La cyber-sécurité dans les systèmes d'automatisme et de contrôle de procédé
Cyber-security of automation and process control systems

Jean-Pierre DALZON – Responsable technique ISA-France
Jean-Pierre HAUET – Consultant - Président ISA-France

MOTS-CLES
Systèmes de contrôle, automatismes, sécurité, Ethernet, Internet, intrusion, PLC, DCS, SNCC, protection, vulnérabilité, analyse de risques

L'ESSENTIEL

Depuis plus une décennie, le monde du contrôle de procédé a intégré les technologies de l'informatique. Stations opérateur et stations de configuration et de maintenance sont supportées par des matériels et logiciels du commerce. Ethernet et Internet sont devenus incontournables. Aujourd'hui, les radiocommunications : Wi-Fi, ZigBee, Bluetooth etc. prennent position dans les systèmes de contrôle. Le coût des systèmes diminue, leurs fonctionnalités s'enrichissent et leur intégration avec le monde de la gestion de production se fait plus étroite. Mais cette évolution rapproche les systèmes de contrôle du monde extérieur et les rend plus vulnérables à des intrusions et à des attaques de toutes natures.

Les risques qui en résultent, pour la production, pour la sécurité des biens et des personnes, sont fortement ressentis aux USA depuis les évènements du 11 septembre. En Europe, la prise de conscience est moindre mais les faits sont là.

Le présent article a pour objectif de sensibiliser les lecteurs à la problématique de la cyber-sécurité et de présenter les organisations à mettre en place pour se protéger. Il s'appuie sur les travaux de normalisation du comité ISA SP99 visant à permettre la conception et l'implémentation d'une politique optimale de protection des systèmes de contrôle contre les cyber-attaques.

SYNOPSIS

Over more than a decade, industrial controls have widely capitalized on the world of information systems. HMI stations and engineering tools are widely using off the shelf hardware and software while Ethernet and Internet have become a must. Moreover, control systems are starting to integrate radio-communications (Wi-Fi, ZigBee, Bluetooth, etc.). Systems cost has substantially decreased, wider functionality is available and integration with production is tighter. But their protection against the external world has simultaneously decreased making them more vulnerable vis à vis intrusions and other attacks.

Corresponding risks for production, installations as well as human safety are strongly perceived in the US since September 11. In Europe, the awareness in not as strong but the facts remain.
The present article aims at giving an overview of the context and at proposing approaches and solutions. It mainly relies on the outputs of the ISA SP99 standardization committee aiming at providing guidelines for the design and implementation of an optimal security policy against cyber-attacks.

1. INTRODUCTION

La nécessité de veiller de très près 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 devait être 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.

Or depuis une dizaine d'années, l'informatique s'est largement introduite dans les systèmes de contrôle :

- au niveau des réseaux, avec Ethernet, TCP-IP, les connexions à Internet,
- au niveau des équipements, avec l'usage de matériels non spécifiques et l'utilisation de Windows.

Cette évolution a été bénéfique sur le plan des coûts et des fonctionnalités:

- accès aux données de production et aux historiques depuis l'informatique de gestion,
- accès distants, pour la collecte d'information, la configuration et la maintenance,
- ouverture au partenariat d'ingénierie à travers d'outils communicants.

Mais cela a multiplié les points d'accès potentiels aux systèmes de contrôle et il devient aujourd'hui difficile de savoir *qui* est autorisé à accéder à un système d'information, *quand* cet accès est autorisé et *quelles* données peuvent être rendues accessibles.

Après la banalisation des équipements de traitement de l'information, le développement des réseaux locaux de radiocommunications, du type Wi-Fi, ZigBee, Bluetooth, dans des bandes de fréquence ouvertes à tous, va générer de nouveaux points d'entrée possible dans les systèmes de contrôle et donc potentiellement de nouvelles failles sécuritaires.

Il existe certes des normes relatives à la sécurité informatique telles que l'*ISO/IEC International standard 17799, Information Technology – Code of practice for security management.* Mais ces normes ne sont pas applicables en l'état aux systèmes de contrôle car la culture des intervenants et le contexte d'utilisation sont très différents :

- l'informatique générale est fortement sensibilisée aux problèmes de protection contre les intrusions. C'est moins vrai pour les automaticiens, plus axés sur la conduite des procédés et pensant être protégés par la spécificité apparente de leurs outils.
- le contexte d'utilisation demeure différent : On hésitera à encrypter des messages si cela nuit au temps de réponse. On admet en informatique des interruptions

momentanées de service, des « reboots » de correction, la contrainte principale étant de ne pas perdre de données. De telles interruptions sont intolérables sur un système dont l'arrêt entraîne l'arrêt de la production.

- En informatique, on a tendance à privilégier la protection des serveurs centraux ; en automatisme, les éléments sensibles à protéger sont les équipements terminaux qui agissent directement sur le procédé.
- Enfin les besoins de former des opérateurs de différents niveaux, de sous-traiter tout ou partie de l'exploitation, voire de délocaliser certaines activités, conduisent à une multiplication d'intervenants, réduisant le niveau de protection traditionnellement réputé résulter de la complexité du système et de son caractère relativement propriétaire.

La sécurité dont il est ici question, concerne la prévention des risques associés à des interventions malintentionnées sur des systèmes programmés de contrôle de procédé (SCADA, DCS, SNCC, PLC…) s'appuyant sur les techniques, matérielles ou logicielles, du monde de l'informatique et sur les réseaux de communication, y compris des réseaux sans fil, associés à ces systèmes.

Les auteurs de ces interventions peuvent être des « professionnels » de l'intrusion frauduleuse, y compris des criminels ayant des visées terroristes. Mais ils peuvent être plus simplement des « hackers » faisant du piratage leur distraction favorite et utilisant des logiciels téléchargés sur Internet, des concurrents peu scrupuleux, ou bien des personnels de l'entreprise ou l'ayant récemment quitté et ayant, pour une raison ou pour une autre, une réelle intention de nuire.[1]

Aucune statistique de « cyber-attaques » n'est disponible[2]. Souvent d'ailleurs les tentatives passent inaperçues et sont découvertes très tardivement. Cependant beaucoup d'articles publiés aux USA font état d'un nombre croissant de tentatives non autorisées d'accès à des systèmes d'information dédiés au contrôle.[3]

Les conséquences peuvent être, selon la nature des attaques, très différentes :

- mise en cause de la sécurité et de la santé du public et des employés,
- perte de confiance dans l'entreprise,
- violation de dispositions réglementaires,
- perte et/ou détournement d'informations propriétaires ou confidentielles,
- pertes de production,
- impact sur la sécurité locale, régionale voire nationale.

