La cyber-sécurité des automatismes et des systèmes de contrôle de procédé. Le standard ISA99

Jean-Pierre Hauet
Associate Partner KB Intelligence
Président d'ISA-France
Membre émérite de la SEE

Un problème maintenant pris au sérieux

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 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 transport, installations réputées sensibles – chimie, pharmacie, agro-alimentaire.

Mais pendant plusieurs années, cette menace a été perçue par beaucoup comme une « paranoïa », cultivée par des organisations ou des consultants davantage préoccupés par le développement d'un nouveau business que par l'intérêt général. La théorie de « l'air gap », c'est-à-dire de la protection par l'isolement du monde extérieur, était encore dominante jusqu'à une date récente et, dans l'industrie, la plupart des responsables de systèmes de contrôle de procédé ne croyaient pas, pas plus que leur hiérarchie, à la réalité de la menace.

On observe, depuis la fin 2011, une évolution sensible de cet état d'esprit, en France comme à l'étranger. Il est vraisemblable que l'attaque **Stuxnet** de 2010, largement médiatisée, a largement contribué à rendre crédible la menace aux yeux des responsables concernés. Cette attaque, mettant en œuvre une construction informatique malveillante, un malware, d'une complexité jamais rencontrée, était directement ciblée sur un type d'équipements, des automates Siemens en l'occurrence, avec l'objectif, assez largement atteint semble-t-il, de créer des dommages aux centrifugeuses de l'usine d'enrichissement d'uranium de Natanz en Iran, dont des automates de ce type pilotaient les moteurs. La sophistication de ce malware a étonné par son aptitude à pénétrer dans les systèmes (par le canal de clés USB ou de failles réseaux), à s'implanter de façon discrète – masqué par des certificats d'authenticité volés – à reconnaître son entourage, à se propager de façon sélective en direction des cibles visées, à collecter de l'information, à la transmettre à l'extérieur, à corrompre de façon sélective certains programmes implantés sur certains types de machi-

ABSTRACT

The need to ensure the cyber-security of automation and process control systems is now recognized. It results, in particular, of the attacks that marked the years 2010 and 2011 (Stuxnet, Night Dragon, DuQu). The problem is a very complex one because of the complexity to imagine all the threats which a system may face and, still more difficult, to fight against.
The ISA (International Society of Automation) is currently completing the development of a set of standards, extending to cyber-security the approach developed within ISA84 and IEC 61508 to address functional safety issues. These ISA99 standards, whose main constituents are already certified IEC 62443, provide a methodological framework that can bring the rationality and the consistency in an area usually out of reach of an objective probabilistic approach and often treated in a more incantatory than rational way. The ISA99 standards rely on the definition of seven Functional Requirements which have to be fulfilled to a certain degree depending on the risk analysis and ranging from 1 to 4, according to precise criteria.
One of the essential contributions of the ISA99 is based on the systematic application of the principles of defense in depth and on the decomposition of systems into zones and conduits. The concept of SAL vectors (Security Assurance Level) permits to characterize the confidence level and guides the operators in the search of proportionate and effective solutions.

nes, etc. Personne ne sait au juste combien de centaines de milliers de PC ou d'automates, restés à l'état de porteurs sains, ont pu être contaminés. Mais la puissance de l'attaque qui tranchait singulièrement avec les attaques traditionnelles par vers, virus ou chevaux de Troie, a étonné et inquiété.

Peu de temps avant Stuxnet, l'attaque « Night Dragon », en « spear phishing » (ou harponnage), avait été identifiée comme venant probablement de Chine avec pour objectif de pirater de l'information au sein d'une douzaine de sociétés spécialisées dans les hydrocarbures, l'énergie et la pétrochimie.

Peu de temps après, l'attaque « DuQu », qualifiée de « The precursor of the next Stuxnet », était détectée par un laboratoire universitaire de Budapest, le Crysys, et documentée par Symantec dans plusieurs publications[1].

Si l'on ajoute à cela les attaques ponctuelles (plus ou moins avérées, il est vrai) qui ont été répertoriées depuis dix ans sur des centrales électriques, des réseaux de distribution d'électricité, des installations de traitement de l'eau – attaques rapportées sur différents sites dont celui du RISI au Canada (Repository of Industrial Security Incidents), il faut convenir qu'il n'est plus possible de considérer les cyber-attaques comme un risque marginal pour les installations de contrôle, notamment celles pilotant les grandes infrastructures publiques ou privées.

En décembre 2011, le FBI reconnaissait le nombre croissant de cyber-attaques contre des installations de SCADA[2] et décidait d'accroître son « cyber-budget ».

Les systèmes de contrôle industriel sont devenus vulnérables

Les systèmes d'automatisme et de contrôle de procédé (IACS en anglais) sont devenus vulnérables aux cyber-attaques pour trois raisons essentielles :

- **La mise en réseau des systèmes de contrôle est devenue systématique**

  Cette mise en réseau a beaucoup d'avantages. Elle permet la surveillance à distance, le debugging et la maintenance. Elle donne accès à des données en temps réel, pour des applications critiques telles que l'équilibrage des réseaux électriques. Elle permet l'intégration des réseaux de contrôle et des réseaux d'entreprise, dans le cadre de la mise en œuvre de progiciels de gestion intégrés, communément désignés MES (Manufacturing Execution System) et ERP (Entreprise Resource Planning).

  Cette intégration constitue évidemment un facteur de productivité majeur mais elle a ouvert de nombreux points d'accès aux systèmes de contrôle qui n'existaient pas auparavant. Le développement des radiocommunications, notamment vers les laptops, les PDA, les smartphones, peuvent également ouvrir de nouvelles brèches si les protections nécessaires ne sont pas mises en œuvre.

