Mensuel
N° 834 - avril 2011
Prix : 18 €
ISSN 0755-219X

Le magazine de l'instrumentation et des automatismes industriels

mesures

www.mesures.com

CYBERSÉCURITÉ

« Nous avons parcouru pl vers la normalisation de

Virus Stuxnet, vols de quotas de CO2, piratage du ministère des Finances : en moins d'un an, plusieurs cyberattaques de grande envergure ont fait couler beaucoup d'encre. Face aux énormes moyens dont semblent disposer les pirates informatiques, les industriels peuvent se sentir désemparés, à juste titre. Heureusement, le comité ISA (International Society of Automation) travaille à l'élaboration du standard ISA-99, relatif à la cybersécurité des systèmes de contrôle-commande. La revue *Mesures* est allée à la rencontre de Jean-Pierre Hauet, président de l'ISA France, pour faire le point sur l'état d'avancement de ce standard et en comprendre les grands principes.

Mesures. Il y a quelques jours seulement, le ministère des Finances a été la cible d'une attaque visant des dossiers sensibles du G20. Les industriels ont-ils autant de raisons de s'inquiéter que ces organismes institutionnels ?

Jean-Pierre Hauet, ISA France. Tout à fait. Beaucoup d'industriels ont été choqués l'été dernier par la découverte de Stuxnet, un ver informatique qui visait des systèmes de contrôle-commande nucléaires pilotés par des automates de marque *Siemens*. Il est fini le temps où l'on pensait que les systèmes informatiques industriels n'intéressaient pas les cyberterroristes.

L'affaire du vol de "quotas CO_2" marqua également les esprits. Pour mémoire, un système de quotas CO_2 a été mis en place par la Communauté européenne pour lutter contre la production de gaz à effet de serre : chaque année, toutes les industries considérées comme polluantes doivent déclarer la quantité de CO_2 qu'elles ont rejeté dans l'atmosphère et elles doivent disposer d'un quota pour chaque tonne de CO_2 rejeté. Si les rejets dépassent la quantité allouée par le gouvernement en début d'année, l'entreprise doit racheter des quotas auprès d'autres entreprises qui ont réduit leurs émissions par rapport à ce qui était prévu. Or, en février, on apprenait que des millions de ces quotas avaient été dérobés. Aujourd'hui, la Communauté européenne s'interroge sur la fiabilité de ce système entièrement informatisé et géré indépendamment par chaque état. On réfléchit d'ailleurs à la mise en place d'une base de données unique gérée depuis Bruxelles. Alors bien sûr, on pourrait penser que cette affaire concerne uniquement les pouvoirs publics, pourtant ce sont bien les industriels qui en subissent les conséquences : nombre d'entreprises qui se sont retrouvées avec des quotas volés ont été obligées de les racheter, et pour eux la facture fut très salée…

> **"L'objectif de l'ISA est que le texte devienne une norme ANSI à l'horizon 2014."**

Mesures. Pourriez-vous nous expliquer comment a démarré le projet de standard ISA sur la cybersécurité ?

L'objectif premier était de combler un manque dans la norme CEI 61508 relative à la sûreté de fonctionnement des systèmes électriques, électroniques et électroniques programmables. Cette norme globale comporte une partie sur la résistance aux agressions extérieures (température, humidité, décharges électromagnétiques…) mais rien en ce qui concerne la résistance aux agressions informatiques. C'est donc tout naturellement que l'association ISA, jouant son rôle de prescripteur de standard, s'est intéressée au problème de la cybersécurité des systèmes de contrôle-commande. Elle a créé le groupe de travail ISA-99 en 2002, avec dans l'idée de transformer ce standard en une véritable norme industrielle. C'est la raison pour laquelle les textes sont transmis au fur et à mesure à l'ANSI (*American National Standards Institute*) qui est l'organisme américain qui rédige les normes propres au monde des automatismes, l'équivalent de l'AFNOR en France. Dans un second temps, le texte sera transmis à la Commission électrotechnique internationale (CEI), dans le but d'être intégrée à la future norme CEI 62443.