Les conséquences des cyber-attaques contre les systèmes de contrôle peuvent être extrêmement dévastatratrices. Les risques attachés à l'Internet et aux virus informatiques ont

[1] Une étude publiée en 2000 par le FBI et le Computer Security Institute on Cyber-crime a montré que 71% des atteintes à la sécurité étaient d'origine interne – Source : Words in collision – Ethernet and the factory floor – *Eric Byres et al.*

[2] *Joe WEISS* – Control system cyber-security – ISA Intech November 2004.

[3] La 5ème conférence « Cyber-security of SCADA and Process Control Systems » organisée par le KEMA à Albuquerque en août 2005 faisait état de 60 attaques identifiées dans le domaine des systèmes de contrôle industriels.

été très fortement médiatisés mais il faut reconnaître que peu d'installations sont réellement sécurisées. Les systèmes de contrôle sont des installations réputées professionnelles où les défaillances étaient jusqu'à présent l'exception. On découvre aujourd'hui que cette immunité appartient au passé et que les systèmes sont, comme les autres systèmes d'information, des cibles possibles pour le cyber-terrorisme, l'espionnage ou la simplement la malveillance.

La définition d'un « *Cyber-Security Management System (CSMS)* » doit s'inscrire dans le cadre d'une politique générale de sécurité dans les compagnies. Elle doit reposer une analyse aussi exhaustive et homogène que possible de tous les risques pesant sur une activité considérée. Elle implique une prise de conscience des responsables de l'entreprise au plus haut niveau et une sensibilisation de tous les échelons accompagnée de la diffusion d'instructions aussi opérationnelles que possible.

La cyber-securité, comme la qualité, se construit, pas à pas, au prix d'analyses, d'expériences, de retour d'expériences et d'essais de quantification des mesures prises. Mais elle constitue l'un des défis des sociétés modernes. Une protection efficace contre les cyber-attaques doit constituer désormais au même titre que le respect des normes environnementales, un élément significatif de la valorisation patrimoniale de toute entreprise industrielle ou commerciale.

2. La démarche de l'ISA et du groupe de travail ISA SP99

Comme précédemment indiqué, il existe différentes normes relatives à la sécurité de fonctionnement, en particulier la norme générique *IEC 61508, Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems*, et les normes dérivées mentionnées en Figure 1.

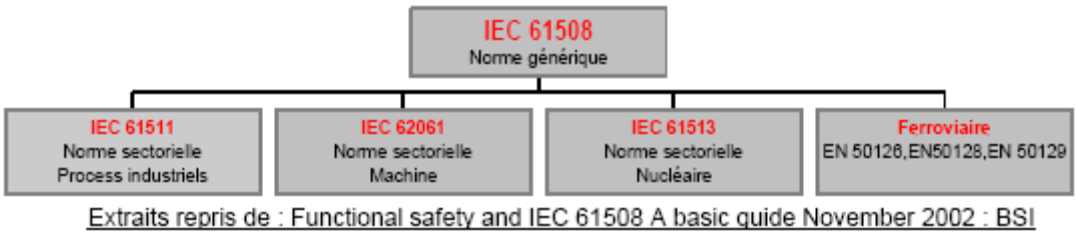

Figure 1 : Norme IEC 61508 et normes dérivées – Source: Guide d'interprétation et d'application de la norme IEC 61508 et des normes dérivées – ISA-France et Club Automation - www.isa-france.org

La norme IEC 61508 développe une approche intéressante, en ce sens où elle propose quatre niveaux de sécurité : les Safety Integrity levels (SIL), s'étageant du SIL1 au SIL4.
La norme ISA S84.01, développée aux USA dans un esprit similaire aux normes IEC, s'identifie à présent à la norme IEC 61511.

Mais au moment de la conception de ces normes, les systèmes de contrôle pouvaient encore être considérés comme isolés de l'environnement informatique général et utilisaient des réseaux de communication, des stations de travail, des « operating systems » spécifiques, ce qui rendait le problème de la vulnérabilité aux intrusions moins critique qu'à présent.

L'ISA[4] a donc décidé de mettre en œuvre une approche spécifiquement dédiée au domaine des automatismes et du contrôle de procédé.

Cette approche, développée au sein d'un groupe de travail, l'ISA SP 99, comporte plusieurs étapes :

- L'élaboration de deux rapports techniques finalisés mi 2004 et téléchargeables sur le site www.isa.org:

    o ISA-TR99.00.01, *Security Technologies for Manufacturing and Control Systems,* qui est un « tutorial » sur les technologies du monde informatique potentiellement utilisables dans les systèmes de contrôle, permettant d'évaluer leur intérêt au regard de la capacité de résistance aux cyber-attaques.

    o ISA-TR99.00.01, *Integrating Electronic Security into the Manufacturing and Control Systems Environment,* qui propose une approche pour auditer un système, déterminer ses failles éventuelles face aux différentes attaques dont il peut être l'objet et faciliter la vérification de la bonne application des mesures de mise en conformité face aux recommandations formulées.

- L'élaboration d'une norme qui s'appuiera sur les rapports techniques précédemment publiés, définira une méthode d'évaluation et pourra déboucher sur une classification en niveaux de maturité au regard du risque de cyber-attaque, permettant à chaque installation de définir et de mette en oeuvre un plan d'améliorations.

Cette approche de l'ISA rencontre un vif succès et est reprise et précisée dans des documents sectoriels. Le lecteur pourra notamment consulter le document « Guidance for addresssing cyber-security in the chemical sector ».[5]

[4] The Instrumentation , Systems ans Automation Society, organisme non lucratif comptant plus de 30 000 membres, essentiellement basé aux USA, mais comportant des représentations dans le monde entier dont la section française ISA-France : www.isa-france.org , liée à la SEE par un accord de coopération.