- **L'utilisation de produits sur étagère (COTS)**

  Le recours à des produits informatiques sur étagère, matériels ou logiciels, est une autre tendance lourde des vingt dernières années. Il n'est pas question d'en revenir, tant les gains en coût et en performances ont été élevés. Mais l'industrie s'est dotée de piles de protocoles de communication non durcis, de systèmes d'exploitation banalisés, pour les stations opérateurs ou d'ingénierie, et d'applications non régulièrement mises à jour. Les COTS sont des boîtes noires, dont l'utilisateur n'a pas la maîtrise. Les IACS sont ainsi devenus progressivement une proie pour toute sorte de logiciels malveillants.

- **Absence de politique de management de la cyber-sécurité**

  La troisième raison est organisationnelle, voire culturelle. Alors que les responsables des systèmes d'information ont pris assez rapidement conscience du risque encouru, dans le monde industriel les choses ont évolué plus lentement ; la surveillance des visiteurs ou des sous-traitants reste souvent insuffisante, les droits d'accès consentis aux employés sont gérés avec relâchement, les mots de passe, lorsqu'ils existent, ne sont pas mis à jour ou sont bien trop faibles.

  Aujourd'hui le risque est reconnu et on ne peut plus prescrire l'installation de systèmes de contrôle évolués sans simultanément traiter les questions de cyber-sécurité. Ces risques peuvent avoir des conséquences graves :
  - pertes de production ;
  - pertes de données sensibles ;
  - incidents sur le procédé, détérioration d'équipements ;
  - mise en danger des personnels d'exploitation et de la santé publique ;
  - atteintes à l'environnement et violation de dispositions réglementaires ;
  - détérioration de l'image de marque de l'entreprise.

  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 simplement la malveillance. L'ISA (International Society of Automation) en a pris conscience en lançant un comité de standardisation, l'ISA99, dont l'objet est de développer un ensemble de standards, de bonnes pratiques et

[1] Voir CrySys : http://www.crysys.hu/ et Symantec : http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet

[2] SCADA: Supervisory Control and Data Acquisition

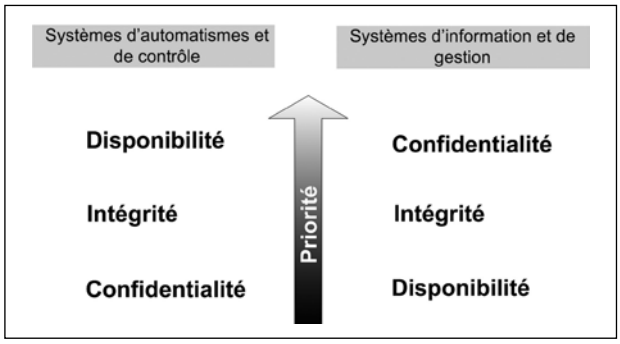

Figure 1 : Les priorités relatives dans les systèmes d'automatismes et de contrôle et dans les systèmes d'information et de gestion.

de recommandations techniques visant à contenir la menace cyber-sécuritaire.

La cyber-sécurité des installations industrielles à la croisée de plusieurs chemins

- Les solutions applicables aux systèmes d'information sont utiles mais ne suffisent pas

Il y a bien évidemment, du fait même de la banalisation des produits informatiques, des liens de parenté étroits entre cyber-sécurité des systèmes de contrôle et cyber-sécurité des systèmes d'information. Toutefois, les solutions développées pour assurer la cyber-sécurité des systèmes d'information ne suffisent pas ou sont mal adaptées.

Deux facteurs de différentiation importants sont à souligner :

• **Les systèmes industriels sont beaucoup plus complexes que les systèmes d'information**

Les matériels sont très diversifiés : stations de travail, serveurs mais aussi automates, capteurs et actionneurs intelligents, variateurs de vitesse, réseaux de toute nature (Ethernet, réseaux de terrain, réseaux temps critique), modems, équipements de radiocommunication, lecteurs d'étiquettes radiofréquences, alimentations de secours (UPS), etc. Ces équipements sont rarement homogènes et résultent souvent d'une accumulation dans le temps. Les personnels qui y ont accès sont très divers : ingénieurs de conception, d'exploitation, techniciens de maintenance, sous-traitants et prestataires externes, etc.

• **Les priorités sont différentes**

Usuellement la sécurité se décline en trois préoccupations principales : la confidentialité, l'intégrité et la disponibilité. Les systèmes d'information et de gestion nécessitent que l'on porte beaucoup d'attention à la confidentialité des données alors qu'au niveau du procédé, c'est la continuité de fonctionnement et donc la disponibilité qui l'emportent.

- Des similitudes, mais des différences avec la sécurité fonctionnelle

On sait que la « safety » (notion mal traduite en français par le terme de sécurité) a trait aux mesures prises pour protéger un système contre des dommages pouvant résulter d'incidents ou d'accidents involontaires. La notion s'applique également aux caractéristiques de l'état qui en résulte : être « safe », c'est par exemple se mettre à l'abri d'un ouragan. La sécurité fonctionnelle (functional safety), appelée encore parfois sûreté de fonctionnement, est la partie de la « safety » qui dépend du bon fonctionnement d'un système ou d'un équipement actif. Un système de détection de fumées relève de la sécurité fonctionnelle, alors qu'une porte résistant au feu n'en relève pas.

La norme CEI 61508 s'applique aux systèmes automatisés, désignés E/E/PE[3], dont la défaillance d'un composant peut mettre en cause la « safety » des personnes et de l'environnement. Lorsque de tels systèmes présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses sécurités sont mises en œuvre. Les systèmes instrumentés de sécurité (SIS) sont utilisés comme moyens de prévention pour réaliser des fonctions instrumentées de sécurité telles que l'on puisse, grâce à elles, avoir une confiance suffisante dans la capacité du système à amener et/ou à maintenir le procédé dans un état sûr. La norme CEI 61508, issue de la norme ANSI/ISA-84.00.01, fixe les prescriptions relatives à la spécification, la conception, l'installation, l'exploitation et la maintenance d'un SIS, et définit en particulier la notion de SIL (Safety Integrity Level, ou niveau d'intégrité de sécurité) qui est un scalaire, allant de un à quatre, caractérisant le niveau de sécurité fonctionnelle offert par un SIS.

