Intelligence

ISA France Section

LA CYBER-SECURITE DES AUTOMATISMES ET DES SYSTEMES DE CONTRÔLE DE PROCEDE

Jean-Pierre HAUET
Associate Partner KB Intelligence
Président ISA-France

8 décembre 2009

Motivation …

- La nécessité de veiller à la sécurité des systèmes d'automatisme et de contrôle de procédé est apparue évidente aux USA en 2001 à la suite des événements du 11 septembre.
- Si des terroristes étaient arrivés à se former au pilotage d'avions sophistiqués, il leur était a priori possible de s'initier au fonctionnement des systèmes contrôlant des infrastructures stratégiques : alimentation en eau, centrales et réseaux électriques, moyens de transports, installations réputées sensibles : chimie, pharmacie, agro alimentaire.

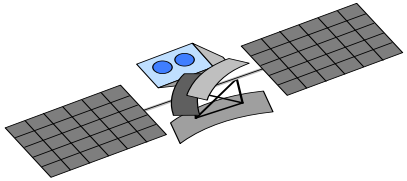
La cyber-sécurité des systèmes de contrôle

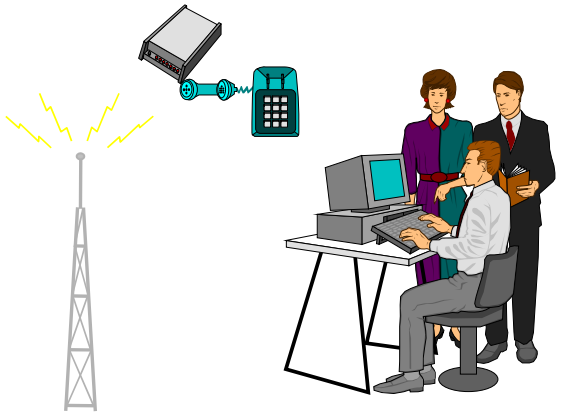
- La cyber-sécurité des systèmes de contrôle a trait à la prévention des risques associés aux intrusions dans le système, liées à des actions malintentionnées, au travers des équipements informatiques et des réseaux de communication.
- Ces risques peuvent se traduire par
  - des pertes de production
  - des pertes de données sensibles
  - des incidents sur le procédé
  - la mise en danger des personnels d ’exploitation
  - des atteintes à l’environnement

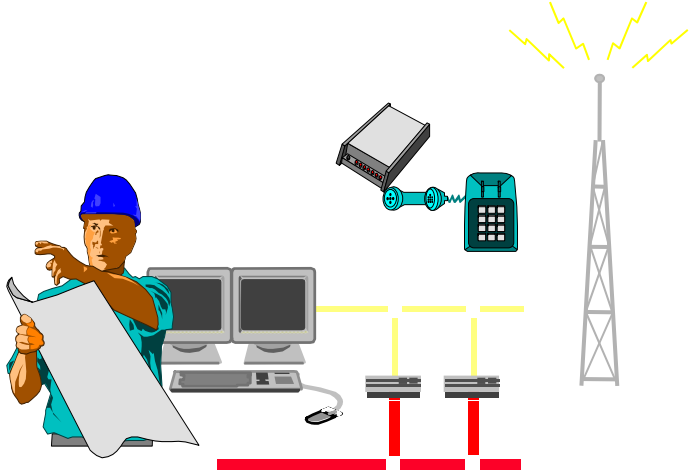
- **Les systèmes de contrôle n’appartiennent plus à un monde isolé.**
- **L’ouverture des systèmes vise à accroitre les points d’accès pour satisfaire de nouveaux besoins**

Des besoins de communication accrus

Gestion, surveillance à distance, aide à la maintenance, télécommande, aide au test et mise en service...

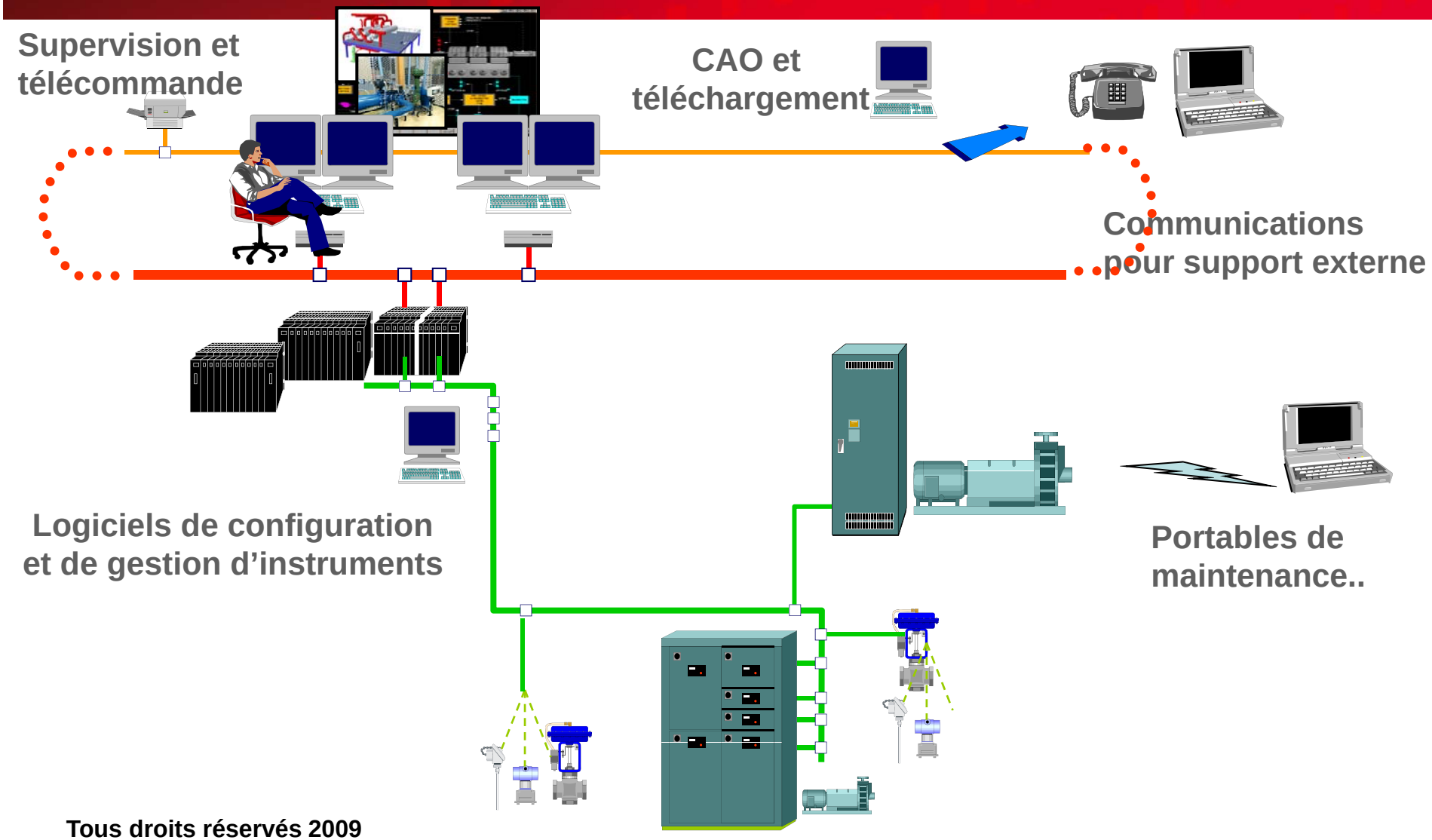






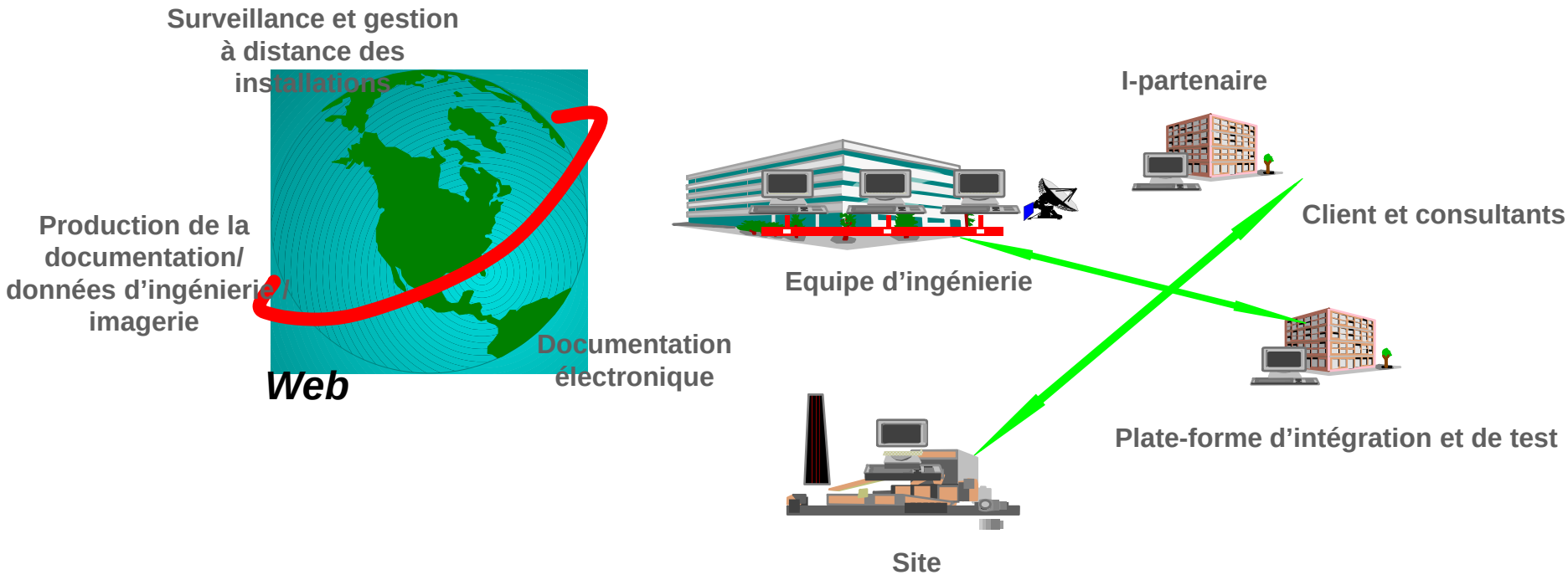
Recours accru à la sous-traitance, aux O&M etc.