[5] Voir www.cidx.org

3. Le rapport technique ISA-TR99.00.01: *Security technologies for manufacturing and control systems.*

Ce rapport propose une revue des différentes technologies sécuritaires présentement disponibles et applicables en environnement de production et de contrôle de procédé : avantages, inconvénients, contraintes de mise en oeuvre et directions possibles pour le futur. Le concept de systèmes de contrôle est pris dans son sens le plus large et inclus tous types d'installations et tous types d'équipements et de façon non limitative :

- les DCS, PLC, SCADA, réseaux de capteurs, de surveillance et d'évaluation des systèmes,

- les interfaces homme-machine associées destinées au contrôle, à ma la sécurité, à la maintenance, à la configuration, pour des applications batch, continues ou discrètes.

Parmi les technologies évaluées, on citera ;

- l'authentification et l'autorisation

- le filtrage, le blocage, le contrôle d'accès,

- le cryptage,

- la validation des données,

- l'audit,

- la mesure,

- les outils de surveillance et de détection,

- les operating systems,

- la sécurité physique des systèmes.

Le rapport technique contient un glossaire définissant le sens à donner aux principales expressions et aux principaux acronymes utilisés dans le domaine de la cyber-sécurité des systèmes de contrôle de procédé.

4. Le rapport technique ISA-TR99.00.02: *Integrating electronic security into the manufacturing and control system environment.*

Le but de ce rapport est de proposer une approche cohérente pour définir, mettre en oeuvre et suivre l'exécution de programmes d'action relatifs à la cyber-sécurité dans les systèmes d'automatisme ou de contrôle de procédé.

Il s'adresse aux utilisateurs, fabricants, fournisseurs et responsables de la sécurité de tels systèmes.

Le rapport insiste sur trois recommandations :

- *identifier les risques et estimer les conséquences,*

Le document développe une proposition de méthode d'analyse basée sur l'examen physique de la structure du système et sur l'identification des points d'ouverture externe, ainsi que sur une évaluation quantitative de la probabilité du risque d'agression et du niveau de criticité des conséquences pouvant en résulter.
Il préconise par exemple d'établir un schéma détaillé du système mettant en évidence toutes les liaisons internes et externes entre équipements constitutifs (Figure 2).

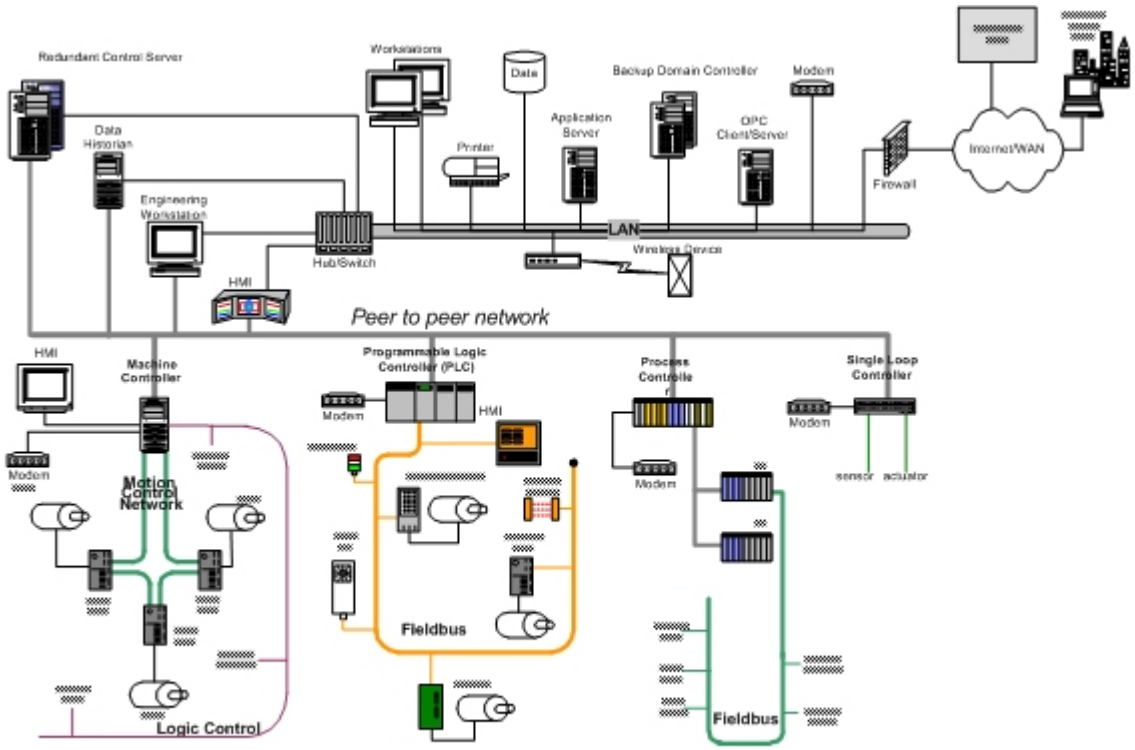

Figure 2 : Plan-type d'un système identifiant les connexions entre composants et les points d'ouverture externe.

.Le document développe une proposition de méthode d'analyse basée sur l'examen physique de la structure du système et l'identification des points d'ouverture externe ainsi que sur une évaluation quantitative de la probabilité du risque d'agression et du niveau de criticité des conséquences.

Il est recommandé d'établir des tableaux d'analyse (ou « grilles de balayage ») pour chaque ressource (réseaux de communication, station physique ou programme) identifiant la probabilité d'attaque, la criticité et mentionnant les protections jugées adéquates (Figure 3).