Un certain nombre de types de menaces, internes ou externes au système, contre lesquelles il y a lieu de se protéger, ont été prises en compte lors de l'élaboration des normes ISA84 et CEI 61508 : défaillances matérielles, défauts logiciels, effets de la température, de l'humidité, des agressions électromécaniques, etc. Mais les menaces d'attaque cyber-sécuritaire étaient quasiment ignorées. L'apparition du risque cyber-sécuritaire a conduit à identifier un nouvel ensemble de menaces contre lesquelles il faut se prémunir, comme en sécurité fonctionnelle, par des contre-mesures appropriées, mais qui diffère de la sécurité fonctionnelle par deux facteurs qui rendent le problème beaucoup plus complexe :

• les attaques sont délibérées ;
• en conséquence, elles ne sont pas probabilisables de façon objective, à la différence de la défaillance des composants électroniques.

[3] E/E/PE = Electrical, Electronic, Programmable Electronic

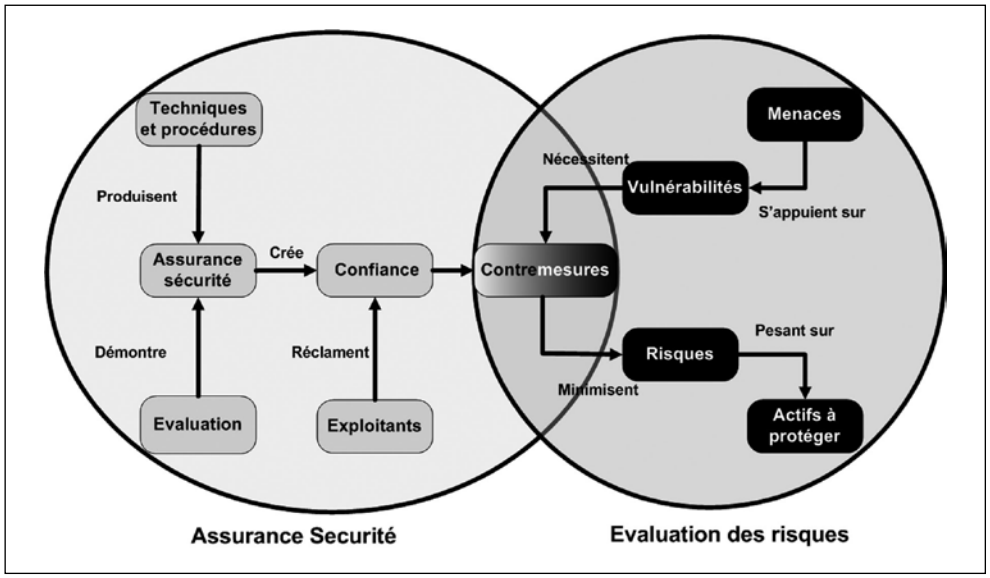

Figure 2 : Approche générale de l'ISA99.

A contrario, la cyber-sécurité peut bénéficier des expériences de Pasteur sur l'absence de génération spontanée : la menace vient toujours de quelque part, et par conséquent la protection cyber-sécuritaire peut et doit se focaliser exclusivement sur les accès au système, quels qu'ils soient.

Le mythe de l'air-gap

Pendant longtemps, la réponse des exploitants de systèmes de contrôle face à un risque supposé de cyber-attaques, a été principalement : « le système est protégé car il est isolé ». Cette réponse n'est pas suffisante : un système n'est jamais complètement isolé du monde extérieur de façon permanente même s'il l'est à certaines périodes, et en particulier en régime d'exploitation. Il existe toujours des moments où il devient nécessaire de procéder à des opérations de maintenance ou de mise à jour, par des moyens divers, notamment ceux qui relèvent des « conduits de compensation » : clés USB, CD-Rom, laptops, etc.

C'est un principe fondamental de l'ISA99 de ne jamais considérer un système comme isolé mais d'imposer l'identification de tous ses points d'entrée, permanents ou épisodiques.

L'approche ISA99

- Aperçu général

Le groupe de standardisation ISA99 mis en place par l'ISA (International Society of Automation) s'est donné comme objectif de développer un ensemble de rapports techniques, de bonnes pratiques et de standards dont le respect permet de conférer aux systèmes d'automatismes et de contrôle – y compris les systèmes répartis du type SCADA – un niveau acceptable de confiance face aux attaques cyber-sécuritaires.

Comme dans la démarche ISA84/CEI 61508, il s'agit de faire se rejoindre :

- une **évaluation des risques**, résultant d'une **analyse des menaces, des vulnérabilités** à ces menaces et de leurs conséquences potentielles ;
- une évaluation de la robustesse du système face à ces risques, que l'on va caractériser non pas par un scalaire (du type SIL) mais par un vecteur, le SAL (Security Assurance Level), afin de tenir compte du caractère multi-facettes des problèmes cyber-sécuritaires.

Cette analyse doit être réalisée au stade de la conception ; elle doit également se faire avant la mise en service et de façon périodique, pendant l'exploitation : la cyber-sécurité n'est jamais définitivement acquise, les menaces évoluent, les pratiques se relâchent et un système peut perdre de sa résilience au fil du temps.

La non-coïncidence entre les deux approches conduit à introduire des **contre-mesures** jusqu'à ce que la cohérence soit atteinte.

- Analyse des risques – Identification des menaces et des vulnérabilités

L'analyse des risques suppose tout d'abord une évaluation des menaces susceptibles de s'exercer sur le système à protéger.

