	fréquents, formalisés et coordonnés	rares, informels et pas toujours coordonnes
Outils automatisés	utilisés fréquemment	limitées, utilisés prudemment (besoin des procédures de test)
«Hosting»	parfois externalisé	toujours local


«Contrôles» ce n'est pas IT ! (2)

	«IT de bureau»	«Contrôles»
Connaissance de sécurité	existe	normalement bas
Firewalls	fréquent	lent ou pas possible
Détection d'intrusion	standard	pas de ficher de signature pour ce trafic…
Trafic de données	Active Directory, scans de sécurité…	charge additionnel à éviter
DHCP	standard	adresses IP fixées dans la configuration hardware
Utilisation de «sans fil»	fréquent	en expansion


«Contrôles» ce n'est pas IT ! (3)

	«IT de bureau»	«Contrôles»
Mis à jour de PCs	fréquent	lent ou pas possible (tests extensives, besoin d'une bande de réseau large)
Antivirus SW sur PC	standard	rarement ou pas possible (scan bloque CPU)
Redémarrage	standard	rarement ou pas possible (arrêt du processus)
Changement de	standard	rarement ou pas possible

Si ce n'est pas cassé — ne touchez à rien !


Le Passé:
La (r)évolution des systèmes de contrôle

Le Présent:
Pas de Sécurité !?


Le monde d’hier…

Beaucoup de systèmes construits «pré-Internet»

- Sûreté toujours pris en compte, mais pas la sécurité
- Sécurité très difficile à intégrer après

Aujourd’hui: Un environnement interconnectable

- «Hard on the outside, soft in the middle» (approche «M&M»)
- Mesures protectives se concentrent
  aux bordures mais pas aux éléments internes du système…

Les bordures deviennent de plus en plus vulnérables

- Inter connectivité et le désire d’avoir un accès à distance
- Confiance au IT
- Augmentation du risque liés aux dommages collatéraux


Le risque

Risque = Vulnérabilité

× Menace

× Conséquence




Vulnérabilités techniques

Systèmes sans protection attaqués

- Systèmes non patchés: OS & applications
- Absence de logiciel d'anti-virus ou de fichier de signatures de virus
- Pas de protection par un firewall local

«Zero Day Exploits»: trous de sécurité sans patches

- Intrusion avant un patch et/ou anti-virus signature est disponible
- Vers se diffusent en quelques secondes

*…mais **comment mettre à jour** des PCs de contrôle ?*

*…**que faire avec des logiciels anti-virus** & firewalls locaux?*


Vulnérabilités humaines

L'homme devient l'élément le plus faible

- Utilisation de mots de passe simples
- Ordinateurs portables / clés USB / … infectés
  sont portés physiquement sur site et sont connectés
- Utilisateurs téléchargent «malware» et ouvrent pièces jointes piégées
- Utilisateurs installent des logiciels prohibés, jeux, P2P, …

Mots de passe connus de plusieurs personnes

- Pas de traçabilité, donc pas de responsabilité
- Manque/défaut/simple mot de passe dans les logiciels