Les systèmes « ouverts » utilisent des composants banalisés avec leurs forces et leurs faiblesses



Les collaborations inter-entreprises

Les collaborations inter-entreprises sont stimulées par les contraintes économiques et facilitées par les communications électroniques. La réalisation de projets est éclatée sur plusieurs sites, avec des échanges de données informatisées

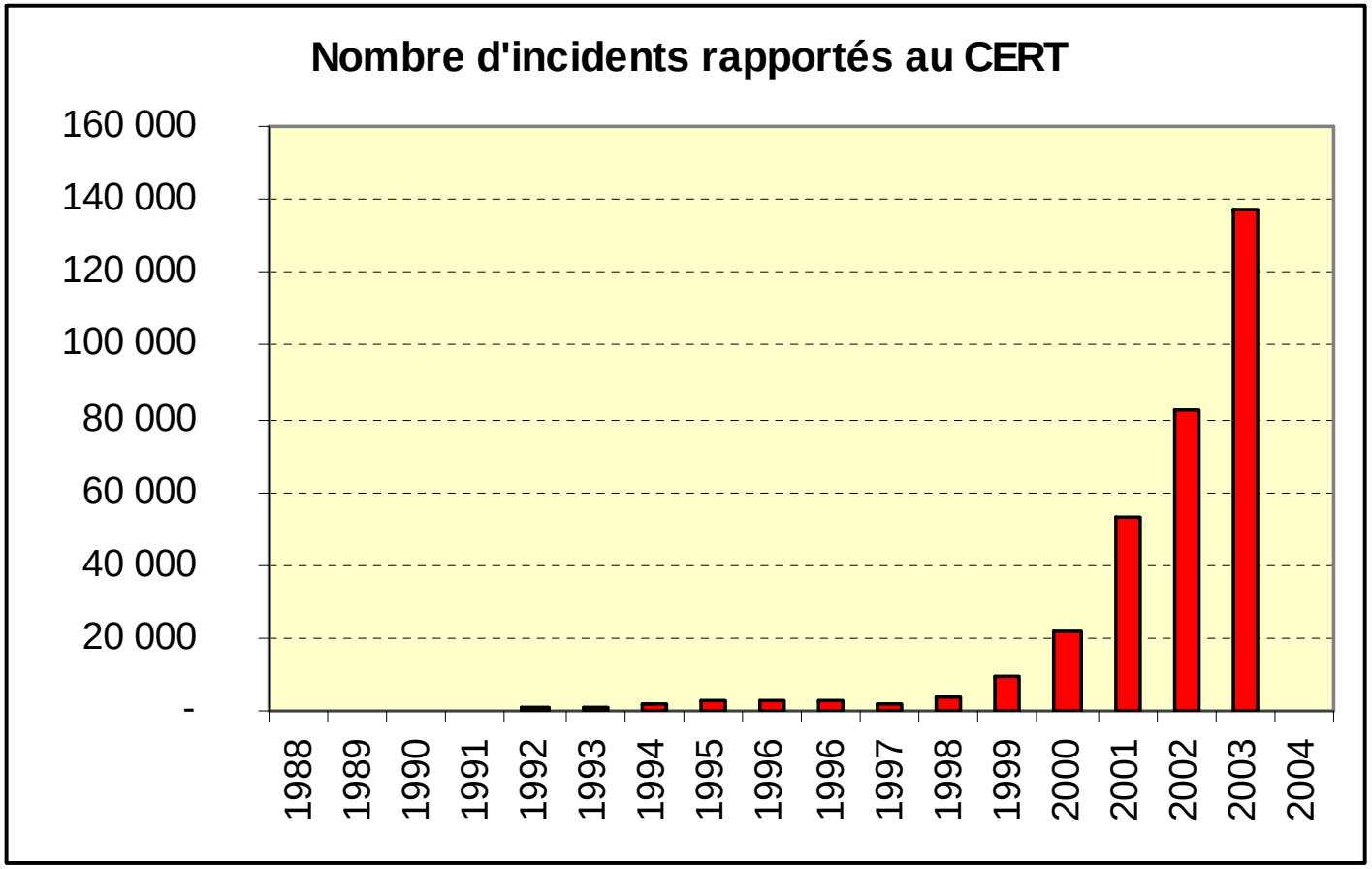


Le problème est-il réel ou est-ce une paranoïa?

- Il est difficile d'obtenir des données fiables : pas d'organisme officiel chargé du sujet en France et en Europe
- Davantage de données sont disponibles en Amérique du Nord

  - CERT (Carnegie Mellon University)
  - BCIT BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY

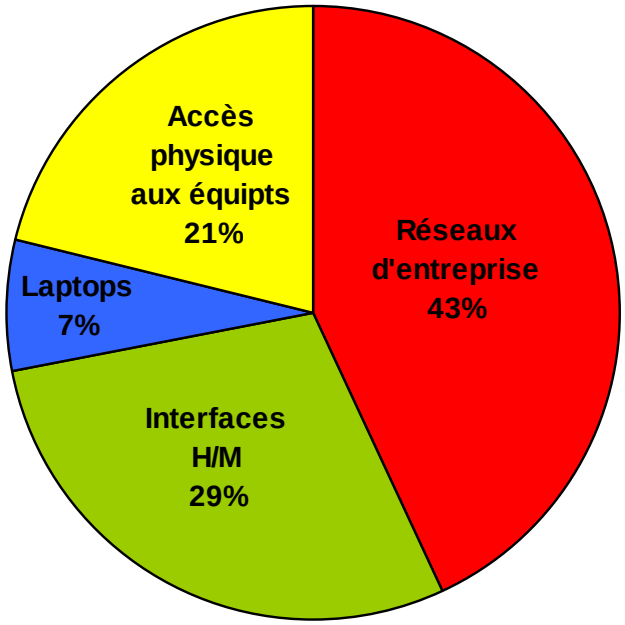
Evolution du nombre des incidents informatiques rapportés au CERT

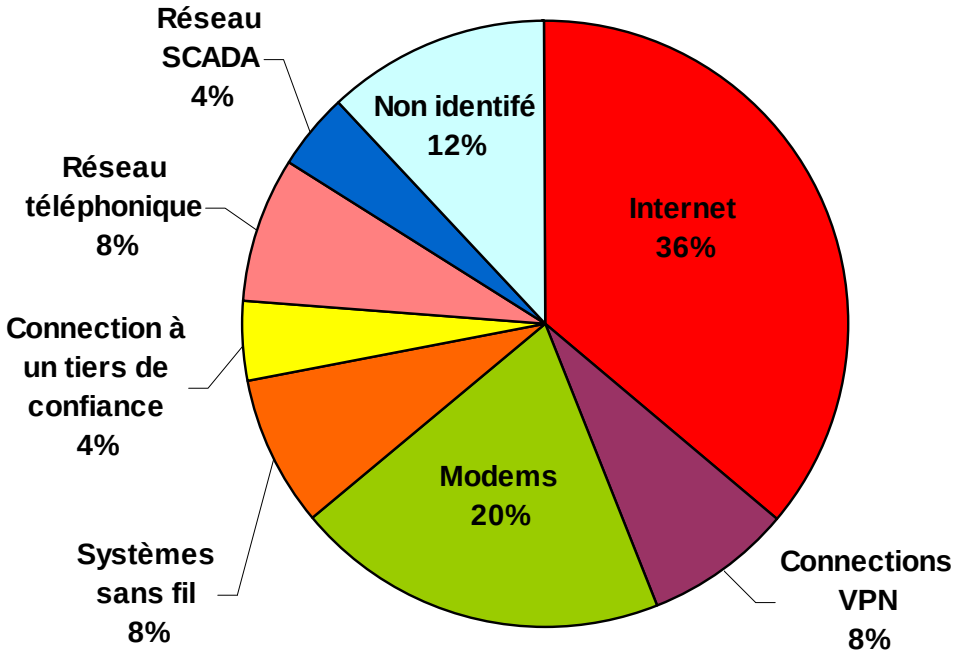


A partir de 2004, en raison de la multiplication des incidents, le CERT a renoncé à les recenser