Probabilité	Criticité
A = Très forte	1 = Impact sévère
B = moyenne	2 = Impact majeur
C = faible	3 = Impact mineur
D = très faible	4 = pas d' Impact

Segment de communication	Probabilité d'attaque
Internet, Wireless, connexion directe sur modem…	A
Internet, connexion modem sécurisée…	B
Réseau de contrôle intégré avec réseau de gestion..	C
Réseau de contrôle isolé	D

Catégorie d'Impact	1 = Sévère	2 = Majeur	3 = Mineur	4 = aucun
Atteinte aux personnes	Perte de vie, amputation.	Hospitalisation	Blessures légères	Aucun
Perte financière	Millions	$100,000	$1,000	Aucune
Rejet dans l'environnement	Dégâts permanents/rejets hors site	Dégâts persistants	Dégâts temporaires	Aucun
Interruption de Production	semaine	jours	Minutes	Aucun
Image publique	Dégradation Permanente	Blâme de longue durée	Ternissement temporaire	Aucun

Figure 3 : Evaluation quantitative du niveau de probabilité d'attaque et de criticité (ex : réseau de communication)

- *mettre en place un « cycle de vie » de la sécurité,*

- *mettre en place un processus de validation et de surveillance en exploitation.*

Il s'agit in fine démontrer par des techniques de vérification appropriées que la management de la sécurité est correctement mis en oeuvre et efficace dans son application. Ceci implique la définition et l'exécution d'une batterie de tests homogènes avec l'analyse initiale.

Ultérieurement, des audits réguliers doivent permettre de s'assurer que le programme d'amélioration se met en place selon l'échéancier prévu et conserve l'efficacité attendue. Des procédures de reporting doivent être prévues et respectées afin que chaque observation soit suivie d'effet.

5. La norme ISA en cours d'élaboration

Face au succès aux USA de son initiative, aussi bien du côté des exploitants que du côté des offreurs, l'ISA a décidé de publier en 2005 des documents à caractère normatif.

Le standard en cours de finalisation vise à couvrir ce qui est spécifique aux systèmes de contrôle, c'est à dire en prenant pour référence le modèle le plus récent de découpage en « niveaux » (ANSI/ISA-95). Les niveaux 1 à 3 sont directement concernés. Le niveau 4 « gestion de production et logistique » se trouve exclu du fait qu'à ce niveau sont utilisées les techniques de l'informatique générale, toutes mesures devant cependant être prises pour préserver l'intégrité des données en provenance des niveaux inférieurs (Figure 4).

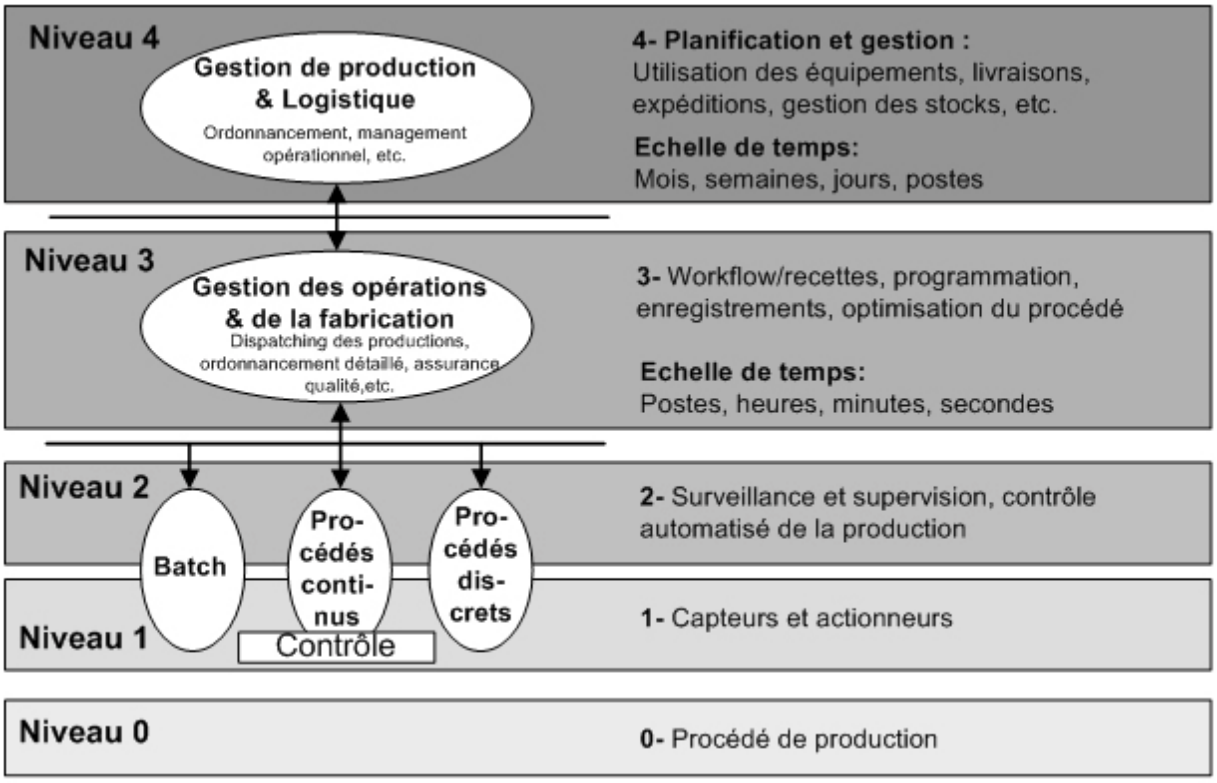

Figure 4 : Les niveaux selon la norme ISA95.

- La première partie du standard (**Models and Terminology)** décrit le contenu du standard, définit la terminologie, propose une double modélisation (modélisation physique et modélisation fonctionnelle) des systèmes de contrôle vis à vis de la sécurité et introduit un concept de découpage des systèmes de contrôle en « **zones de sécurité »**, avec identification des **« conduits »** d'information à protéger entre ces différentes zones.

Zones et conduits :

Une **zone de sécurité** est un regroupement logique de ressources ayant les mêmes exigences en matière de sécurité. Une zone se définit à partir des modèles physique et fonctionnel de l'architecture de contrôle.Une politique de sécurité relative à chaque zone peut alors être fixée.