*…comment **restreindre un PC d'opération ?***

*…et comment traiter des **comptes d'opérateur ?***

*…et **fixer des directives pour les mots de passe ?***

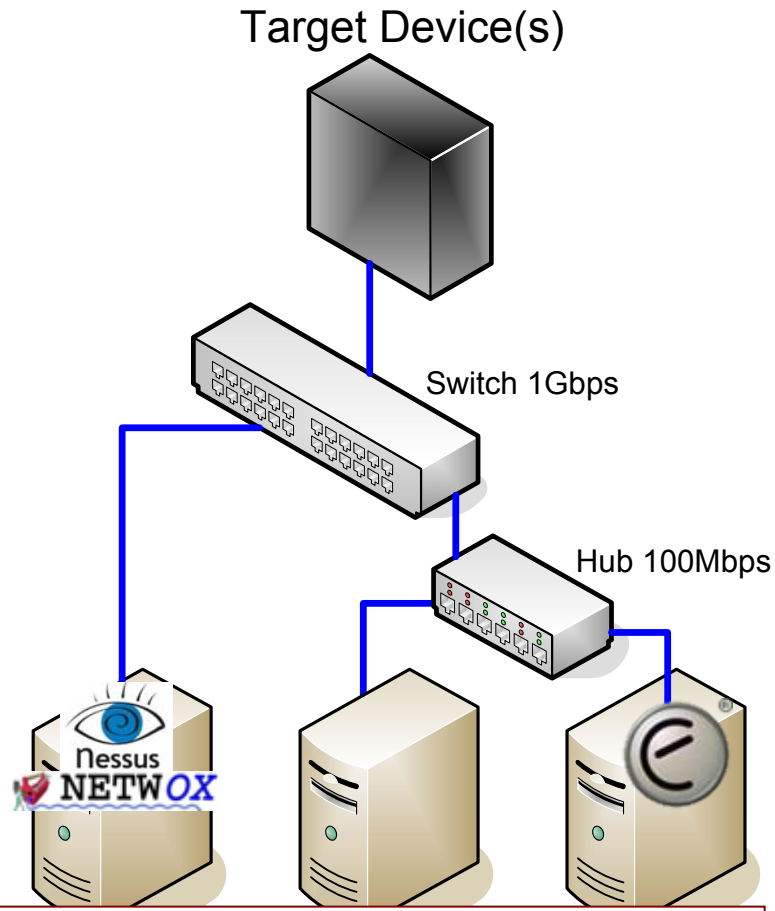

Banc de test «TOCSSiC»

Automates industriels sans mécanisme de protection

- PLC, appareils de terrain, alimentations, …
- Sécurité non incluse

Création de «Teststand On Controls System Security at CERN» (TOCSSiC)

- Scanner de vulnérabilités «Nessus» (utilisé au IT de bureau)
- Attaque DoS avec «Netwox»