Mesures. A quelle échéance l'ISA-99 accédera-t-il au statut de véritable norme ?

L'objectif de l'ISA est que le texte devienne une norme ANSI à l'horizon 2014. La ratification par la CEI devrait demander, quant à elle, une année supplémentaire. Nous ne

us de la moitié du chemin l'ISA-99 »

Jean-Pierre Hauet est directeur de la société *KB Intelligence*, Président de l'ISA-France et responsable de l'ISA pour la zone Europe, Russie, Moyen-Orient et Afrique. Il joue donc un rôle clé au sein de l'*International Society of Automation* en relayant toutes les actions entre les Etats-Unis et le reste du monde, ce qui ne l'empêche pas de développer des actions spécifiques à la France.
Dans l'Hexagone, l'ISA compte une centaine de membres et bénéficie du statut d'association loi 1901.
Ses missions : participer au développement des standards, assurer des services de formation, organiser des sessions d'information par le biais de conférences et de publications, mais aussi maintenir et faciliter l'accès à la masse documentaire de l'ISA. En effet, plus de 150 standards ont déjà été développés. Ils touchent des activités aussi variées que la modélisation des échanges au sein de l'entreprise (ISA-95) ou les communications sans-fil (ISA-100).
Dans le cas de la cybersécurité (ISA-99), Jean-Pierre Hauet reconnaît qu'il est agréable de travailler sur un sujet aussi transversal : *« Il n'y a pas de phénomène de concurrence entre industriels, ou entre Etats, comme cela peut être le cas notamment lors des débats sur les technologies sans-fil, et du coup les travaux avancent relativement efficacement. »*

nous faisons pas de souci pour l'adoption du texte en tant que norme ANSI, étant donné que l'ANSI a complètement délégué à l'ISA la responsabilité de l'élaboration de ce texte. Le passage devant la CEI sera différent car nous ne serons pas seuls, la CEI ayant constitué son propre groupe d'experts en cybersécurité. Quoi qu'il en soit, nous faisons notre possible pour faciliter l'adoption de notre texte : il y a deux ans, nous avons entièrement revu la nomenclature du standard afin d'être en harmonie avec les attentes de la CEI. Le moment venu, cela devrait faciliter l'intégration de notre texte au sein de la future norme CEI.

Mesures. De quoi se composent concrètement les textes sur lesquels travaille le comité ISA-99 ?

On part des considérations générales pour aller vers le particulier. Trois des textes qui composent l'ISA-99 sont déjà ratifiés par l'ANSI. Le premier, l'ISA-99.01.01, définit la terminologie, les concepts et les modèles qui permettent d'assurer la sécurité des systèmes automatisés. Sont explicitées, entre autres, les notions de contrôle d'accès, d'intégrité des données, de contrôle de l'usage des équipements, ou encore de disponibilité des ressources. Le second texte, l'ISA-99.02.01, donne des indications sur les procédures à suivre. Ratifié par l'ANSI en 2009, il propose des méthodes pour évaluer les risques d'attaque sur une installation donnée. Il présente aussi des procédures à mettre en place en matière de politique d'entreprise. Enfin, le troisième texte, l'ISA-TR99.03.01, constitue en quelque sorte un "tutorial" pour découvrir les technologies déjà disponibles en matière de cybersécurité.

Mesures. Quel est le point de départ de la méthode préconisée par l'ISA-99 ?

Un aspect primordial de l'ISA-99 est de fournir aux industriels un état précis du niveau de sécurité de leur installation, que ce soit pour évaluer une installation existante ou pour réaliser un nouveau projet. C'est la raison pour laquelle le standard introduit le concept de vecteur SAL (*Security Assurance Level*) tel que défini dans le document ISA-99.03.03. Comme leur nom l'indique, les vecteurs SAL s'inspirent des niveaux SIL (*Safety Integrity Level*) définis par la norme CEI 61508. Sauf qu'au lieu de caractériser la sécurité fonctionnelle d'une installation, on s'intéresse à la résistance aux attaques informatiques. Cela fait une grande différence. En effet, dans le domaine de la sécurité fonctionnelle, on combine les probabilités de défaillance de chaque composant et on →