Source : www.cert.org

Analyse des incidents récents par le BCIT



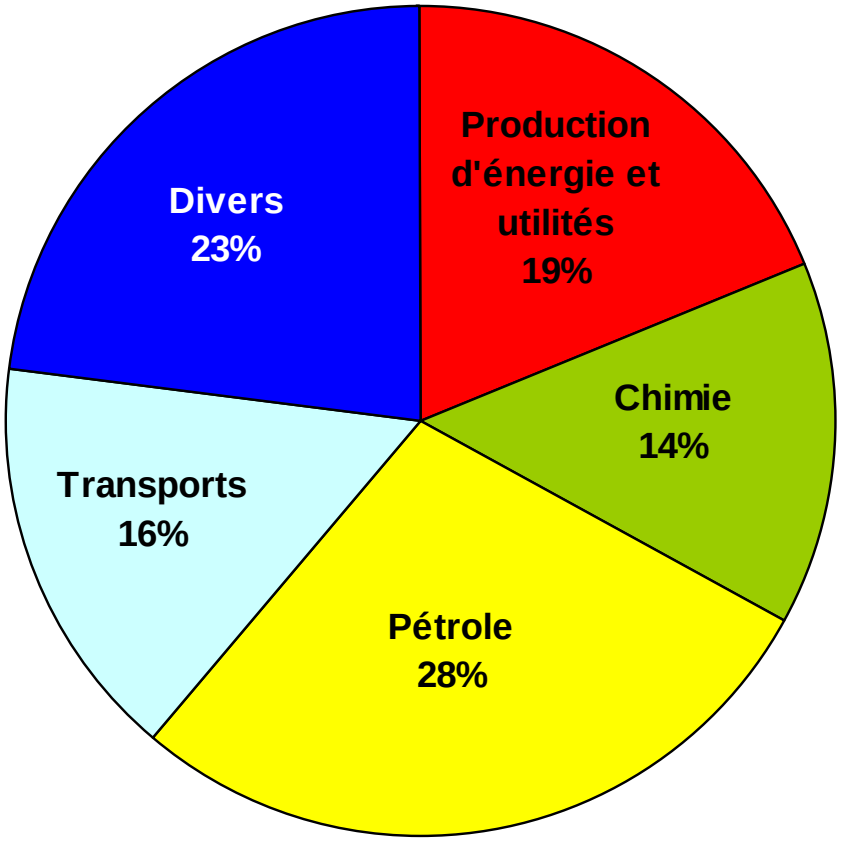


Répartition des incidents de sécurité internes en fonction des points d'entrée ➔ les points les plus vulnérables

Répartition des incidents de sécurité externes en fonction des points d'entrée ➔ les points d'entrée les plus fréquents pour les attaques d'origine externe

Source : Eric Byres BCIT

Qui a été visé ?



Source : Eric Byres BCIT

Les « utilités » ne sont pas à l ’abri…

- **Le 20 juin 2003 "SQL Slammer Worm ".**
  Le ver slammer se propageant et se multipliant sur le réseau ATM a bloqué le trafic sur un réseau desservant des sites industriels et plusieurs entreprises.
- **Tempe, Arizona Domaine, déclenchement du 29 juin 2007.**
  La panne a duré 46 minutes et 98 700 clients touchés, ce qui représente 399 mégawatts (MW) de perte de charge. Il a été causé par l ’activation inexpliquée du programme de délestage dans le système de gestion de l'énergie (SGE) à la Salt River Project (SRP).
- **Réseau sans fil en Australie : hacking en 2000**
  Un ancien consultant, mécontent d'une firme australienne qui mettait en œuvre un SCADA radio pour contrôler une installation de traitement des eaux usées, a dérobé sa voiture avec les équipements hertziens et les a reliés à un ordinateur. Il a roulé autour de la zone au moins 46 fois, en émettant des commandes d’ouverture des soupapes de décharge d’eaux usées.
- **Nuclear Power Plant : incidents cybernétiques**
  Le 19 août 2006, les opérateurs à Browns Ferry, installation nucléaire, ont du faire un arrêt manuel de l ’unité N°3, suite à la perte des pompes de recirculation primaire et secondaire du réacteur causée par une attaque sur le système de contrôle de ces pompes.
- Le **Large Hadron Collider (LHC)** inauguré en septembre 2008 au CERN sous la frontière franco-suisse, a été le même jour attaqué par un groupe de hackers grecs afin de montrer sa vulnérabilité ».


Les spécificités des systèmes de contrôle - Les solutions « IT » sont insuffisantes ou inadaptées

Spécificités des systèmes de contrôle

- Complexité en termes de matériels, de programmation, et de communication,
- Les systèmes de contrôle sont un mélange de technologies de l'information (IT) et de contrôle industriel (IC). Les systèmes de contrôle utilisent (au moins pour les automatismes) des OS "temps réel" spéciaux (au sens IT)
- Les architectures, vis-à-vis du risque sont différentes : les points critiques (PLCs, drives, instruments...) sont davantage répartis et hétérogènes
- Faible conscience des enjeux sécuritaires dans le monde des automatismes, à l'exception des domaines critiques

Les solutions IT ne suffisent pas

- Exigences de performances (temps réel ou critique, messages courts et fréquents)
- Exigences de disponibilité
- Gestion du risque différente (priorité à la sécurité des biens et des personnes
- Les objectifs peuvent être inversés

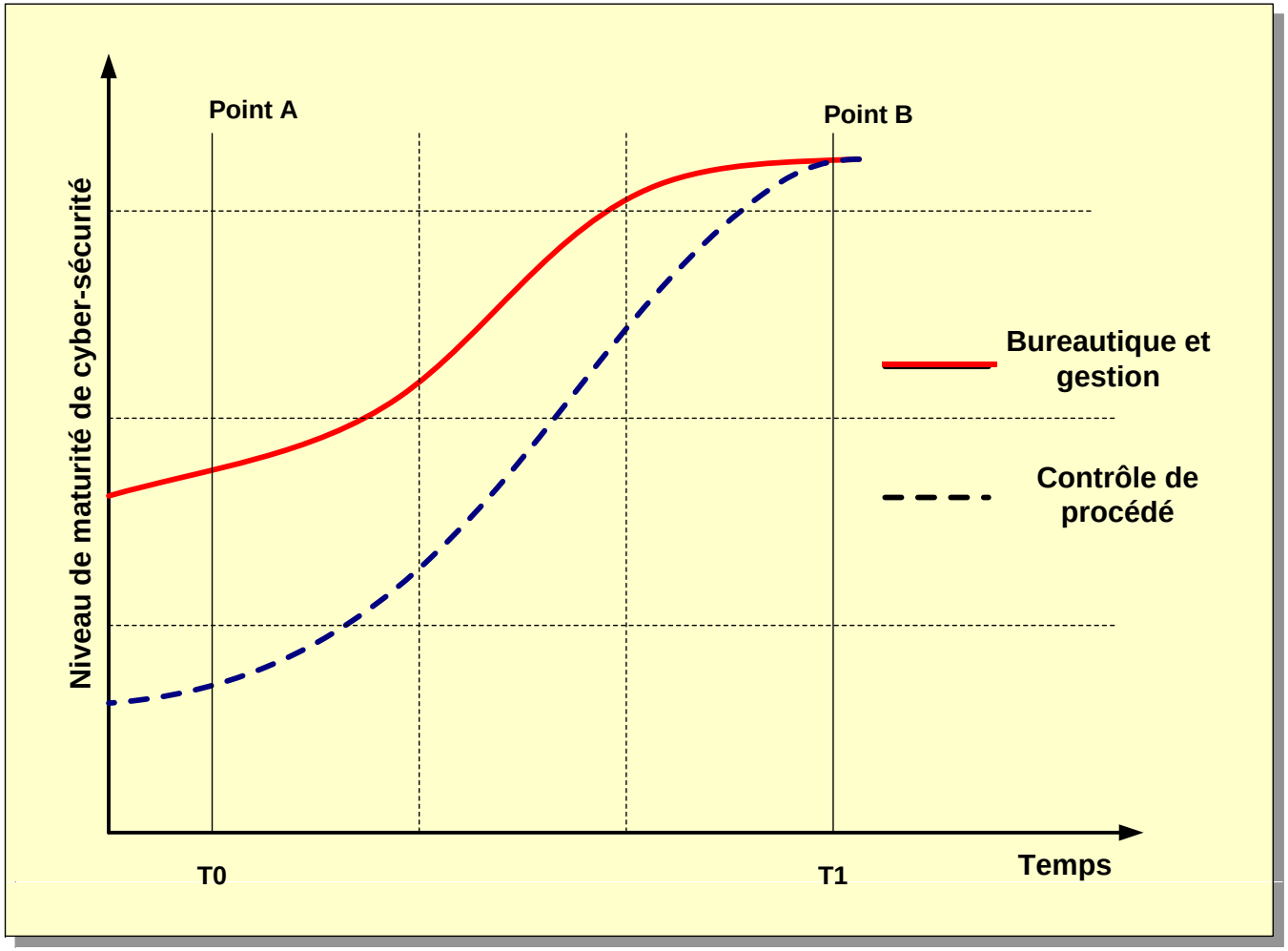
Systèmes de contrôle

- Disponibilité
- Intégrité
- Confidentialité

Systèmes d'information

- Confidentialité
- Intégrité
- Disponibilité

Mais le niveau de sécurité doit être homogène



La nécessité d'agir

- Les conséquences des cyber-attaques contre les systèmes de contrôle peuvent être extrêmement dévastatrices. Les systèmes de contrôle sont des installations réputées professionnelles où les défaillances étaient jusqu'à présent l'exception mais peu d'installations sont réellement sécurisées.