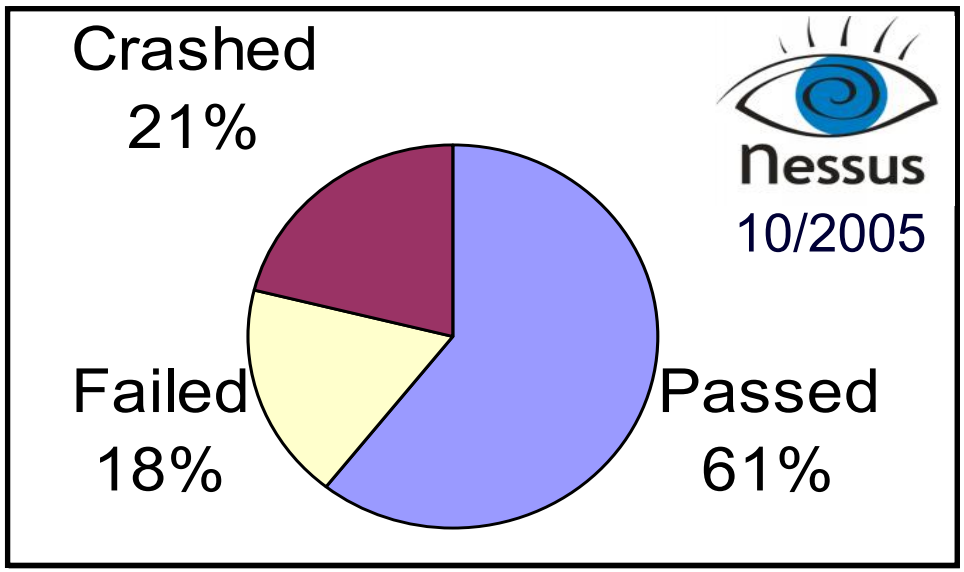


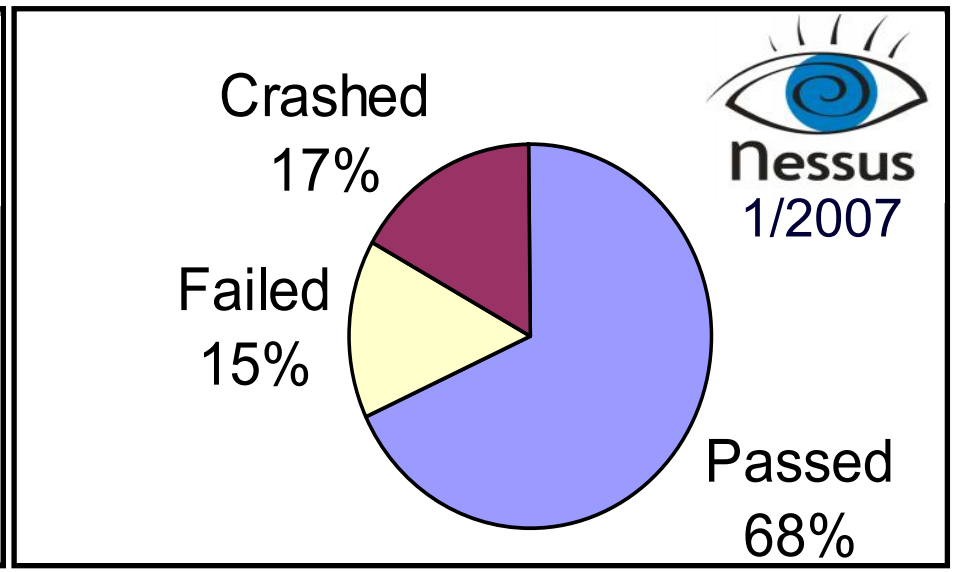
Pourquoi faire compliquer quand on peut faire simple ?


TOCSSiC: PLC attaqué !

31 appareils de 7 fournisseurs différents (53 tests au total)

Tous sont configurés proprement (sans processus de contrôle)

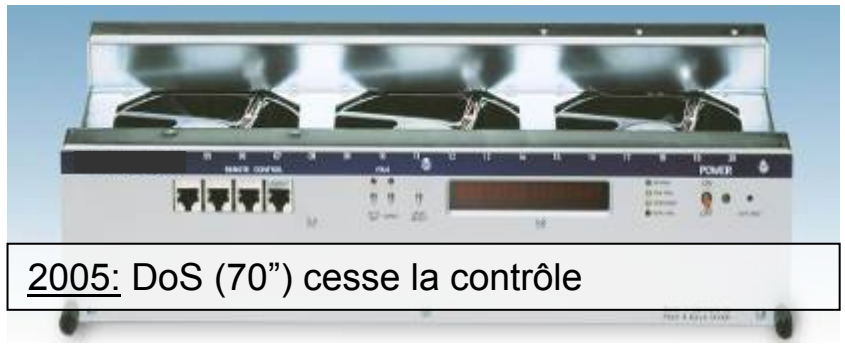




…PLCs en production ***défaillissent plus souvent !!!***

*…**Les résultats s'améliorent** avec les versions de firmware plus récent* ☺


Résultats de TOCSSiC (1)



2005: DoS (70”) cesse la contrôle

- **L’appareil plante**
  pendant le réception de requêtes spéciales non-conformes

  …Violation de standards TCP/IP !!!

- **Serveur «ModBus» plante** pendant le scan de port 502

  …Ces protocoles sont bien documentés («Google hacking») !

Résultats de TOCSSiC (2)

- **Serveur FTP offre une plateforme d'attaque**
- **Serveurs FTP & Telnet plantent**
  par des commandes / paramètres très looooooongs

  …les deux sont des protocoles anciens sans cryptage !

- **Server HTTP plante** par des URL très looooooongs
- Serveur HTTP permet **«directory traversal»**

  …qui a demandé un serveur web & eMail sur un PLC ?

- **Les «community names» de SNMP sont fixés par «public» & «private»**

  …ces noms doivent être configurables !


Résultats de TOCSSiC (3)

▶ PLCs sont sans défense

- **Arrêts possible sans problèmes**
  (...il y a Google…)
- Mots de passe non cryptés
- PLCs éventuellement sans identifiant

…Autorisation, vérification d'intégrité de données et cryptage doivent être obligatoires !

▶ PLCs *vraiment* sans défense

- Services (HTTP, SMTP, FTP, Telnet, …) non désactivable
- Pas du firewall local

… Isolation de la configuration par défaut !!!