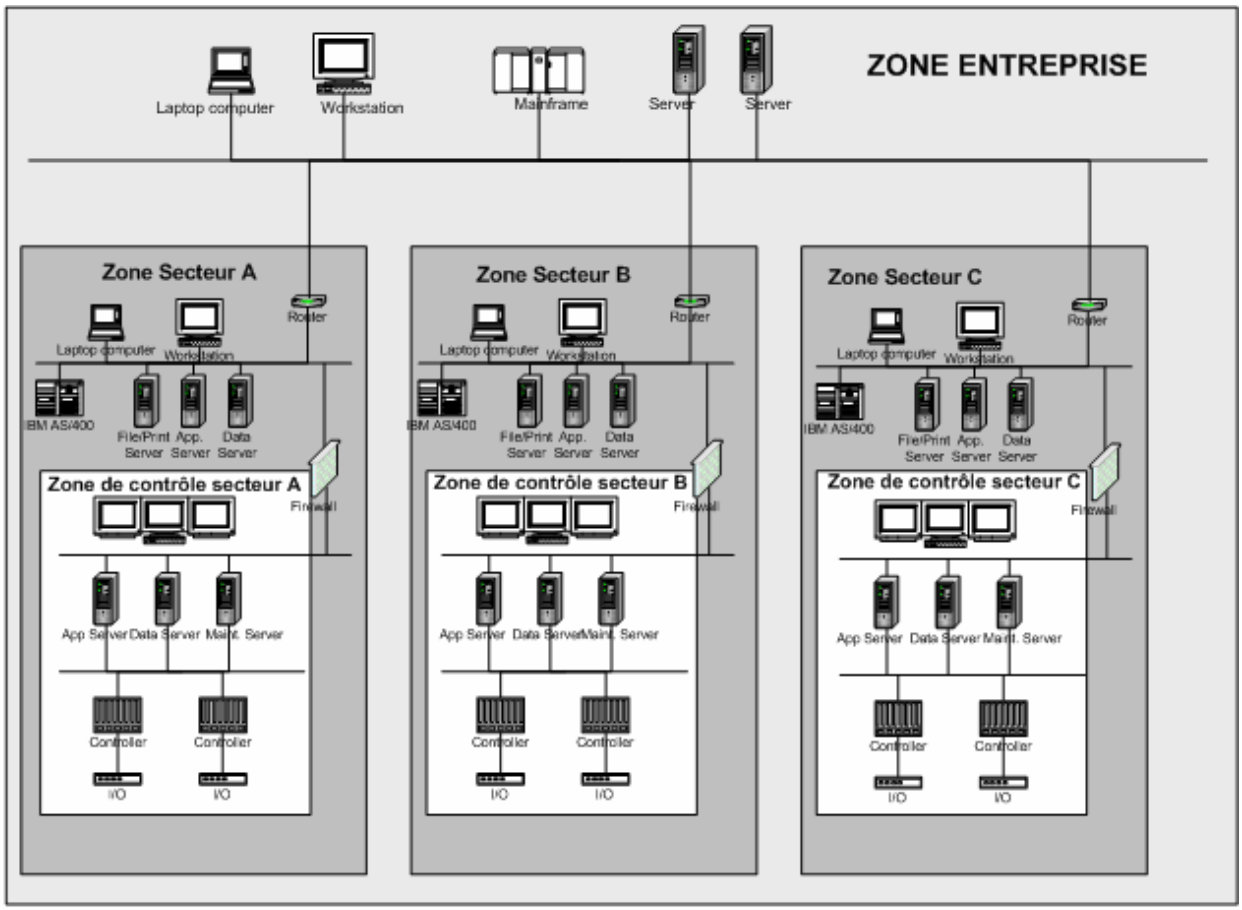

Figure 5 : Découpage d'un système en zones de sécurité

Le processus de définition des **« zones »** démarre à l'aide du modèle de représentation « physique » du système sur lequel viendront se greffer les fonctionnalités et les activités (de l'exploitation à la maintenance, en passant par les réglages). Lorsqu'une ressource supporte plusieurs fonctions, ou activités, on l'affecte à une zone correspondant à l'exigence de la fonction la plus contraignante, ou bien on crée une zone séparée dotée d'une politique spécifique de sûreté.

A titre d'exemple on peut citer les serveurs d'historiques. Pour fonctionner, ces serveurs doivent accéder aux données critiques de fonctionnement. Mais, du point de vue de la sécurité, ils relèvent davantage de la gestion car de nombreux utilisateurs potentiels (superviseurs, équipe d'optimisation de procédé, statisticiens, contrôleurs qualité) sont intéressés par les données recueillies et doivent disposer d'un accès aux informations. Dans ce cas, on peut envisager de créer une zone spécifique pour ces serveurs, voire créer une zone d'accès libre : « Demilitarized zone (DMZ) ».

Un « **conduit »** désigne les moyens de communication entre éléments de l'architecture. Un conduit regroupe plusieurs ressources permettant d'assurer un canal de communication, externe (entre zones différentes) ou interne (à l'intérieur d'une même zone). Ces conduits englobent et protègent les différents canaux de communication, équivalent à des « câbles » en fournissant les liens entre les ressources du système.

Le plus souvent un conduit est matérialisé par un réseau de communication et les composants qui le supportent : connectique, câblage, routeurs, commutateurs, stations de gestion ou de maintenance du réseau. Les conduits peuvent regrouper des profils de communication différents et aussi comporter plusieurs « canaux de communication » utilisant le même support physique. Par exemple, sur un réseau de terrain, peuvent cohabiter un trafic cyclique de données de contrôle de procédé et un ou plusieurs trafics de messagerie d'observation, configuration et réglage, chacun des canaux ayant des exigences et vulnérabilités différentes vis à vis de la sécurité. Ces conduits servent de base à l'analyse des vulnérabilités et des risques potentiels pouvant exister au niveau de la communication à l'intérieur d'une zone et au niveau des échanges entre zones de classes différentes.

- La deuxième partie du projet de standard inclut les références normatives, la description d'un système de gestion de la sécurité pour les systèmes de contrôle, la proposition de niveaux de maturité pour la mise en place des protections au niveau d'une usine ou d'une entreprise, les prescriptions pour la mise en place d'un programme de sécurité (analyse de risque et vulnérabilité, cycle de vie de la sécurité, contre-mesures, traitement des incidents, processus d'amélioration permanent). Elle reprend en annexe la méthodologie d'analyse de risques développée à l'occasion de la publication du second rapport technique.

Il n'est évidemment pas possible de réduire la mise en place d'une politique de sécurité à l'application de règles préfabriquées. Le projet de standard ISA99 propose un guide de conduite identifiant les éléments à prendre en compte dans la définition d'une telle politique et donne un canevas de mise en oeuvre pour les systèmes de contrôle.