l'industriel de se fixer des objectifs, quel que soit l'état d'avancement de son projet. Le comité ISA a donc décidé de créer plusieurs types de vecteurs SAL. On trouve les vecteurs SAL de type T (pour *Target*, ou cible), de type D (pour *Design*, ou conception), de type A (pour *Achieved*, ou réalisé) et de type C (pour *Capability*, ou aptitude). Cela permet aux industriels, aux fournisseurs de composants et aux chargés d'audits de se comprendre, sinon chacun parlerait de vecteurs SAL différents. Ainsi, un vecteur SAL-T sera utile dans les cahiers des charges des installations, lorsque le donneur d'ordres souhaite que son système de contrôle-commande bénéficie d'un degré de sécurité donné. Le vecteur SAL-D servira à vérifier les choix de conception, par exemple, si un concepteur demande à un expert de valider que les plans sont bien cohérents avec les objectifs. Le vecteur SAL-A sera, quant à lui, pris en compte pendant les phases d'audit : le vecteur SAL-A annoncé par l'auditeur devant au minimum égaler le vecteur cible SAL-T. Pour finir, le vecteur SAL-C est réservé à l'étude des composants d'un système. En cybersécurité comme ailleurs, on considère que la vulnérabilité totale est au plus égale à la vulnérabilité du composant le plus faible. Aussi, évaluer le vecteur SAL d'un composant rendra possible l'identification des points faibles d'une installation.

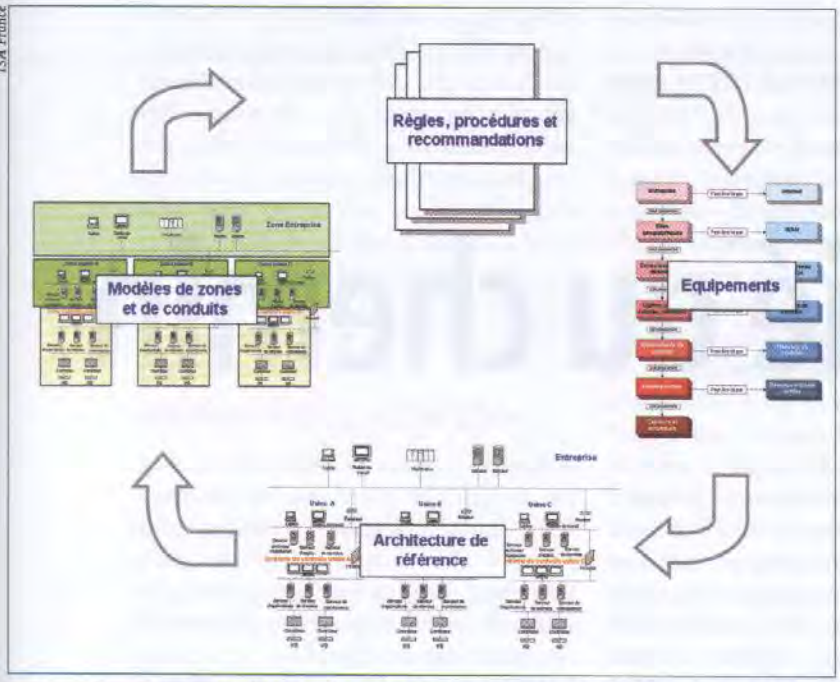
Mesures. Ce principe d'évaluation des SAL n'est-il pas un peu complexe ?

Dans la pratique, évaluer un vecteur SAL n'est pas plus compliqué que de déterminer des niveaux de sécurité SIL, d'autant que ces derniers demandent des compétences avancées en mathématiques probabilistes. Il faut dire aussi que, dans l'immense majorité des cas, l'industriel confiera ces travaux à un expert… Bien sûr, le fait de travailler avec plusieurs vecteurs SAL simultanément peut être source de confusion. Mais, contrairement aux systèmes de sécurité concernés par les niveaux SIL qui ne subissent que peu d'évolutions, les systèmes de protection informatique ont besoin d'être régulièrement réévalués. Que l'on soit en phase de conception ou en phase de réalisation, on pourra mesurer à tout moment la robustesse de son design ou de son installation en la comparant avec le vecteur SAL-T ou vecteur cible.