Suivi des résultats TOCSSiC

Discussion avec les fournisseurs concernés

- Reconnaissance seulement après beaucoup de persuasion
- Maintenant, ils font aussi des tests «Nessus»

…Les résultats s'améliorent avec les versions de firmware plus récent ☺

Retransmission et coopération

- …Avec des instances officielles
- …Médiation par les fournisseurs concernés au tiers

CPNI Centre for the Protection of National Infrastructure

Bundesamt für Sicherheit in der Informationstechnik

Nutzfahrzeuge

DESY

Présentations aux industriels

- Discussions sur les «Demandes de Sécurité Industrielle de Systèmes de Contrôle»

PLCopen for efficiency in automation

ZVEI

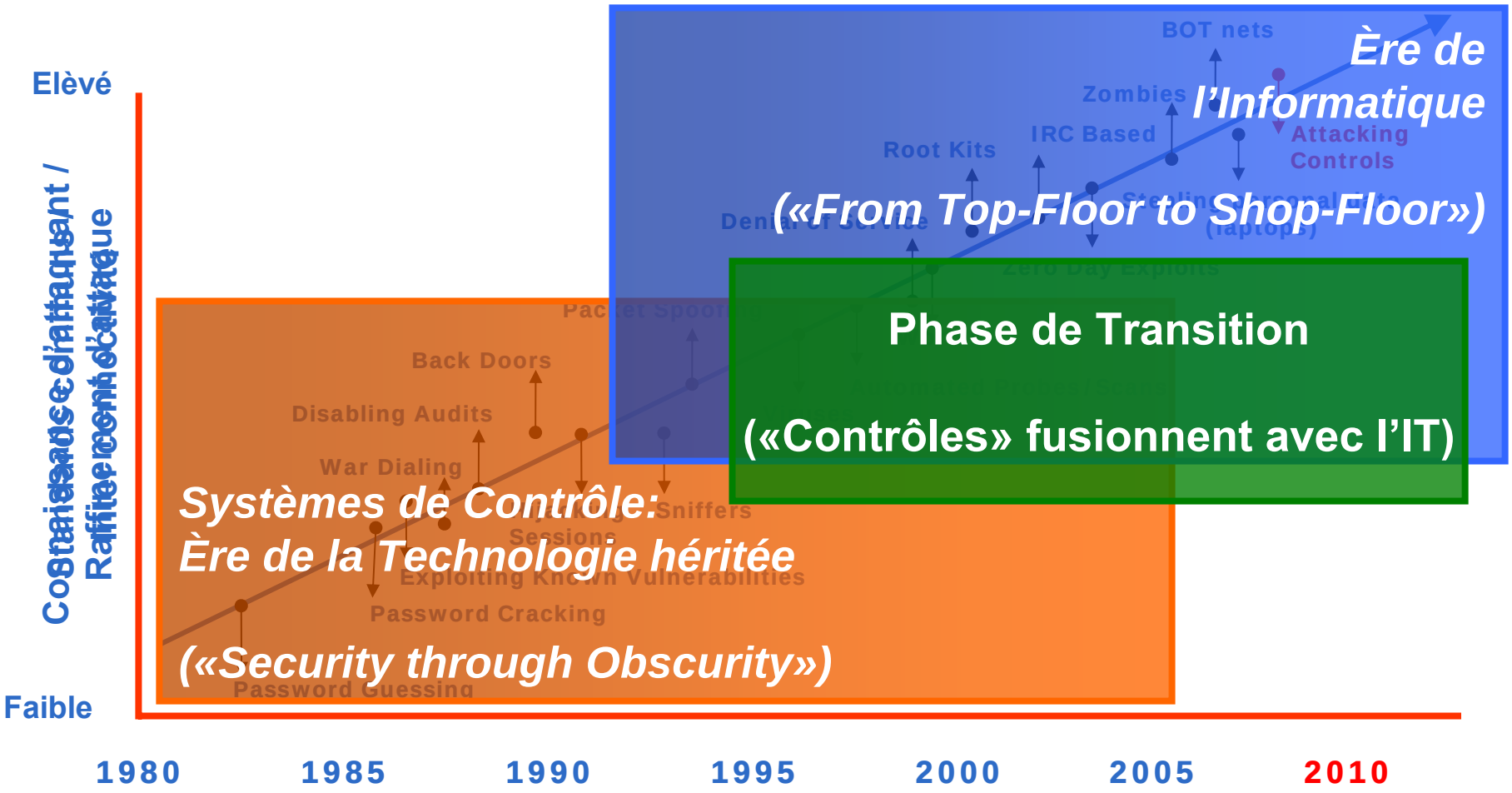
…cependant beaucoup d'ignorance («Il n'y a pas de demande»)


Le facteur «Menace»

Risque = Vulnérabilité

× Menace


Menaces cyber — Péril actuel




Conscient ou paranoïaque ? (1)

"….Gazprom, a state-run gas utility, came under the control of malicious hackers last year…."
- The Register [2000]

2000: Un ex-
46 fois une s
sous-sol de l

2003: Le ver «Slamme
systèmes de surveillar
centrale nucléaire «Da
pendant 5h.