- L'immunité des systèmes de contrôle appartient au passé et ces systèmes sont, comme les autres systèmes d'information, des cibles possibles pour le cyber-terrorisme, l'espionnage ou la simplement la malveillance

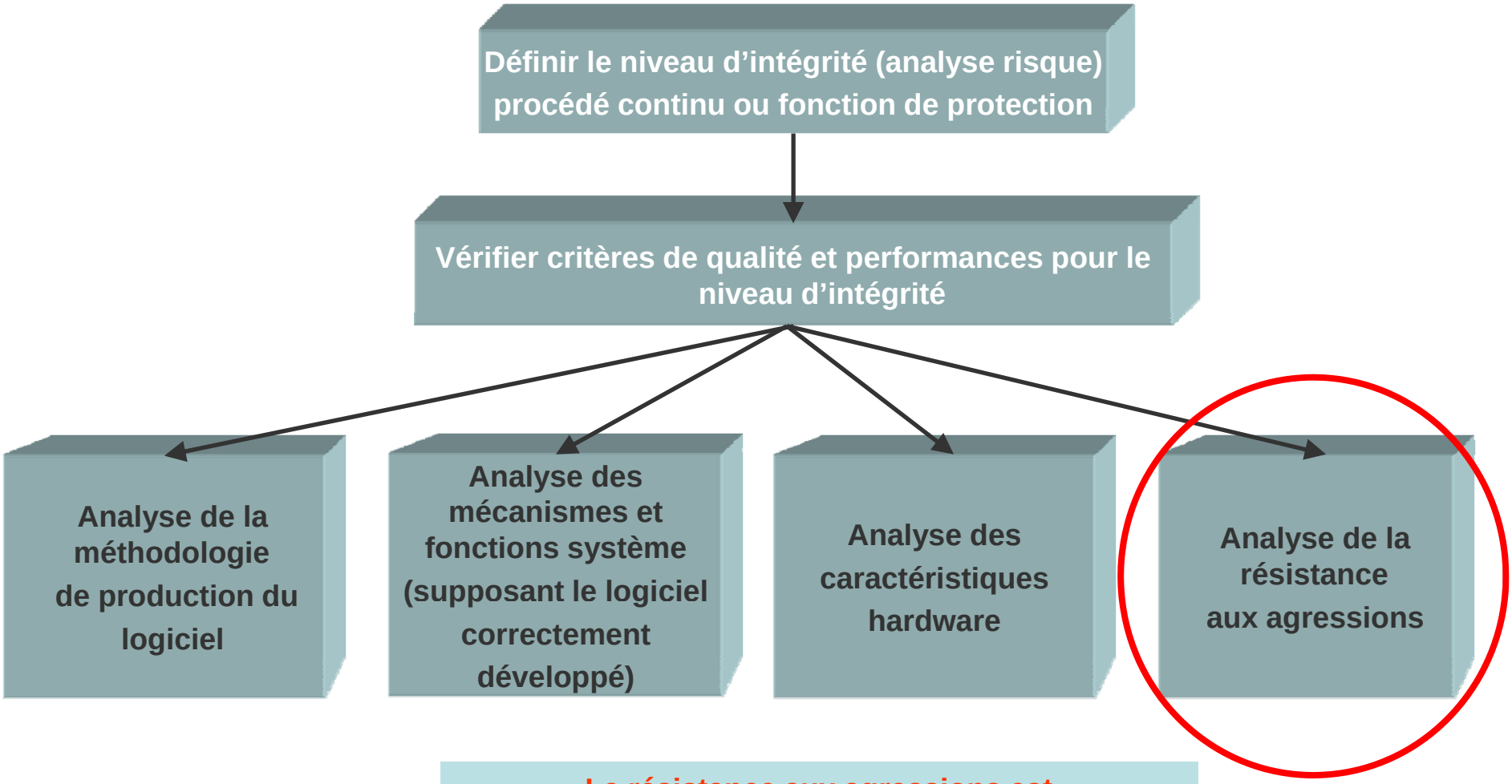
D'où le besoin de pratiques, de standards de référence, d'outils et services d'évaluation adaptés au monde du contrôle de procédé → **ISA-99**


Quelques aspect normatifs

Sécurité fonctionnelle et cyber-sécurité

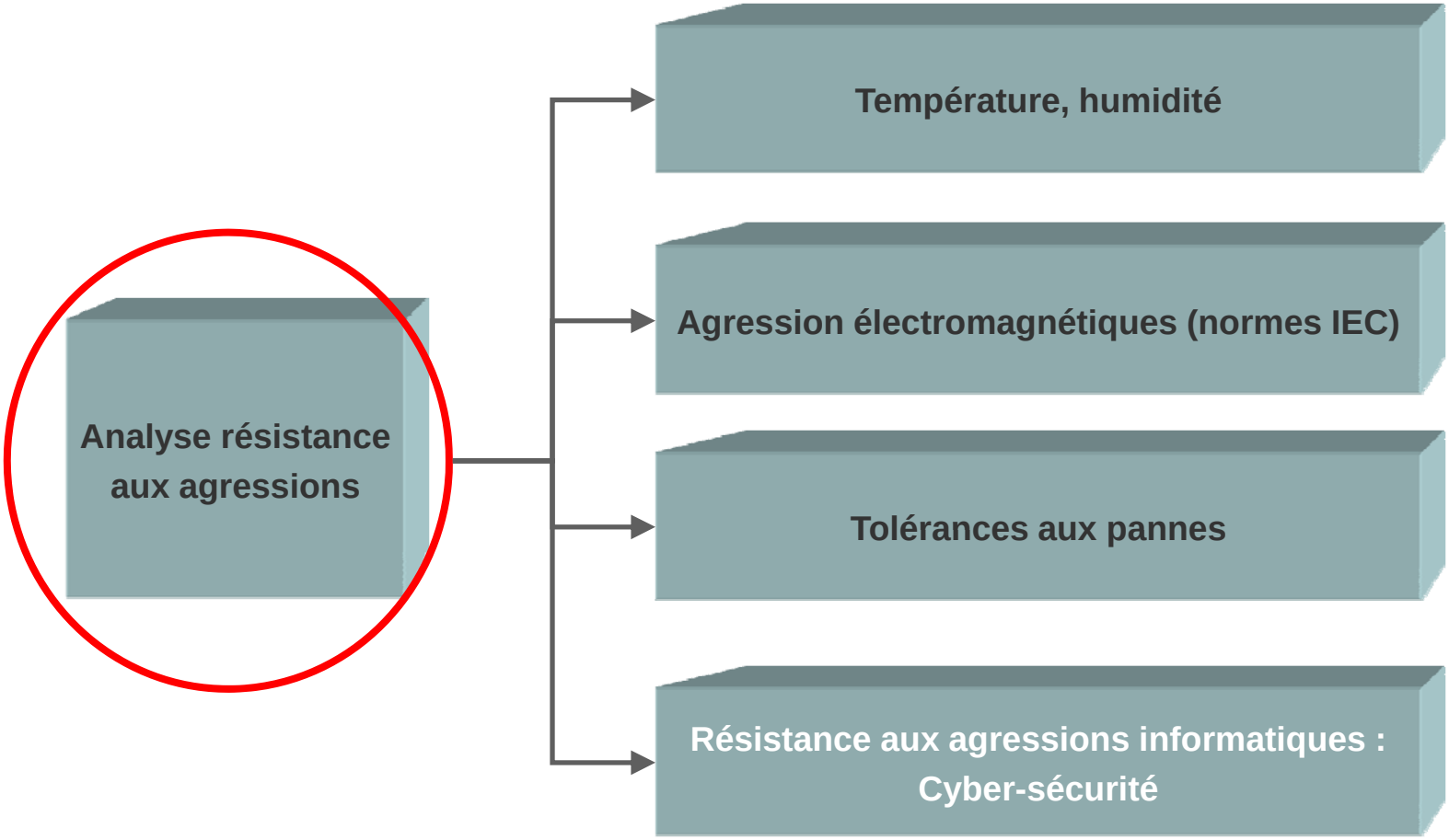
- La cyber-sécurité est un sous ensemble de la **sécurité fonctionnelle** (ou sûreté de fonctionnement), correspondant à la protection contre un certain type d'agressions externes
- La sécurité fonctionnelle se fonde actuellement sur la norme CEI 61508 et sur ses dérivés.
- Cette norme impose l'analyse du système face aux agressions internes et externes.
- Elle introduit par la notion de*(Safety Integrity Level),* , comme un indicateur et une mesure de la sécurité fonctionnelle (SIL1 à SIL4)
- Mais au moment de sa conception, les cyber-attaques étaient du second ordre (isolement et technologies spécifiques des systèmes de contrôle)

Principes d'analyse de la conformité à la norme IEC 61508



La résistance aux agressions est
un point important et englobe plusieurs aspects

La cyber-sécurité devient une discipline à part entière



Traitée de façon très succincte lors de l'adoption de la norme 61508 – Les systèmes de contrôle étaient alors considérés comme spécifiques et auto-protégés.

L’intervention de l’ISA

« Les systèmes de contrôle-commande, les systèmes de supervision, les systèmes MES sont de plus en plus ouverts au monde extérieur et à Internet (ne serait-ce que pour visualiser des informations à distance ou réaliser des opérations de télémaintenance). Beaucoup d’industriels s’inquiètent des conséquences qui en découlent, telles que l’apparition de virus ou le piratage des informations (espionnage, corruption ou destruction). Pour ces raisons, la cyber-sécurité est en train de devenir un enjeu majeur..