Nous terminerons cet article en résumant les lignes directrices permettant de comprendre le processus de la mise en place d'une politique de sécurité selon ce projet de standard.

6. Comment bâtir un programme de cyber-sécurité

Bâtir un programme de « cyber-sécurité » dans une société est une tâche délicate. Par où commencer ? Dites moi ce que je dois faire ? Telles sont les questions initiales les plus fréquemment posées. Malheureusement, il n'existe pas de recette unique en raison de la variété des contextes (système nouveau ou amélioration d'un système existant, niveaux de maturité et de diversité des technologies…et des intervenants). En fait la réponse ne peut être que relative et s'intégrer dans la politique générale de l'entreprise. La sécurité parfaite est un idéal et une solution de compromis est à rechercher en considérant le coût du développement face au coût des conséquences des risques potentiels.

Niveau de maturité de cyber-sécurité

Plutôt que de définir des recettes et des niveaux prédéterminés de maturité, l'idée de base du futur standard est de considérer, pour une installation donnée, l'état de l'art intégrant les meilleures connaissances actuelles et de comparer la situation constatée dans une installation à ces meilleures pratiques. Il est alors possible de se faire une idée précise du niveau de maturité de cyber-sécurité atteint et d'élaborer un programme d'amélioration de la cyber-sécurité qui sera, en règle général, incrémental dans sa mise en œuvre et qui permettra de se rapprocher des meilleures pratiques..

Bon nombre de société ont d'ores et déjà mis en œuvre des mesures de protection de leur système informatique mais bien moins nombreuses sont celles qui ont étendu ces mesures à

leur système de contrôle de production. Comme aujourd'hui les technologies « ouvertes » de l'informatique sont utilisées à grande échelle dans les systèmes de contrôle de production, un niveau d'expertise supplémentaire est requis pour pouvoir utiliser de façon sûre ces technologies dans le contexte de conduite de procédé. Informaticiens et automaticiens doivent travailler en étroite collaboration et mettre en commun leurs connaissances pour traiter efficacement les problèmes de cyber-sécurité.

Dans les industries à risques vis à vis de la sûreté, de la santé publique ou de l'environnement, il est important de mettre en place un processus rationnel de gestion de la sécurité et une politique de contrôle des accès. Le but à atteindre est un programme de sécurité « mature », c'est-à-dire connu, maîtrisé et respecté par l'ensemble des personnes concernées et intégrant tous les aspects de la cyber-sécurité y compris la bureautique et l'informatique conventionnelle, le système de gestion et le système de contrôle du procédé. La cyber-sécurité doit couvrir l'ensemble de la chaîne de production et tout le cycle de vie, depuis la conception jusqu'au stade final de la vente et de l'après-vente, en prenant en compte les clients, les fournisseurs et les sous –traitants.

Elle suppose, de la part de l'entreprise, un effort de « rattrapage » portant prioritairement sur la sécurité du contrôle de production de telle sorte, qu'in fine l'entreprise présente un niveau de protection homogène vis-à-vis des cyber-attaques, niveau difficile à quantifier dans l'absolu mais que l'entreprise, en fonction de son activité, de son histoire, de son expertise, du contexte dans lequel elle opère, peut discrétiser en paliers successifs de progrès dans le cadre d'un plan d'amélioration faisant partie de sa stratégie d'ensemble (Figure 6).

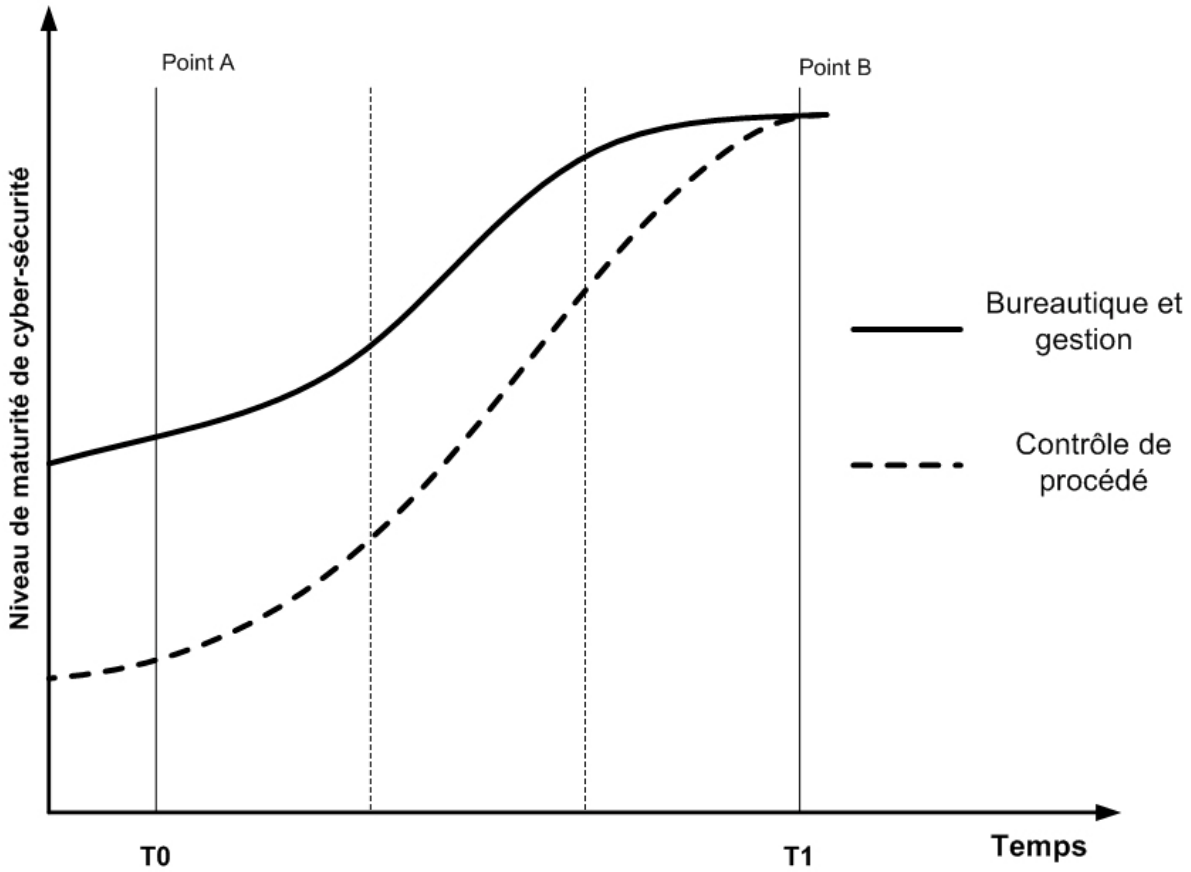

Figure 6 : Courbe de maturité pour un système intégré de gestion de la sécurité.