2003/08/11: W32.Blaster.Worm


Conscient ou paranoïaque ? (2)


```
220-<<<<<<>==< Haxed by A¦0n3 >==<>>>>>>
220- ¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸
220-/
220-|    Welcome  to this fine str0
220-|    Today is: Thursday 12 January, 2006
220-|
220-|    Current througput: 0.000 Kb/sec
220-|    Space For Rent: 5858.57 Mb
220-|
220-|    Running: 0 days, 10 hours, 31 min. and 31 sec.
220-|    Users Connected : 1 Total : 15
220-|
220^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^°°¤ø,¸¸,ø¤°°^
```

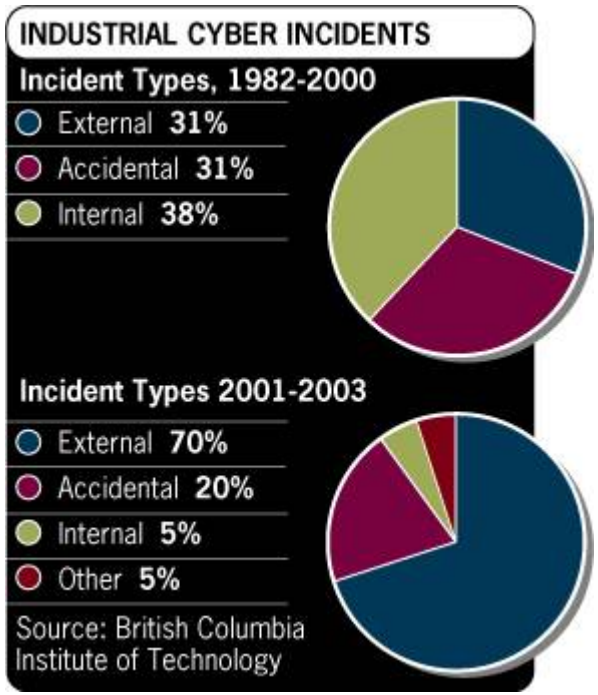
2006: Oscilloscope pirate au CERN (tournant Win XP SP2)

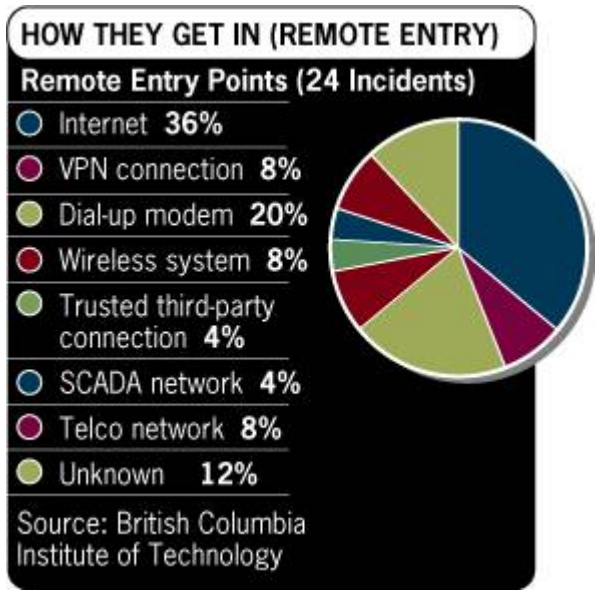

«Industrial Security Intrusion DB»

Collecté par E. Byers du British Columbia Institute of Technology

Printemps 2006: 135+ cas connus (intentionnels ou pas)

- Electricité: Transmission & distribution, fossile, hydro, et nucléaire
- Fioul & gaz
- Eau
- Chimiques
- Production
- Transport






Qui menace la sécurité ?