Mesures. Concrètement, comment peut-on atteindre le niveau de sécurité que l'on s'est fixé ?

Sur ce point, les travaux de l'ISA sont encore en cours. Mais les industriels peuvent commencer à avancer, car l'ensemble documentaire de l'ISA-99 est déjà très riche. On trouve déjà des pistes et des recommandations solides pour améliorer le degré de confiance dans un système. Un exemple concret parmi d'autres : on ne pourra pas décoller du niveau de sécurité le plus bas tant que l'on n'aura pas désactivé tous les ports USB des PC utilisés dans les systèmes de contrôle. Plus important encore : l'ISA-99 prévoit un découpage des systèmes informatiques sous forme de zones et de conduits afin de limiter une éventuelle contamination.

Dans son état actuel, le standard donne des indications générales pour assurer un niveau de sécurité qui soit le plus élevé possible, mais il ne fournit pas de règles précises pour atteindre telle ou telle caractéristique dans ➜



Tout comme la qualité, la cybersécurité est une démarche qui doit se mettre en place par itérations successives. L'ISA-99 introduit la notion de vecteur SAL "cible" qui favorise la mise en place d'une politique d'amélioration continue.

→ obtient la probabilité de celle du système complet. Ce raisonnement est valable uniquement car chaque défaillance technique peut être exprimée sous forme de probabilité, mais ce n'est pas le cas des cyberattaques. Ces dernières peuvent être de nature très diverses et il est très difficile de quantifier les risques avec précision.

Pour en revenir aux vecteurs SAL, le standard ISA-99 définit sept exigences fonctionnelles (FR, pour *Functional Requirements*) qui portent sur sept aspects d'un système de contrôle. Elles sont numérotées de FR1 à FR7. On trouve d'abord les exigences concernant le contrôle d'accès, puis celles relatives au contrôle d'usage, à l'intégrité des données, à la confidentialité des données, à la limitation de la circulation des données, au temps de réponse suite à un incident, et enfin au taux de disponibilité des ressources. Le standard prévoit de qualifier un système (ou un composant du système) en lui associant une note de 0 à 3 en réponse à chacune des sept exigences. On obtient une suite de notes du type : SAL (système) = { 3 3 2 3 0 0 1 }. On comprend pourquoi on parle de "vecteur" SAL et non pas simplement de "niveau" SAL. Ce concept permet de porter davantage d'informations qu'un simple scalaire (comme c'est le cas avec les niveaux SIL 1, 2, 3 ou 4) et donne donc une image plus fine du degré de protection face à un ensemble varié de menaces.

Mesures. Comment fait-on pour noter chacune de ces sept exigences ?

On utilise un tableau qui est inclus dans le texte de la norme. Pour chaque exigence, le niveau de sécurité est calculé en combinant les risques d'attaque à la vulnérabilité du système. Ensuite, on pondère ce résultat avec les conséquences de cette vulnérabilité.