Etablissement du système de gestion de la cyber-sécurité

Le résultat à obtenir doit être une situation cohérente couvrant toutes les activités de la société, incluant le système de contrôle, la gestion, toute la chaîne de création de valeur y compris les relations avec les divers partenaires (clients, fournisseurs, transporteurs, sous-traitants) mais on comprend que l'effort à réaliser variera fortement d'une société à une autre.

La démarche nécessite un brassage de culture des intervenants et doit être pragmatique et progressive. Le programme général de cyber-sécurité doit prendre en compte le niveau de risque, qui peut être différent d'un type d'activité à un autre, ainsi que les différents modes d'exploitation.

Une attention particulière devra être portée à la convergence progressive des cultures des informaticiens d'une part et des « gens de procédé et de contrôle de procédé » d'autre part. Ou du moins, l'une et l'autre des populations devront-elles comprendre et admettre les spécificités de chacun des métiers, avec le souci de parvenir à une situation homogène dans l'entreprise.
En particulier, le personnel de contrôle de procédé devra être formé aux enjeux et aux technologies de cyber-sécurité. Le personnel informatique devra lui être initié à la compréhension des technologies et des contraintes des techniques de contrôle de procédé.

Comme le montre schématiquement la Figure 7, c'est de l'intégration des ressources d'origine diverse dans l'entreprise et de la mise en commun de leur expertise et de leur expérience que naîtra le progrès en matière de cyber-sécurité.

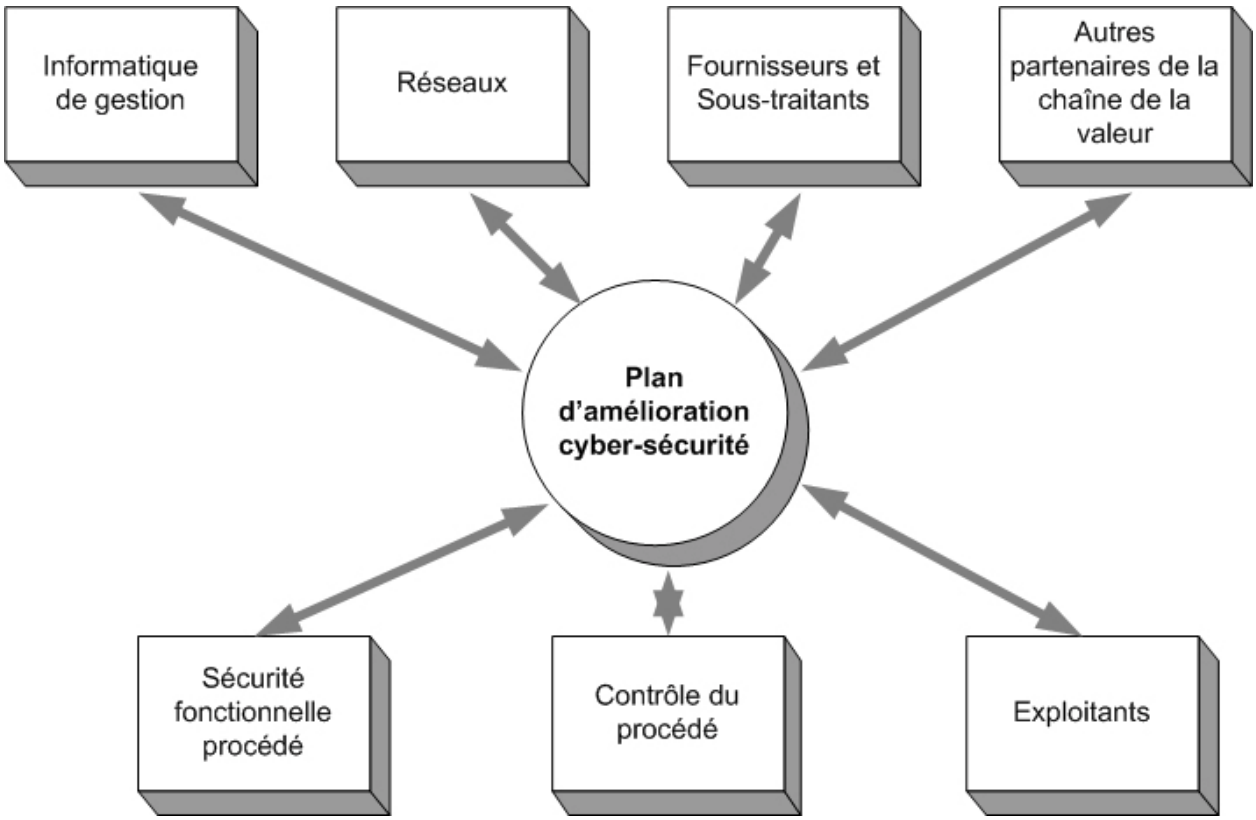

Figure 7 : Intégration des ressources de l'entreprise dans l'élaboration du plan d'amélioration de la cyber-sécurité.

Le système de cyber-sécurité constitue une structure d'accueil de l'ensemble de la politique et des actions collectives menées dans la société.

Au fur et à mesure de la réalisation des actions le niveau de maturité de cyber-sécurité s'accroît. Le projet de standard identifie et détaille les éléments jugés fondamentaux pour l'établissement et la mise en œuvre d'un programme efficace. De façon classique, ces éléments sont répartis en quatre phases principales, identiques à celles rencontrées dans les processus d'amélioration de la qualité (Figure 8).