Attaque ciblée par…

- Trojans, viruses et vers
- (Ex-)employés fâchés & saboteurs
- Attaquants & terroristes

Manque de robustesse & beaucoup de stupidité

- Appareils mal configurés ou cassés noient le réseau
- «Finger trouble» d'ingénieur

Manque de procédures

- Updates ou patches erronés du vendeur ou mandataire
- Règles ou procédures de test inappropriées


Le facteur «Conséquence»

Risque = Vulnérabilité

× Menace

× Conséquence




Les consequences

Perte du contrôle ou de la sûreté:

- Blocage de la CPU ou des ressources
- Dysfonctionnement ou interruptions
- Coupure ou arrêt d'équipement

Perturbations dans l'usine / l'industrie:

- Perte ou réduction de la production
- Relations publiques mauvaises ou perte de la confiance
- Dommage ou **destruction** d'équipements
- **Perturbations significatives** (⇨ «Critical Infrastructure»)
- Blessure ou **décès**

€€€ CHF £££ $$$


Le Passé:
La (r)évolution des systèmes de contrôle

Le Présent:
Pas de Sécurité !?

Le Future (!):
Une solution c'est «Defence-In-Depth»


Mythes concernant la sécurité

«Sécurité de réseau, c'est tout !»

«Le firewall vous protège.»

«Cryptage vous protège.» «VPNs vous protègent.»

«Appareils de terrain ne peuvent être piratés.»

«IDSs peuvent identifier des attaques potentielles de systèmes de contrôles.»

«Vous êtes en sécurité si l'attaquant ne peut entrer.»

«Vous pouvez garder les attaquants au dehors.»

«Plus de meilleurs gadgets pouvent résoudre des problèmes de sécurité.»

«Tout peut être résolu par la technique.»


«Defence-In-Depth»

«Defence-in-Depth» c.-à-d. sécurité sur chaque niveau !

- …la sécurité de l'appareil même,
- …le firmware et le système d'opération,
- …les connections de réseau et les protocoles,
- …les applications et logiciels (p.ex. pour la programmation de PLC),
- …les logiciels d'un tiers, et
- …les utilisateurs, développeurs & opérateurs.

Les constructeurs et fournisseurs font partis de la solution !

- L'exigence de sécurité doit être inclus à la commande ou à l'ouverture

«Contrôles» fusionnent avec l'IT —
mais aussi avec «Sécurité Industrielle» !!!