Une menace est une violation potentielle de la sécurité liée à une circonstance, une action ou un événement. Les menaces doivent être identifiées et catégorisées. Elles peuvent être :

- internes (employé mécontent ou congédié) ou externes ;
- accidentelles (négligences : modifications non validées sur OS, programmes d'application non mis à jour, accès à des

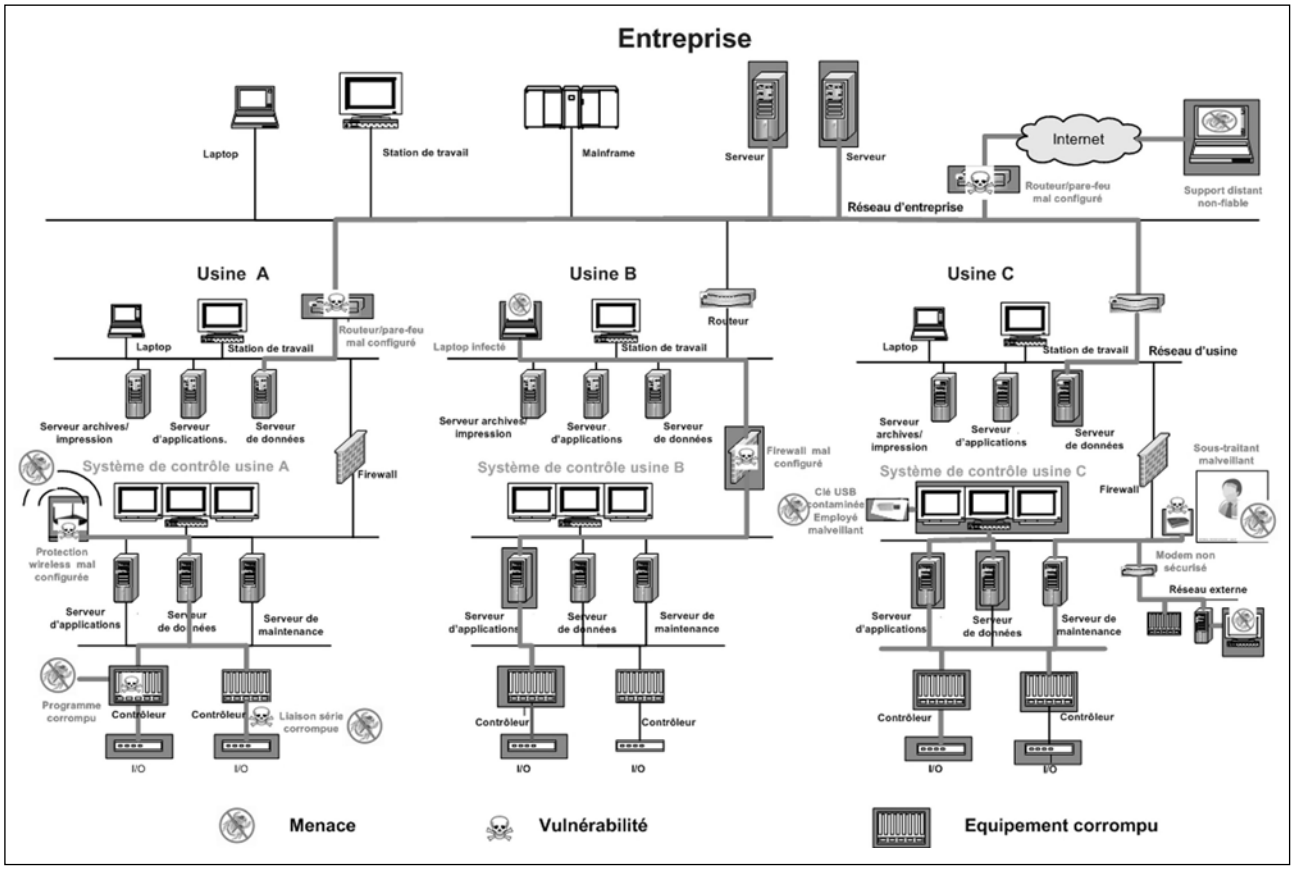

Figure 3 : Exemples de menaces et de vulnérabilités sur un système de contrôle.

sites contaminés, connexion de PC contaminés) ou volontaires (introduction de malwares, perturbation des communications, pénétration dans les bases de données, injection de données erronées, piratage d'information, hameçonnage, appâtage, « défacement » de site Web, déni de service, etc.) ;

- générales ou spécifiques au système.

L'identification des menaces doit prendre en compte un ensemble de circonstances plausibles. L'analyse du passé est importante aussi bien que les informations sur les menaces du moment.

A chaque menace est attaché un certain niveau de **vulnérabilité** (typiquement un antivirus absent ou non mis à jour). La vulnérabilité peut résulter de choix techniques intentionnels ou malencontreux. Il faut tenir compte également de l'effet de l'âge, de l'obsolescence des équipements.

Un système initialement non vulnérable peut le devenir dans un nouvel environnement, avec des conditions d'exploitation différentes, un nouveau personnel, etc.

L'identification de toutes les vulnérabilités est un point clé de l'analyse. Il faut en particulier :

- identifier tous les points d'intrusion potentiels à partir d'un schéma d'architecture détaillant les communications ;
- ne pas oublier les outils d'ingénierie, la chaîne de données, la téléassistance et « l'asset management » ;
- analyser les liaisons sans fil, les modems, les connexions par Internet, avec PC portables et tout matériel ou logiciel susceptible d'être connecté (clés USB, CD-Roms, smartphones) ;
- analyser la sous-traitance de développement logiciel et l'utilisation de logiciels non soumis à validation ;
- ne pas oublier les matériels et logiciels qui auraient pu être préalablement connectés à un système non protégé ;
- penser à la mise à jour irrégulière des logiciels de protection et des logiciels des machines exposées, OS et applications (par souci de disponibilité et crainte d'effets secondaires).

La figure 3 positionne à titre illustratif quelques menaces et vulnérabilités que l'on peut fréquemment rencontrer sur un système de contrôle.

Une menace, si elle se réalise, engendre un dommage plus ou moins grave. Le risque peut se caractériser par deux grandeurs :

- sa probabilité d'occurrence, qui résulte de la combinaison de la probabilité de réalisation de la menace avec celle que la menace soit effectivement exploitée :

$$Probabilité_{Occurence} = Probabilité_{Réalisation\ menace} \times Probabilité_{Exploitation\ vulnérabilité}$$

- sa criticité, qui caractérise la gravité des dommages éventuels.