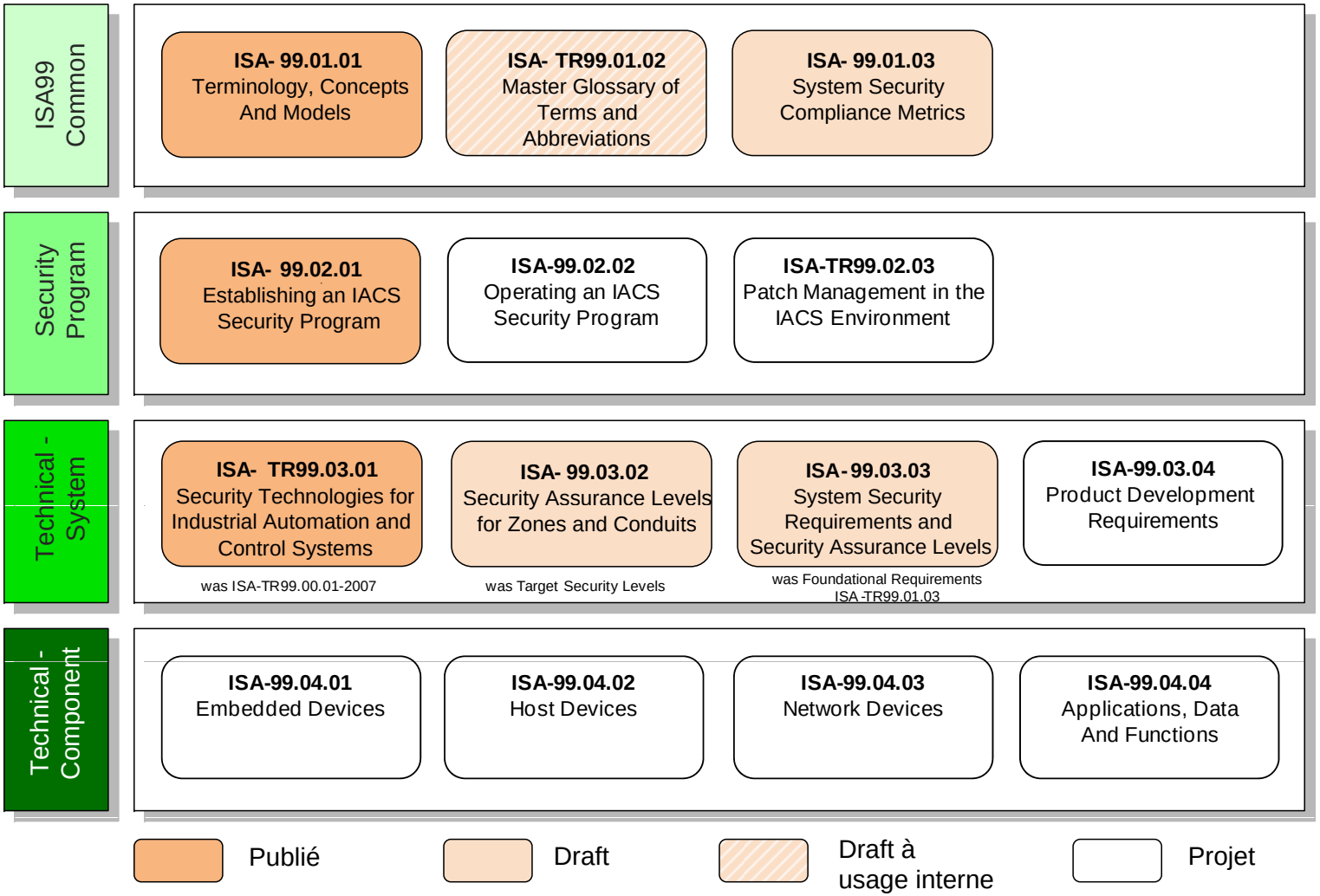
L’ISA, sans conteste la plus grande association d’ingénieurs dans le monde et connue pour ses cours de formation et ses travaux en faveur des normes, est aux premières loges en matière de cyber-sécurité. Son groupe de travail ISA99 a élaboré des guides (et notamment le TR99.00.01), qui va être proposé à l’ANSI, le célèbre organisme de normalisation américain… »

Revue Mesures octobre 2007

Le champ d'application de l'ISA-99

- Essentiellement les systèmes industriels d'automatisme et de contrôle (IACS) tels que définis dans le modèle de référence
- Y compris les systèmes de supervision rencontrés dans les industries de process
- Y compris les Scadas (Supervisory control and data acquisition) :
  - Réseaux de transport et de distribution d'électricité
  - Réseaux de distribution d'eau et de gaz
  - Production de gaz et de pétrole
  - Pipelines et gazoducs
- Autres applications éventuelles

Structure documentaire ISA-99 (harmonisée avec le projet IEC 62443)




La démarche ISA-99

Les exigences fondamentales selon l'ISA

Principales exigences à prendre en compte pour assurer la sécurité des systèmes de contrôle

- **Contrôle de l'accès** à certains équipements et à l'information
- **Contrôle de l'usage** fait de certains équipements et de l'information
- **Intégrité des données** (protection contre des modifications non autorisées
- **Confidentialité** des données
- **Contrôle des flux de données** pour éviter une diffusion non souhaitée
- **Temps de réponse aux événements** (réactivité aux violations)
- **Disponibilité des ressources**, afin de faire face aux dénis de service notamment

Démarche générale d'élaboration d'un CSMS (Cyber-sécurité management system)

Analyse des risques

- Identification et valorisation des actifs à protéger : physiques, logiques, humains,
- Analyse des pertes potentielles
- Analyse des vulnérabilités, des risques et des menaces

Définir les contremesures

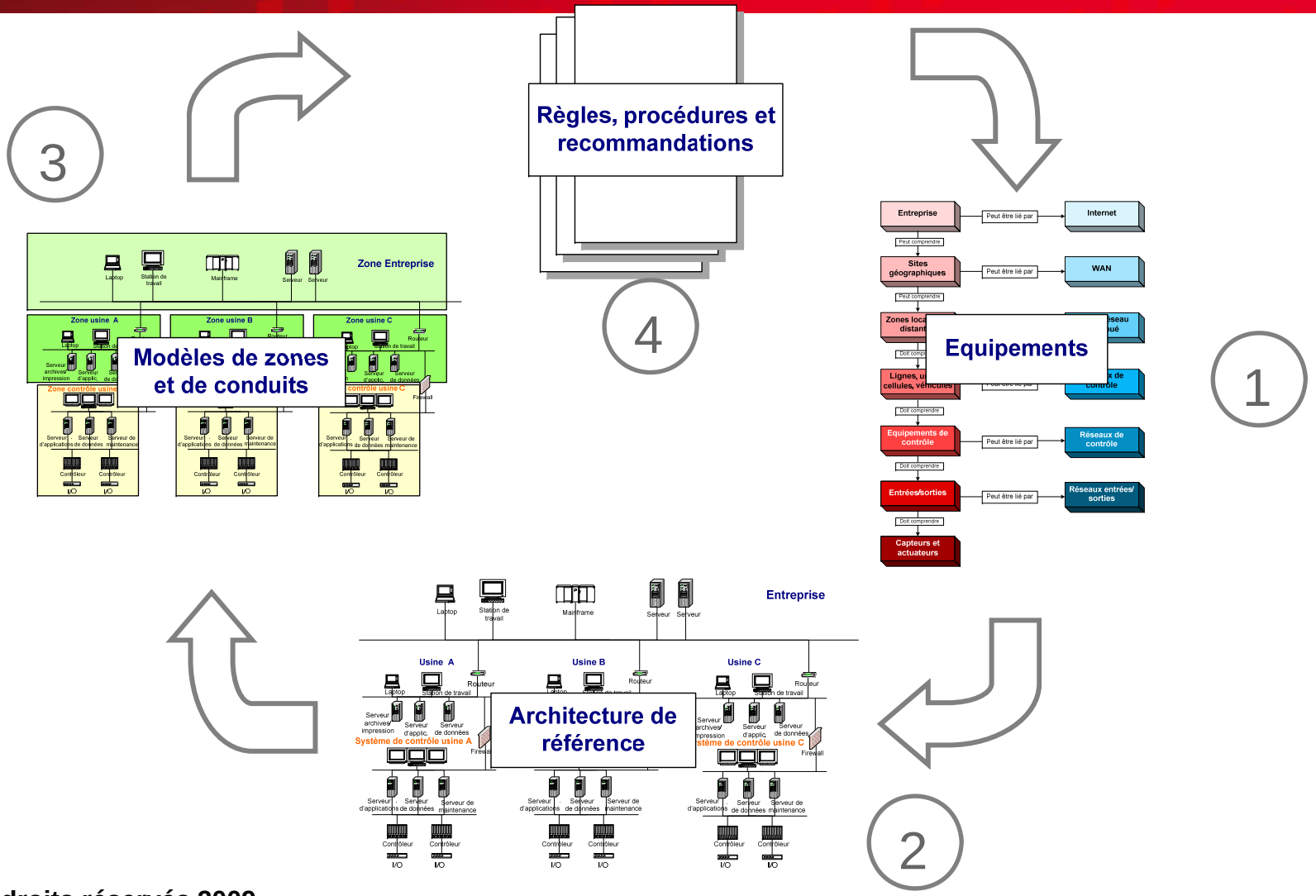
- Dispositions générales, règlements de sécurité
- Dispositions particulières
  - Authentification des personnes, des équipements, des messages
  - Contrôle d'accès, détection d'intrusion
  - Chiffrement, signatures numériques
  - Isolement de certaines ressources
  - Scan des malware
  - Monitoring de l'activité du système, surveillance physique