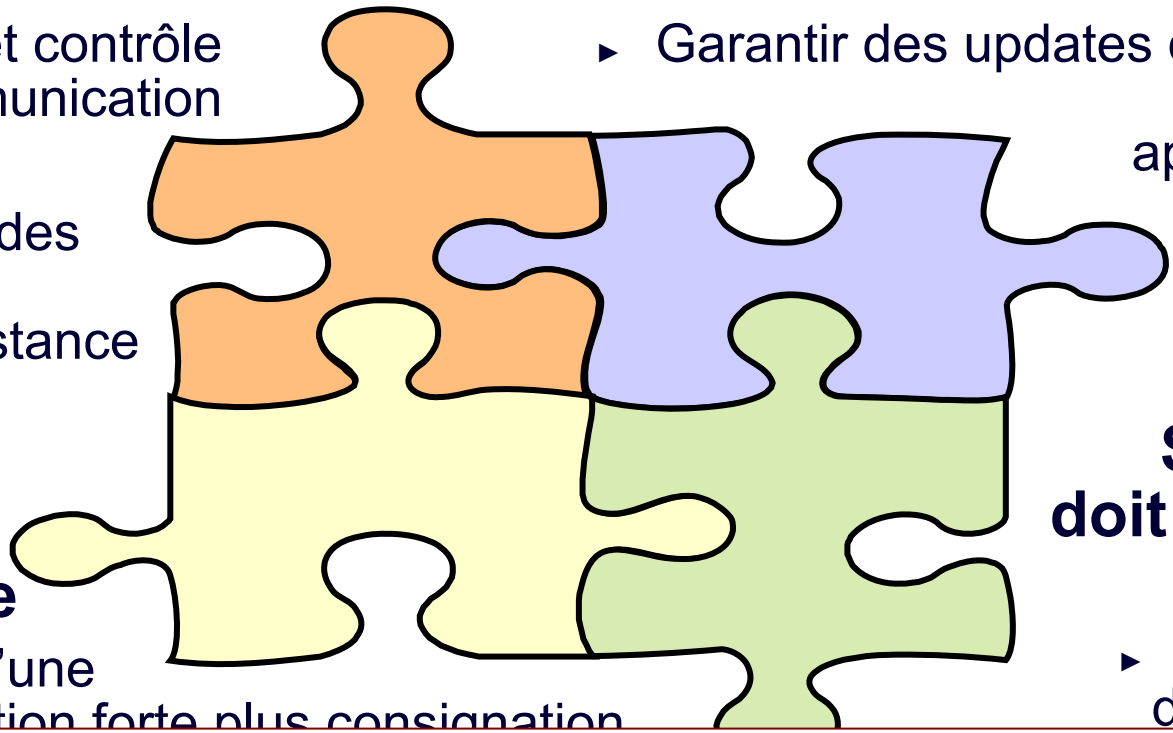

Règles fondamentales

Séparation des réseaux contrôles et business

- Réduction et contrôle d'intercommunication
- Établir IDS
- Application des règles pour l'accès à distance

Utilisation de système managé centralement si possible

- Garantir des updates de sécurité immédiats: applications, anti-virus, OS, etc.



Emploi d'un contrôle d'accès propre

- Utilisation d'une authentification forte plus consignation

Sécurité doit devenir un but

- Directives de sécurité

«Asset Management» !!!


(Trop de ?) Recommandations

- “Security for Manufacturing and Control Systems”
  “Integrating Electronic Security into Manufacturing…”
  (American National Standards Institute & Int'l Society for Measurement and Control)
  (ANSI/ISA SP99 TR1 & TR2)
- “Code of Practice for Information Security Management”
  (Int'l Organization for Standardization / Int'l Electrotechnical Commission / British Standard)
  (ISO/IEC 17799:2005, BS7799, ISO27000)
- “Common Criteria” (ISO/IEC 15408)
- “System Protection Profile for Industrial Control Systems”
  (U.S. National Institute of Standards and Technology NIST)
- “Cyber-Security Vulnerability Assessment Methodology Guidance”
  (U.S. Chemical Industry Data Exchange CIDX)
- “Good Automated Manufacturing Practices: Guideline for Automated System Security” (Int’l Society for Pharmaceutical Engineering ISPE)
- Standard de NERC (North American Electric Reliability Council)
- Standard d’AGA (American Gas Association)


Vous n'êtes pas tous seuls !

Dialogue avec utilisateurs, chercheurs, instances officielles

ExxonMobil BCIT CPNI Centre for the Protection of National Infrastructure NISCC

VATTENFALL Nutzfahrzeuge

Process Control Systems Forum — Collaborating to Advance Control System Security

Bundesamt für Sicherheit in der Informationstechnik

Informatikstrategieorgan Bund ISB
Unité de stratégie informatique de la Confédération USIC
Organo strategia informatica della Confederazione OSIC
Organ da strategia informatica da la Confederaziun OSIC

- L'USIC et CPNI offrent des échanges d'info pour les secteurs CIP (électricité, transport, fioul & gaz, pharmaceutique, bancaire, …)

Réveiller la connaissance

- Des campagnes pour informer les utilisateurs des systèmes de contrôle concernant la «sécurité industrielle»
- Au CERN et dans la communauté HEP

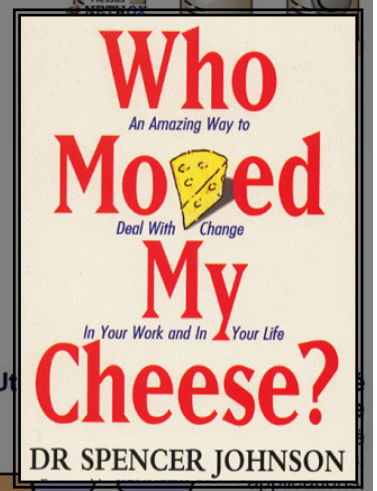
Fermilab PAUL SCHERRER INSTITUT PSI CCLRC DESY IN2P3 Institut National de Physique Nucléaire et de Physique des Particules TRIUMF


Résume

«Contrôles» fusionnent avec l'IT...

...sauf mécanismes de protection...

Et vous, vous voudriez agir AVANT ou APRÈS l'incident ?



...ont besoin d'une «Sécurité Industrielle» !!!

«Defence-In-Depth» offre une solution 100%-ε

Merci beaucoup !