Niveau de risque et SAL correspondant		Criticité des conséquences			
		Pas d'impact	Mineure	Majeure	Très sévère
Probabilité	Haute	Risque moyen SAL 2	Risque élevé SAL 3	Risque très élevé SAL 4	Risque très élevé SAL 4
	Moyenne	Risque moyen SAL 2	Risque élevé SAL 3	Risque très élevé SAL 4	Risque très élevé SAL 4
	Faible	Risque faible SAL 1	Risque moyen SAL 2	Risque moyen SAL 2	Risque élevé SAL 3
	Très faible	Risque faible SAL 1	Risque faible SAL 1	Risque moyen SAL 2	Risque élevé SAL 3

Tableau 1 : Exemple de matrice d'évaluation des risques.

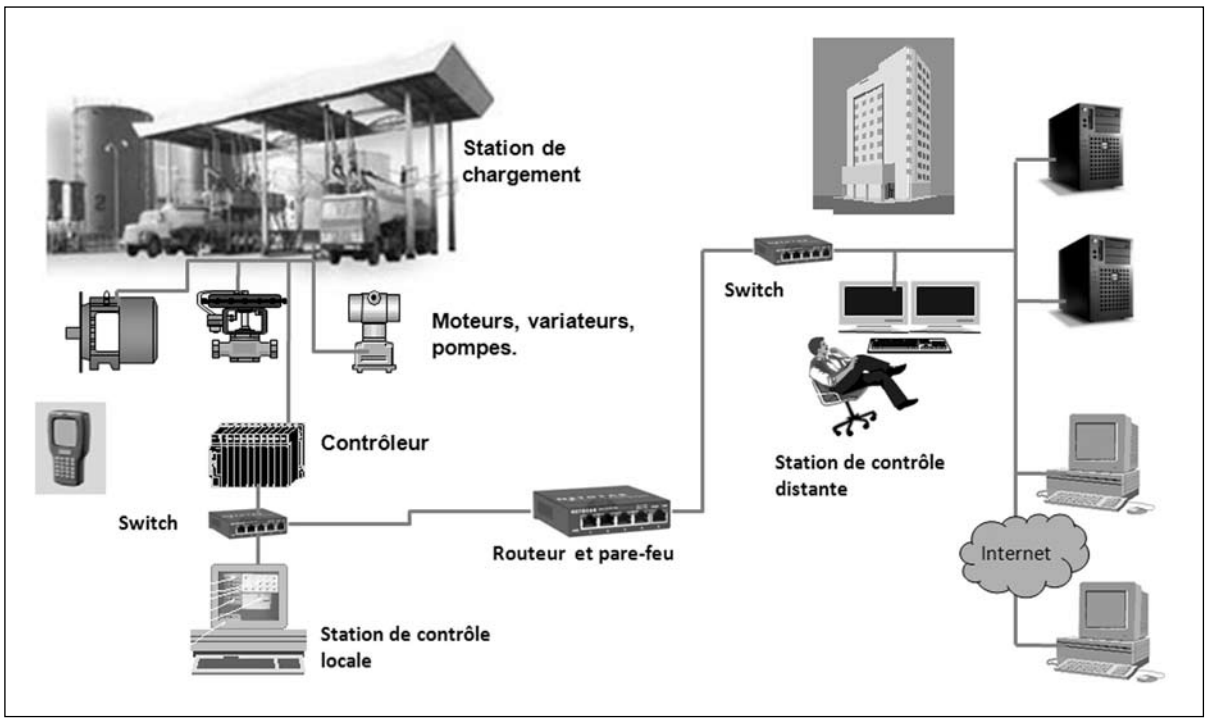

Figure 4 : Station de chargement de produits dangereux.

La norme impose que soient définies des échelles de valeur pour chacune de ces deux grandeurs, qui pourront être typiquement à trois ou à quatre niveaux. Si des échelles à quatre niveaux ont été retenues, elles pourront se combiner sous forme d'une matrice d'appréciation des risques du type de celle du tableau 1.

A chaque niveau de risque, sera attaché un niveau d'assurance sécurité à atteindre (voir plus loin), d'autant plus élevé que le risque aura été reconnu comme élevé.

- Défense en profondeur - Décomposition en zones et conduits

L'analyse des risques et l'évaluation de la robustesse face à ces risques ne se fait pas au niveau du système mais au niveau de **zones** et de **conduits**.

Une **zone de sécurité** est un regroupement logique, et en règle générale physique, de ressources ayant des exigences similaires en matière de sécurité. Une zone se définit à partir des modèles physique et fonctionnel de l'architecture de contrôle. C'est au niveau de la zone qu'une politique de sécurité doit être définie en fonction des menaces et des vulnérabilités recensées sur cette zone, et des conséquences qui peuvent en résulter.

Le découpage en zones procède de deux logiques complémentaires :

- d'une part celle de la **défense en profondeur** visant à circonscrire les conséquences d'un dommage et à opposer à une menace des remparts successifs ;
- d'autre part celle de la **défense des accès à la périphérie** de préférence à un durcissement de chacun des constituants, approche plus difficile et plus onéreuse.