Mettre en œuvre, évaluer et améliorer

La démarche pratique ISA-99

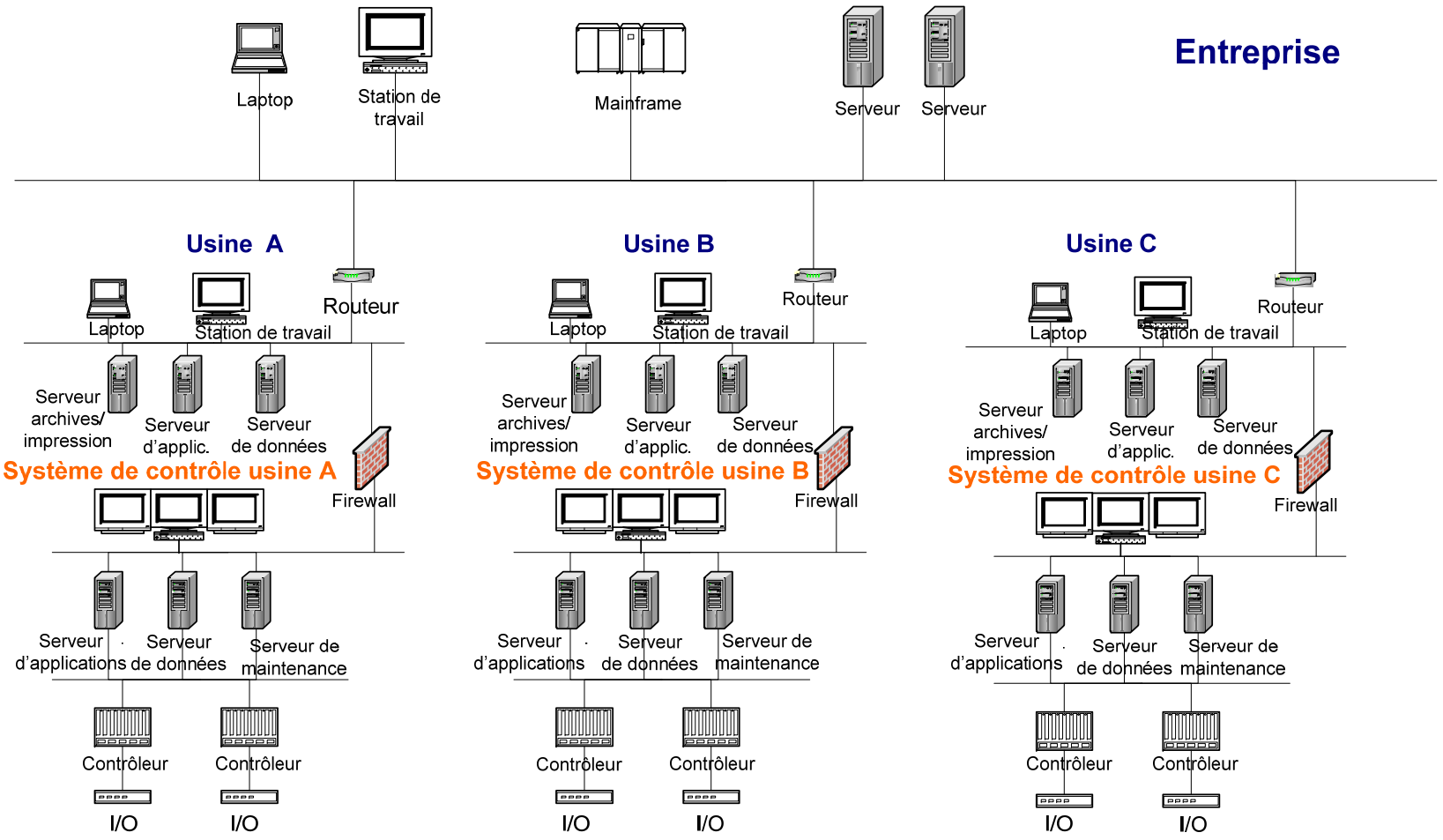
- La cyber-sécurité du système se construit à partir d'une **analyse des actifs** (matériels ou immatériels) à protéger, de leurs forces et faiblesses, des risques encourus, des menaces potentielles
- Cette analyse nécessite une **mise en forme de l'architecture** et une **décomposition du système en zones homogènes**,
- L'analyse de chacune des zones permet de définir des **règles et procédures** qui constituent le programme de sécurité
- Des **itérations** sont nécessaires