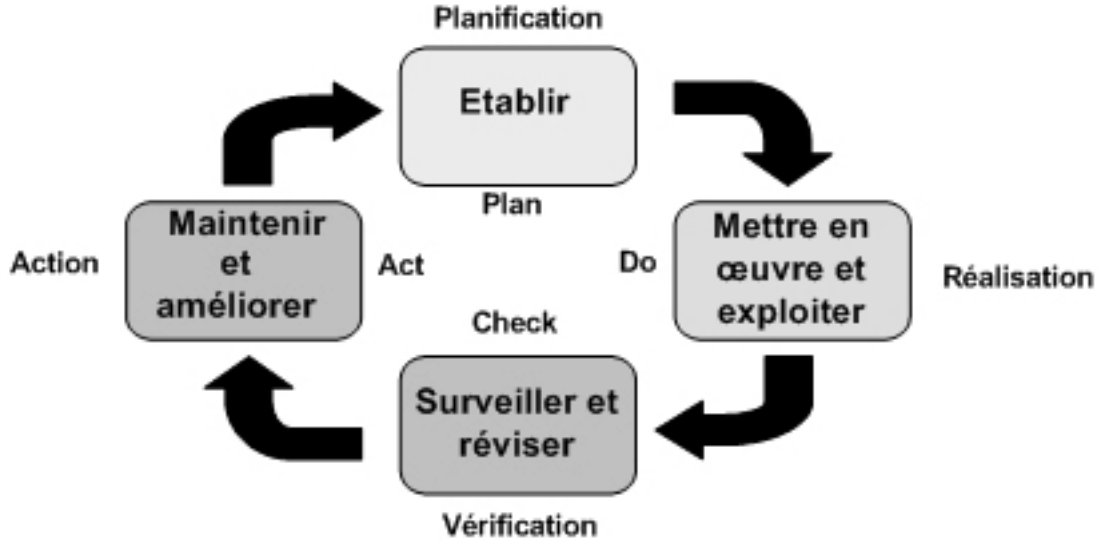

Figure 8 : Etapes principales d'établissement du système de gestion de la cyber-sécurité

Planification: établissement des limites du système et de la politique de la société, identification, classification et évaluation des risques, développement d'un plan stratégique d'action continue.

Réalisation: mise en oeuvre, exploitation et maintenance du système .Ceci couvre en particulier l'organisation transversale mise en place, la sécurité physique, es contrôles d'accès, les procédures de traitement des incidents, la gestion des communications, de l'exploitation et de la documentation.

Vérification: surveillance, évaluation et mesures d'efficacité du système. Organisation des rapports et revues périodiques de résultats**.**

Action: organisation des actions correctives et préventives. Actions de maintien à niveau. Ces actions sont des actions permanentes pour maintenir le niveau de protection au niveau de sécurité voulu.

Le standard détaille chaque élément des actions à mener et guide dans leur réalisation, en s'appuyant sur des expériences concrètes dans divers domaines d'activité. La mise en place des divers éléments s'effectue progressivement avec un certain recouvrement entre actions. La formation est une activité transversale et continue.

7. L'intérét des normes ISA pour les industriels et les exploitants

La sensibilité aux agressions potentielles des systèmes de contrôle est, pour l'instant, moins vive en Europe qu'aux Etats-Unis, en partie du fait qu'il n'existe pas de règles et recommandations spécifiques équivalentes à celles préparées par l'ISA.Cependant, il nous semble extrêmement judicieux pour les industriels européens de prendre, comme leurs partenaires ou concurrents américains, des mesures préventives appropriées, fondées sur

l'expérience et les connaissances rassemblées dans les documents produits par l'ISA. Cette démarche peut leur éviter beaucoup de tâtonnements et de recherches coûteuses.

Les documents aujourd'hui disponibles incluent des outils facilitant la mise en œuvre du standard : grille d'évaluation du niveau de maturité, méthode d'identification, d'analyse et d'évaluation des risques.
Pour les installations nouvelles, les documents de l'ISA aident à intégrer dès le début la préoccupation de cyber-sécurité dans la réflexion sur le cycle de vie global du système, de façon à optimiser les coûts de protection.

Pour les offreurs de systèmes et intégrateurs, il sera sans doute de plus en plus nécessaire de proposer aux utilisateurs finaux des solutions de sécurité intégrées à l'offre de façon native, selon un standard universellement reconnu. Le projet de standard inclut à cette fin une rubrique de prescription spécifique dédiée aux vendeurs de système.

Les 10 et 11 mai 2006, un séminaire international sera organisé par l'ISA-France (www.isa-france.org) à Nice afin de présenter plus en détail au monde industriel l'approche de l'ISA en matière de cyber-sécurité.

Jean-Pierre Dalzon, Ingénieur AINPG, a été longtemps responsable chez Cégélec puis ALSTOM du Marketing et de la définition des systèmes des systèmes de contrôle dédiés aux applications critiques notamment dans le secteur de l'énergie. Il consacre actuellement une partie de son temps à l'étude des améliorations technologiques et normatives dans le cadre d'associations scientifiques et professionnelles et est notamment l'un des leaders technologiques d'ISA-France.

Jean-Pierre HAUET, a dirigé le centre de recherches de Marcoussis d'Alcatel avant d'être directeur Produits et Techniques de Cégélec. Il a été nommé Chief Technology Officer d'ALSTOM, lors de l'acquisition de Cégélec par cette dernière. Depuis 2003, il est consultant, Associate Parnter de BEA Consulting. Il préside l'ISA-France, section française de l'ISA.

Références :

Rapport ISA TR99.00.01: “Security Technologies for manufacturing and control systems”. www.isa.org

Rapport ISA TR99.00.02: “Integrating Electronic Security into the manufacturing and control systems environment”. www.isa.org

Travaux du groupe de travail ISA SP99. www.isa.org

Joe Weiss: “Control system cyber-security” – ISA Intech Nov 2004.

Jean-Pierre Dalzon : « Ne laissez pas votre système de contrôle ouvert au piratage » – Journée 2004 Club de la Mesure Provence Côte d’azur.

CIDX: Guidance for addressing cyber-security in the chemical sector. www.cidx.org

Bryan L. Singer: ISA SP99 Proposed architecture and plan.

Eric Byres, Joël Carter, Amr Elramly, Dr. Dan Hoffman – Worlds in collision – Ethernet and the factory floor.

Eric Byres, Ron Derynck and Nicholas Sheble: SP99 counterattacks – Intech 2004