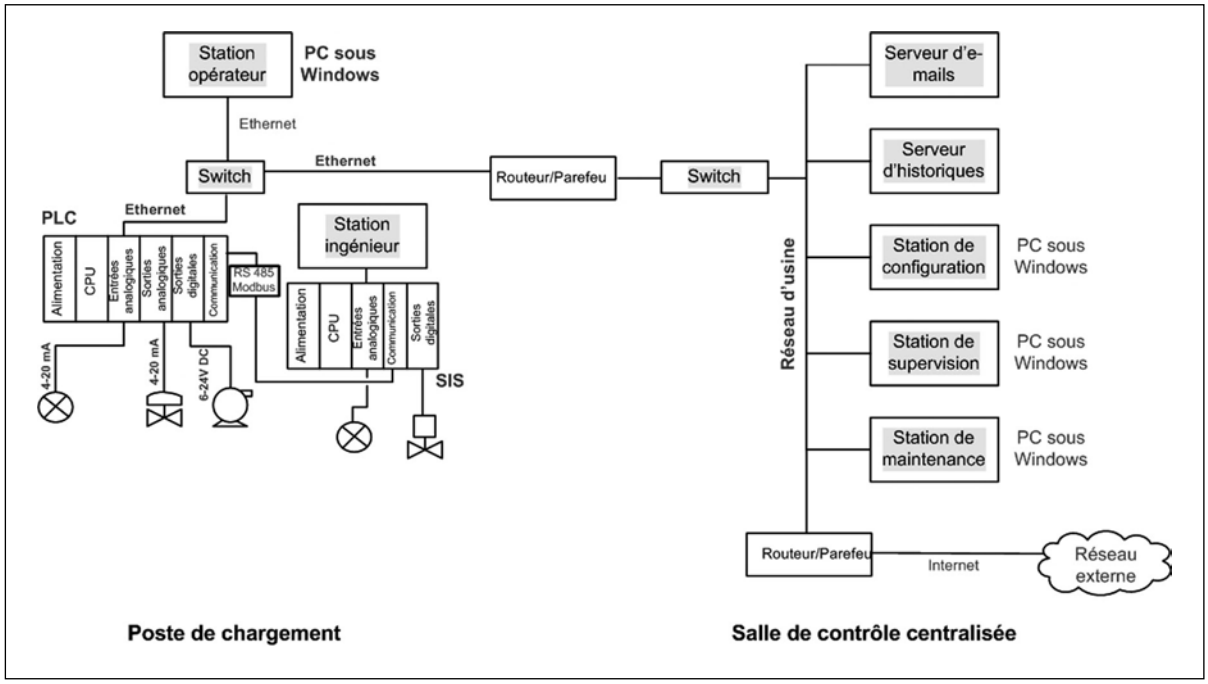

Figure 5 : Schéma fonctionnel de la station.

Les zones ne sont jamais isolées. Elles sont reliées, soit au monde extérieur, soit à une autre zone par un ou plusieurs **conduits** qui regroupent des canaux de communication, réels (réseaux et équipements associés) ou équivalents (conduits de compensation : connexions USB ou autres). Un conduit est une forme de zone particulière, qui ne peut pas être décomposée en sous-zones mais qui constitue une enveloppe de protection des canaux qu'il contient, à la manière d'un fourreau qui abrite des câbles. Selon le niveau de protection offert par ce conduit (protection externe du type **VPN** et/ou protection interne du type **pare-feu**), un conduit pourra rehausser le niveau de protection d'une zone aval ou au contraire le laisser s'abaisser en transférant sur cette zone le niveau d'assurance sécurité de la zone amont.

L'ISA99 définit des règles pour le découpage en zones et conduits, qui ne doit être ni trop complexe ni trop sommaire. Une attention particulière doit être portée aux SIS, aux systèmes sans fil et aux équipements mobiles ou nomades (laptops, PDAs, smartphones). Ces systèmes peuvent faire l'objet d'une zone spécifique. Une zone démilitarisée (DMZ) peut également être introduite lorsqu'il est nécessaire d'introduire une zone tampon par laquelle passeront toutes les communications vers une zone sensible telle que la zone de contrôle.

Les figures 4 à 6 décrivent ce processus de décomposition en zones et conduits pour un exemple simple mais représentatif : celui d'une installation de chargement de produits toxiques dotée d'un système instrumenté de sécurité. Elles montrent comment, d'un descriptif physique, on passe

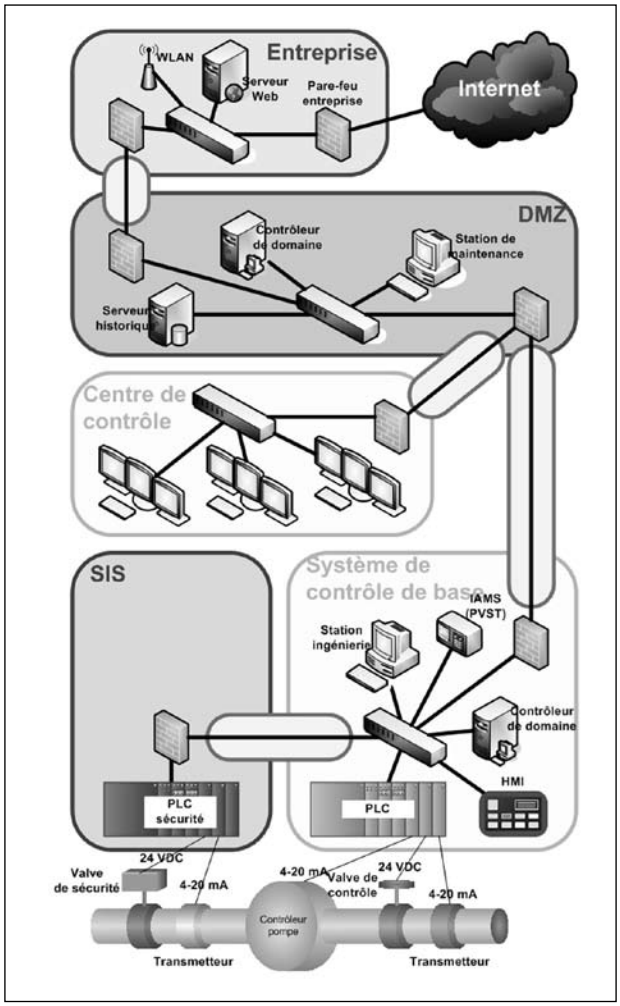

Figure 6 : Décomposition de la station en zones de sécurité - Source : ISA.

à un schéma fonctionnel et finalement, après une analyse de risques, à la définition des zones de sécurité à protéger.