Le cycle d'analyse

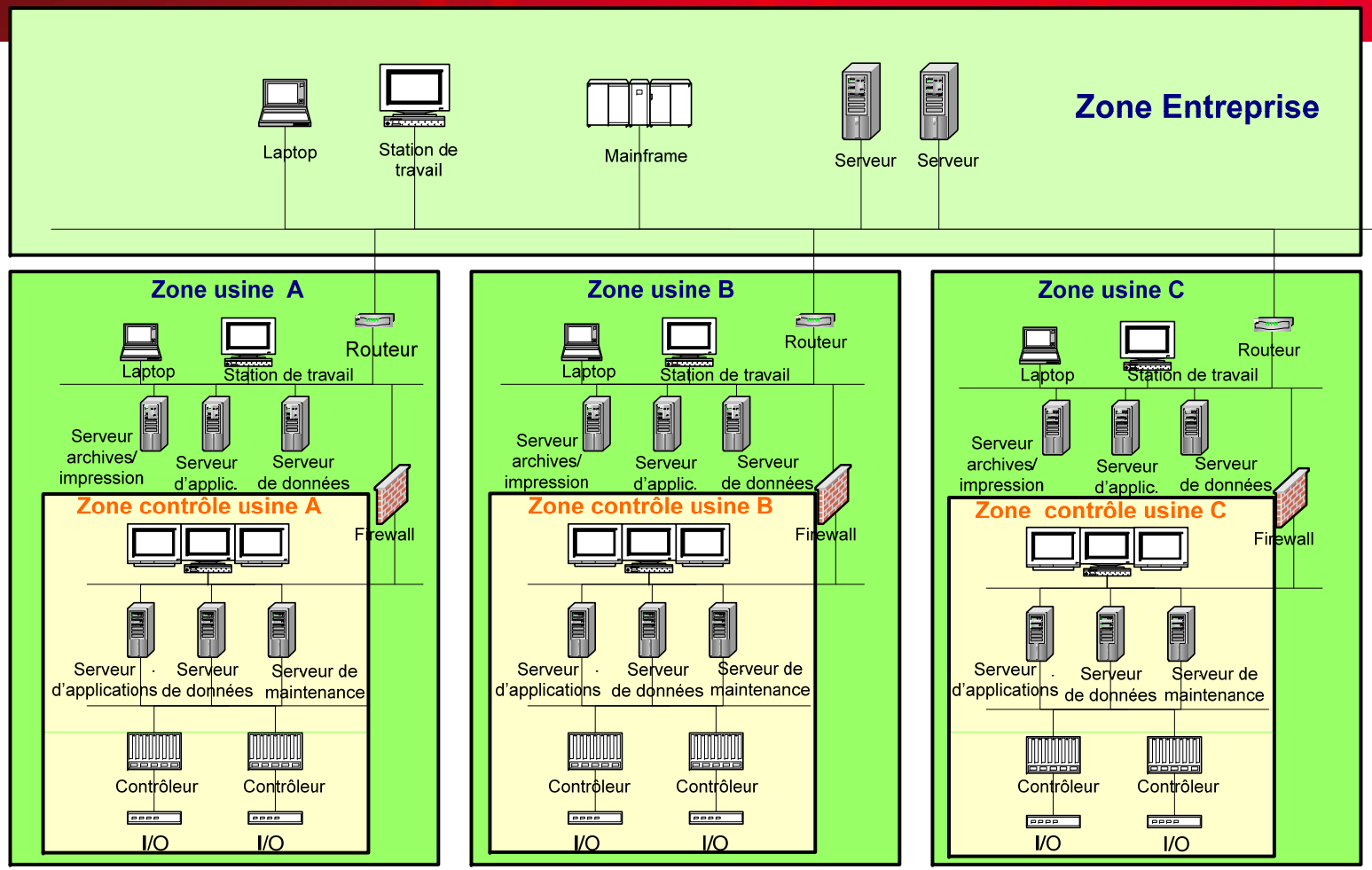


Architecture de référence

Exemple d'architecture de référence simplifiée

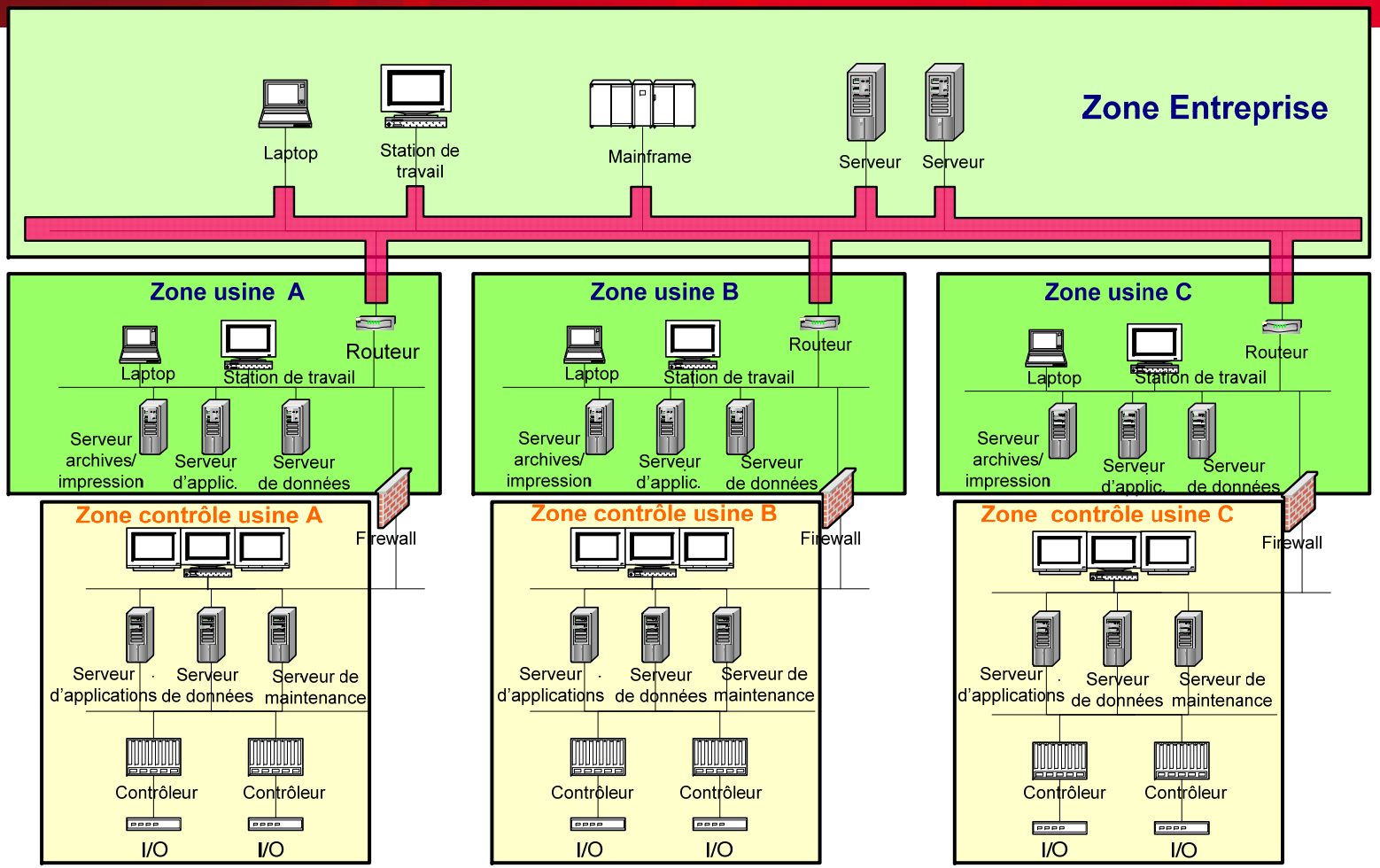


Exemple de zones hiérarchisées



Les zones « filles » héritent des propriétés des zones « parents »

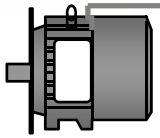
Des zones particulières : les conduits

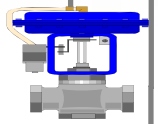


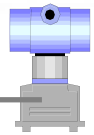
Conduit d'entreprise

Exemple d’une station de remplissage de camions transportant des produits dangereux

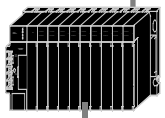
Station de remplissage







Moteurs, variateurs, pompes, capteurs, etc.