- Exigences fondamentales et vecteurs SAL

L'analyse de risques et la décomposition du système en zones de sécurité, permet d'attribuer à chaque zone un objectif d'assurance sécurité (« target »). Cet objectif s'exprime sous forme d'un vecteur qui comporte sept composantes, chacune d'entre elles correspondant à l'une des exigences fondamentales de cybersécurité selon l'ISA99. Ces exigences sont les suivantes :

- FR1 – Identifier et authentifier les utilisateurs avant de leur donner accès au système ;
- FR2 – Contrôler que tous les utilisateurs identifiés (humains, process et équipements) disposent des privilèges les autorisant à opérer les actions qu'ils veulent mettre en œuvre sur le système ;
- FR3 – S'assurer de l'intégrité des informations (protection contre des modifications non autorisées) ;
- FR4 – S'assurer de la préservation de la confidentialité des informations ;
- FR5 – Segmenter le système pour éviter une propagation inutile des données ;
- FR6 – Réagir aux atteintes à la sécurité par un reporting rapide et une prise de décisions dans des délais appropriés ;
- FR7 – Assurer la disponibilité du système et des actifs, y compris en cas d'attaque en déni de service.

En fonction des risques, ces exigences devront être respectées à un niveau plus ou moins élevé allant, dans le projet de standard, de un à quatre (comme pour le SIL).

Un vecteur SAL (SAL « target ») aura donc typiquement la forme suivante, pour une zone donnée :

$$S^{target}_{Zone\ de\ contrôle} = \{4,3,4,2,3,2,3\}$$

Nota : Il est tout à fait possible qu'au niveau des objectifs toutes les composantes soient placées sur un plan d'égalité et que le vecteur se résume alors à un scalaire.

- Evaluation des systèmes

La cotation du système en termes d'objectif d'assurance sécurité doit être rapprochée de son évaluation en termes de réalisation (SAL « achieved ») résultant d'un audit du système. Le standard fixe, pour **chaque exigence fondamentale**, un ensemble de critères qui permettront, selon qu'ils sont respectés ou non, d'attribuer une note correspondant au niveau atteint. On aura par exemple, pour reprendre celui de la zone de contrôle, un SAL « achieved » du type suivant :

$$S^{achieved}_{Zone\ de\ contrôle} = \{3,3,4,2,3,3,3\}$$

La comparaison entre les niveaux « target » et les niveaux « achieved » permet d'identifier des insuffisances éventuelles et de les localiser. C'est là que devra porter en priorité l'effort de mise en œuvre de contre-mesures afin d'amener, en réalisation, toutes les composantes des vecteurs SAL aux niveaux définis en objectif.

Les contre-mesures

Le choix des contre-mesures à mettre en œuvre reste bien évidemment de la responsabilité du maître d'ouvrage ou de l'exploitant. Le standard ISA99 liste cependant, dans un rapport technique, les pistes à suivre pour parvenir à l'objectif visé.

- Réduire la surface d'attaque

Réduire la surface d'attaque, c'est prendre toutes les mesures nécessaires pour donner le moins de prise possible à une attaque :

- limiter le nombre de protocoles et de choix technologiques ;
- éviter les protocoles faibles (Telnet, SNMP V1 & V2, Modbus TCP, Http, SMTP, POP3, OPC Classic) qui peuvent être facilement identifiés et écoutés ;
- limiter au maximum les conduits vers l'extérieur y compris vers les niveaux de gestion de l'entreprise ;
- surveiller les « conduits de compensation » : clés USB, portables et tablettes, CD-Roms ;
- activer les sécurités partout où elles sont prévues ;
- bloquer toutes les communications non nécessaires vers les zones sensibles (SIS) ;
- surveiller très soigneusement les accès à distance.

- Organiser la défense en profondeur

La défense en profondeur commence par la segmentation de l'architecture en réseaux physiquement distincts desservant chacun une zone qui sera en outre elle-même convenablement protégée. C'est aussi, chaque fois que possible, organiser une segmentation virtuelle en n'autorisant, par des switchs ou des routeurs convenablement programmés, que les trafics nécessaires. C'est enfin créer, lorsque cela est utile, des DMZ entre les zones de contrôle et les salles de commande notamment, afin d'y loger les serveurs qui s'interfacent avec les niveaux supérieurs et inférieurs.

- Protéger les zones et programmer correctement les pare-feux

La protection des zones se fait prioritairement par l'installation de pare-feux industriels ayant les performances requises. La qualité de leur programmation est essentielle. Les pare-feux doivent filtrer tout le trafic non autorisé (par adresse et/ou par type). Ils doivent être dotés d'un mécanisme de

reporting chaque fois qu'un trafic anormal est constaté. Ils doivent être testés pour s'assurer que les trafics non autorisés sont bloqués. Ils peuvent être reconfigurables dynamiquement par des serveurs situés en amont ou en aval.

La fonction d'observateur de réseau est primordiale. Il est rare que les attaques sophistiquées aboutissent du premier coup. Des signes avant-coureurs, tentatives de connexion, trafic anormal, en interne comme en externe, peuvent être détectés à temps si les mécanismes d'observation ont été mis en place et sont régulièrement consultés.

- Durcir les composants et installer des antivirus

Les antivirus sont loin de constituer la protection absolue car ils ne fonctionnent que lorsqu'on dispose d'une signature des logiciels malveillants. Ils sont donc inefficaces en cas d'attaques utilisant des failles zéro-day (c'est-à-dire non préalablement identifiées ou publiées), ce qui était le cas de Stuxnet. Ils peuvent également être contournés par encodage des malwares. Ils sont utiles cependant et complètent les pare-feux. Ils relèvent à ce titre de la défense en profondeur. Leur mise à jour doit être aussi fréquente que possible, en tenant compte des contraintes de l'exploitation.

- Gérer les mots de passe

Les mots de passe offrent souvent une protection illusoire. La mise en place de principes de gestion rigoureux mais pragmatiques est nécessaire, en tenant compte des contraintes opérationnelles. Quelques règles simples doivent être observées :

- ne jamais les envoyer en clair sur un réseau ;
- les changer régulièrement ;
- les partager aussi peu que possible ;
- refuser les mots de passe de moins de huit caractères ;
- ne pas utiliser de mots existant dans des dictionnaires ou désignant des lieux géographiques ;
- utiliser des caractères complexes.

Veiller cependant très attentivement à la façon dont sont formulées les instructions. Des mots de passe successifs tels que Juliet@01, Juliet@02, Juliet@03... satisferont souvent aux instructions édictées sans pour autant apporter une sécurité suffisante.

- Sécuriser les accès distants

Les accès distants constituent de tels facteurs de progrès dans l'entreprise qu'il n'est pas envisageable de les interdire. Nous entrons dans un monde de réseaux, l'avenir est au « cloud computing » et aux services déportés. Il faut par contre s'assurer de leur utilité et prendre toutes les précautions que la technique rend aujourd'hui possibles.

Au niveau du réseau d'usine ou d'entreprise, les accès doivent se faire impérativement par mise en œuvre d'un Virtuel Private Network (VPN), en utilisant les technologies du type TLS (Transport Layer Security) ou mieux IPSec (Internet Protocol Security) qui assurent l'intégrité, la confidentialité, l'authentification et la protection contre le rejeu.

Au niveau du contrôle, on évitera les connexions filaires. Par contre, les connexions sans-fil, à la condition expresse que soient activés les modes de sécurité du type AES CCMP avec serveur d'authentification Radius, offrent de meilleures garanties, en combinant la protection physique résultant du saut de fréquence et/ou de l'étalement de spectre avec les techniques les plus avancées de chiffrement (clés asymétriques basées sur des courbes elliptiques).

- Former et sensibiliser les personnels

Enfin, il va sans dire que la protection par la technique reste insuffisante si elle n'est pas accompagnée d'un programme de sensibilisation et de formation du personnel. Ce dernier sera d'autant plus motivé pour y adhérer que les mesures prises ne relèveront pas de l'incantation mais s'appuieront sur une approche professionnelle telle que préconisée par l'ISA99.

En conclusion

Le nombre des vulnérabilités rapportées sur des systèmes de contrôle, soit par des organismes officiels (US-CERT), soit par des experts (Dillon Beresford, Eric Byres, Luigi Auriemma, Ruben Santamara, Joe Weiss), soit par des sociétés spécialisées (Scadahacker, Applied Control Solutions, Controlglobal, The H security), a tendance à croître. Tous les grands fournisseurs sont concernés, y compris les développeurs de logiciels.

L'attaque la plus redoutée est désormais du type « à la Stuxnet » avec :

- mise en évidence ou création d'une « porte dérobée » ;
- intrusion, introduction d'un payload, modification de programmes, modification ou vol de données.

Les responsabilités sont partagées entre fournisseurs et utilisateurs : lenteur des réactions et non divulgation des failles d'un côté, négligences de l'autre. Les enjeux sont sérieux et ils iront probablement en croissant. Il faut en prendre conscience et analyser les risques et la résilience des systèmes.

L'ensemble de standards ISA99 fournit un référentiel méthodologique abordant le problème dans sa globalité, à la différence d'autres cadres normatifs, qu'il faut cependant connaître (ISO 27000, NERC-CIP, NIST 800-82, draft CEI 62645 pour le nucléaire). Les constituants de l'ISA99 ne sont pas encore tous achevés ; cependant, les textes essentiels

sont d'ores et déjà repris par l'ANSI et la CEI sous la référence CEI 62443. Ils sont accessibles à partir du site www.isa.org. Chacun peut apporter sa contribution en participant au comité ISA99 et aux groupes de travail associés. Une organisation, l'**ISA Security Compliance Institute**, délivre un label de conformité : l'**ISA Secure**.

Les apports essentiels de l'ISA99 résident, d'une part, dans l'énoncé d'un cadre méthodologique permettant à chaque partie intéressée de construire une méthode d'élaboration d'un programme de cyber-sécurité adapté à ses besoins, d'autre part, dans la rationalité et la cohérence apportée à un domaine échappant aux probabilités objectives et souvent traité par l'incantation plus que par la raison.

Face à des menaces de plus en plus sophistiquées, la cyber-sécurité reste cependant un chantier toujours ouvert. Médecine des temps modernes, elle nécessite que des moyens suffisants lui soient alloués pour que les thérapies, curatives et surtout préventives, l'emportent sur les risques de contamination, et que l'automatisation des procédés et des grandes infrastructures puisse continuer à progresser.

L'AUTEUR

Jean-Pierre Hauet est ancien élève de l'Ecole Polytechnique et ingénieur du corps des mines. Il a occupé différentes positions dans l'Administration, en particulier celle de rapporteur général de la Commission de l'Energie du Plan. Il a dirigé le centre de recherches de Marcoussis d'Alcatel avant d'être nommé directeur produits et techniques de Cegelec, puis Chief Technology Officer d'Alstom. Depuis 2003, il est Associate Partner de KB Intelligence, spécialisé dans les questions d'énergie, d'automatismes industriels et de développement durable. Il préside l'ISA-France, section française de l'ISA (International Society of Automation). Il est membre Emérite de la SEE et membre du comité de rédaction de la REE.

Glossaire

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CCMP	Counter-Mode/CBC-Mac protocol
CEI	Commission Electrotechnique Internationale
CIP	Critical Infrastructure Protection
COTS	Commercial off-the-shelf
DMZ	DeMilitarized Zone
E/E/PE	Electrical/Electronic/Programmable Electronic
ERP	Entreprise Resource Planning
FBI	Federal Bureau of Investigation
FR	Functional Requirement
HTTP	HyperText Transfer Protocol
IACS	Industrial Automation and Control System
IPSec	Internet Protocol Security
ISA	International Society of Automation
ISO	International Organization for Standardization
MES	Manufacturing Execution System
ModBus	Modicon Bus
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OPC	OLE (Object Linking and Embedding) for Process Control
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
POP3	Post Office Protocol 3
RISI	Repository of Industrial Security Incidents
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
Telnet	TELecommunication NETwork ou TErminal NETwork
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual Private network