Automate de contrôle

Switch

Routeur et pare-feu

Poste de contrôle local

Switch

Salle de contrôle distante

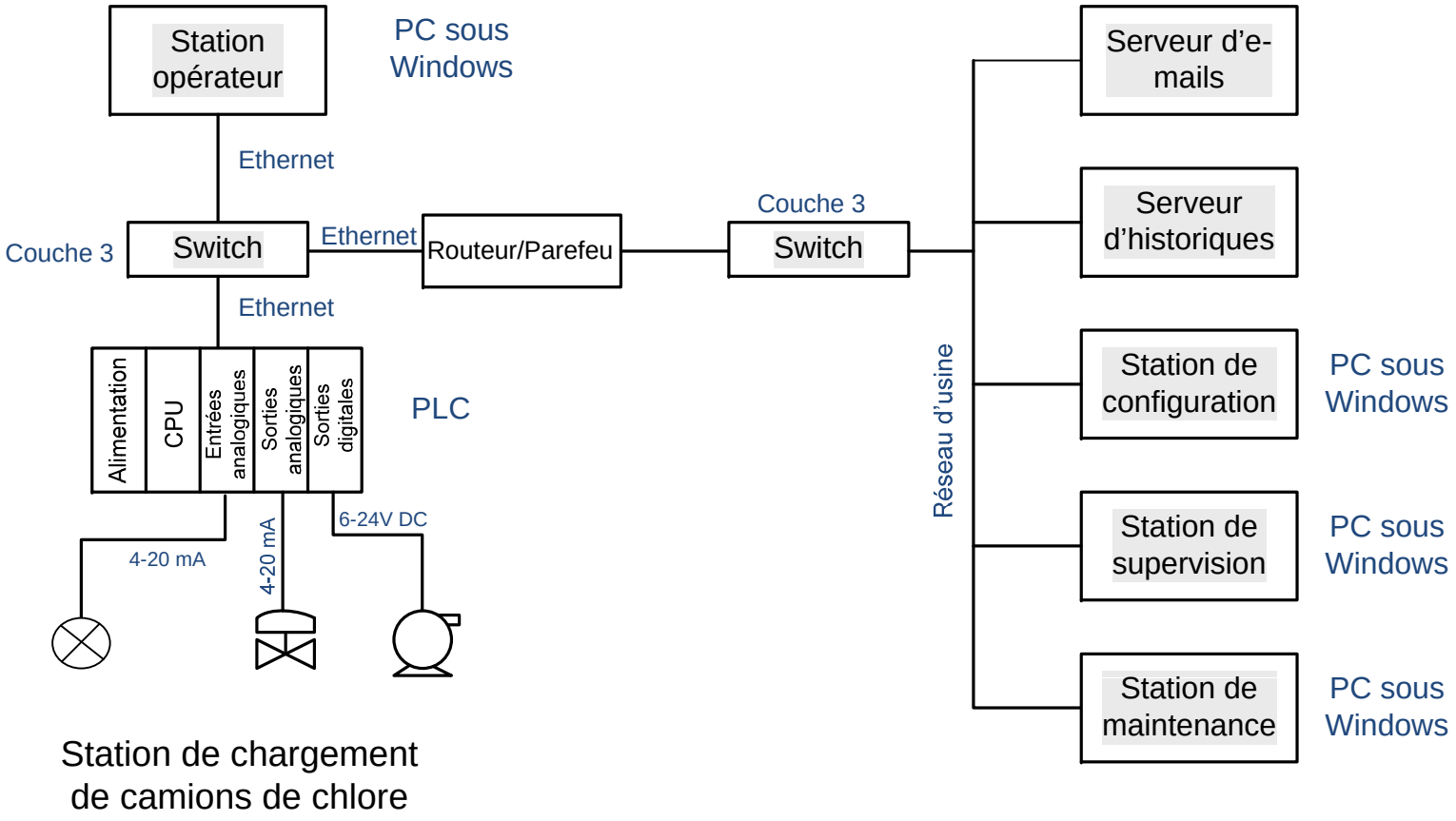
Serveur d’e-mails

Serveur d’historiques

Configuration

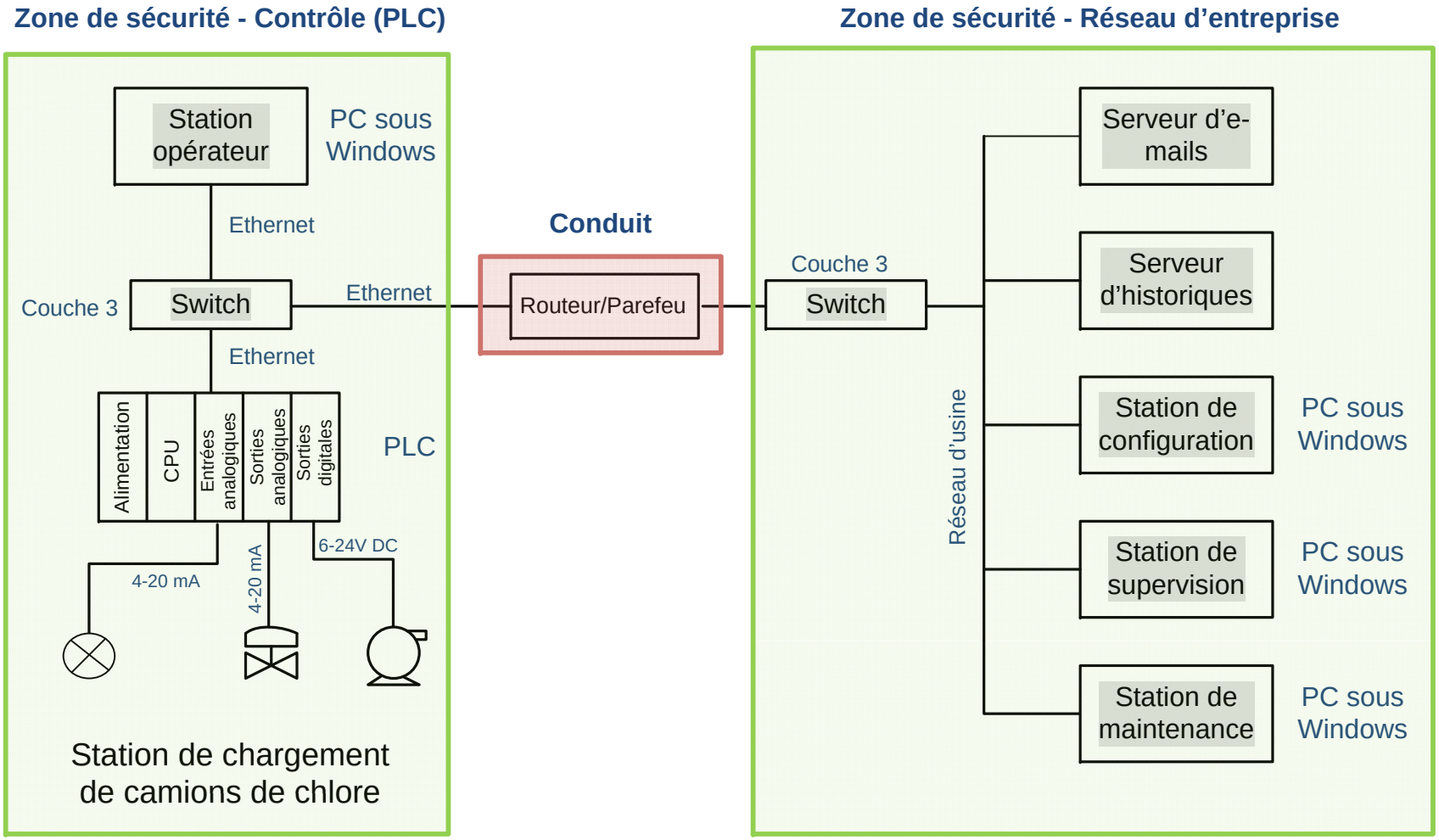
Maintenance

Définition de la topologie du système



Station de chargement
de camions de chlore

Définition des zones



Les objectifs de sécurité

- Après définition des zones et des conduits, le standard ISA-99.03.02 définit une méthodologie permettant d'assigner des objectifs de niveaux de sécurité à chaque zone
- Les catégories de sécurité vont de 1 à 4
- Le niveau de sécurité résulte d'une combinaison de la probabilité d'occurrence des risques et de de la criticité des conséquences
- Le standard donne également des éléments pour diagnostiquer le niveau de sécurité effectivement atteint.
- Les métriques seront précisées dans les standards à venir

La stratégie de limitation du risque se définit face à un niveau de risque

Application d'une matrice de décision pour l'implantation de firewalls

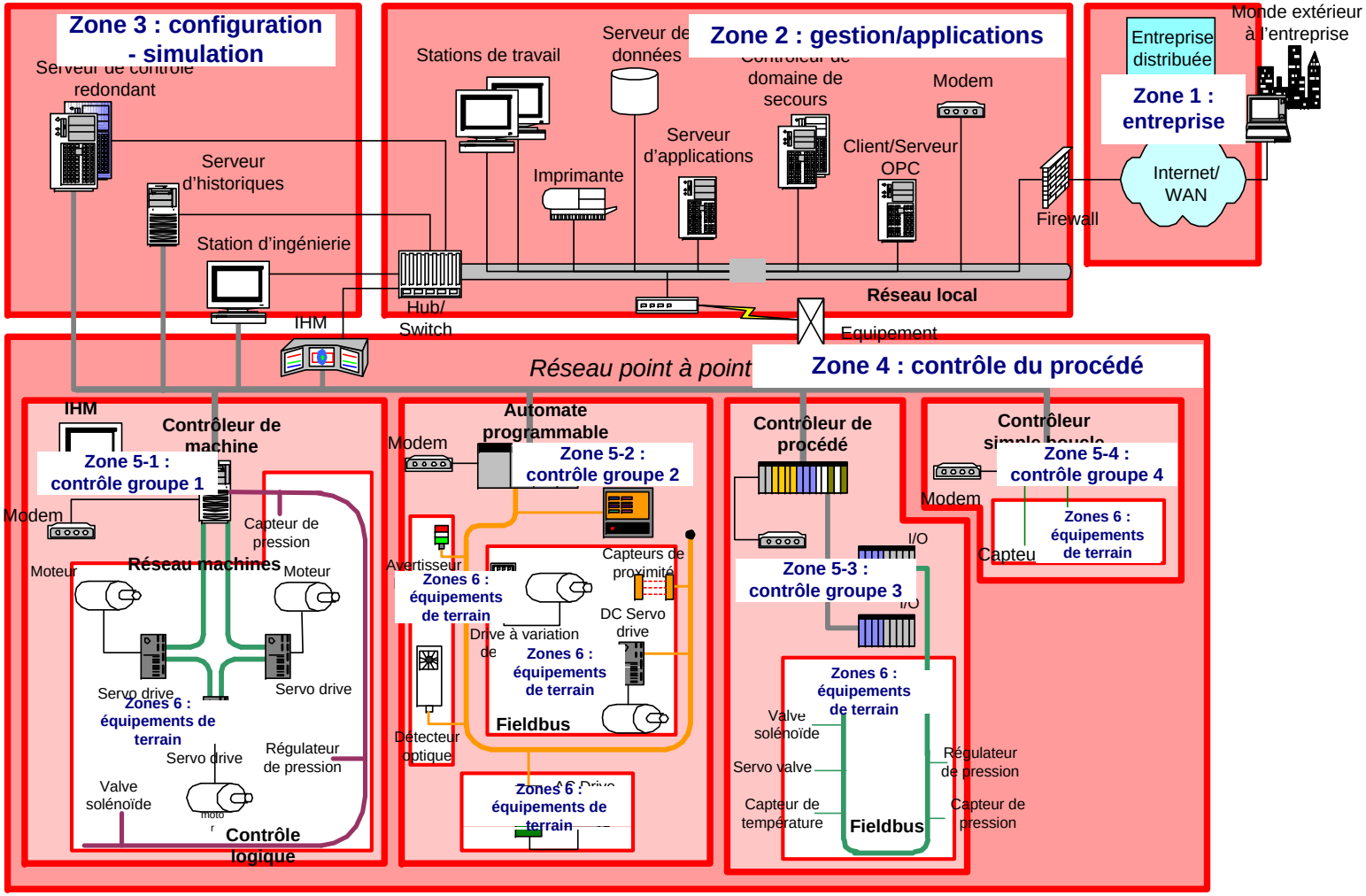
Réseau de contrôle - Equipements		Criticité			
		1 = Sévère	2 = Majeur	3 = Mineur	4 = pas d'impact
Probabilité	A = Très forte	Firewall exigé	Firewall exigé	Firewall exigé	
	B = moyenne	Firewall exigé	Firewall exigé	Firewall recommandé	
	C = faible	Firewall exigé	Firewall exigé	Firewall recommandé	
	D = très faible	Firewall recommandé			

Conclusion : firewall nécessaire

Défense en profondeur

- Une seule technologie de « barrière » n'est pas suffisante pour limiter suffisamment le risque (exemple de la ligne Maginot)
- La **défense en profondeur** consiste
  - à multiplier les mesures faisant barrière au risque, de façon hiérarchisée et /ou par redondance
  - À faire en sorte de cloisonner les effets de défaillances éventuelles suite à attaque (contre exemple du Titanic)
- Quelques exemples de défense en profondeur :
  - Segmentation des réseaux et barrières multiples, le niveau le plus protégé pour les applications les plus critiques
  - Séparation logique entre réseau entreprise et réseau contrôle (firewall régulièrement inspectés),
  - DMZ (pas de trafic perturbant les automatismes depuis le réseau entreprise)
  - Redondance des éléments critiques (hard et soft)
  - Différentiation technologique et diversité (par ex : antivirus de différents fournisseurs) etc.

La définition des zones : une partie importante de la défense en profondeur



Des outils sont utiles pour mener les évaluations

- Pour la qualification des réseaux de communication, Wurldtech Laboratory est en train de s'imposer comme une référence
- Une attente : adaptation de l'outil support **CS2SAT**(Control Systems Cyber Security Self-Assessment tool) aux standards ISA/IEC

Ces outils apportent une aide mais ne dispensent pas d'une analyse en profondeur de la conception et de l'implémentation


Conclusion

Cyber-sécurité et sécurité informatique

- La démarche cyber-sécuritaire nécessite un brassage de culture des intervenants et elle doit en général être réaliste et progressive. Le programme général de cyber-sécurité doit prendre en compte le niveau de risque, qui peut être différencié d'un type d'application à l'autre, et les différents modes d'exploitation.
- Pour résorber les différences culturelles entre les informaticiens et les « gens du contrôle de procédé », il faut :
  - Former le personnel du contrôle de procédé aux enjeux et aux technologies de cyber-sécurité
  - Former le personnel informatique à la compréhension des technologies et contraintes des systèmes de contrôle de procédé
  - Développer la collaboration et la formation d'équipes intégrées avec des experts de divers horizons.

Intelligence

ISA France Section

Merci de votre attention

Pour tout renseignement complémentaire :

info@isa-france.org

jean-pierre.hauet@kbintelligence.com