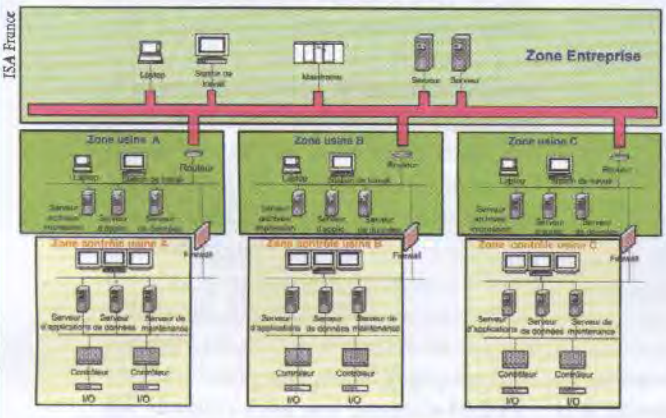
Mais avant d'aller plus loin, il faut expliquer la différence entre risque et vulnérabilité. Cette différence peut s'illustrer en prenant l'exemple d'une épidémie de grippe. L'analogie est d'autant plus frappante que l'on parle également de "virus". Dans un pays donné, il y a toujours une certaine probabilité pour qu'une épidémie de grippe se déclare, et cette probabilité varie en fonction du mois de l'année et de la région dans laquelle on se trouve. Toutefois, ce n'est pas parce qu'une épidémie de grippe est déclarée qu'un individu X va forcément attraper le virus, car chaque personne est plus ou moins vulnérable. Il en va de même en cybersécurité. Face à un risque de contamination, l'industriel doit commencer par évaluer ce risque. Un exemple : on considère que le risque de *phishing* (ou hameçonnage) est élevé, car c'est à l'heure actuelle l'attaque la plus répandue dans l'industrie comme dans le grand public. La vulnérabilité traduit, quant à elle, la probabilité que le risque se matérialise en une attaque effective (et dans le cas du *phishing*, il suffit d'apprendre à le repérer pour être moins vulnérable).

C'est seulement une fois que l'on a combiné ces deux probabilités (risque et vulnérabilité) que l'on peut prendre en compte les conséquences de l'attaque. Pour cela, l'ISA-99 prévoit quatre niveaux de criticité : 1 pour "impact sévère", 2 pour "impact majeur", 3 pour "impact mineur" et 4 pour "pas d'impact". La norme fournit quelques exemples de ce que peut être un impact sévère, un impact majeur, etc., mais c'est surtout à titre d'exemple car c'est à l'industriel de se forger son propre système d'évaluation des risques, selon ce qu'il estime acceptable et non acceptable. En effet, une perte de plusieurs milliers d'euros pourra être plus ou moins catastrophique selon qu'il s'agit d'une PME ou d'un grand groupe.

Mesures. Que faire une fois que l'on a calculé le vecteur SAL d'un système ?

Le but d'un vecteur SAL est de permettre à

Des zones et des conduits...



Le texte ISA-99.03.03 fournit des pistes et des règles à suivre pour construire des systèmes informatiques sécurisés. L'une des règles primordiales est la notion de "défense en profondeur". Il faut définir des zones de sécurité pour limiter l'impact d'une défaillance. Au minimum, un site devra comporter des zones différentes pour le contrôle et pour la supervision. Mais attention à ne pas reproduire l'erreur du Titanic : il ne suffit pas de cloisonner, il faut aussi éviter que les compartiments puissent communiquer. C'est pourquoi l'ISA-99 introduit le principe des conduits pour relier les zones entre elles. Un conduit, c'est une enveloppe de réseau de communication à laquelle on doit appliquer des protections particulières (des pare-feu, notamment).

Zones et conduits doivent regrouper des composants homogènes d'un point de vue géographique et d'un point de vue fonctionnel. Les zones doivent être hiérarchisées et on doit leur appliquer le cas échéant un principe d'"héritage" : une zone située à l'intérieur d'une autre zone doit au minimum hériter des mêmes propriétés que celle qui l'englobe.

Déterminer le niveau SAL d'un système automatisé

Le standard ISA-99 propose une méthode pour définir le niveau de sécurité d'une installation, d'une zone ou d'un conduit. Il s'agit de déterminer le vecteur SAL (pour *Security Assurance Level*) d'un système informatique. Pour connaître ce "vecteur" SAL, il faut évaluer la réponse du système face à sept exigences. Ces exigences sont les suivantes :

- Contrôle de l'accès aux équipements et à l'information ;
- Contrôle de l'usage des équipements et de l'information ;
- Intégrité des données (on cherche à savoir s'il existe des protections contre les modifications non autorisées) ;
- Confidentialité des données ;
- Contrôle des flux de données pour éviter une diffusion non souhaitée ;
- Temps de réponse aux événements (cela inclut la réactivité face à une violation d'accès) ;
- Disponibilité des ressources (cela inclut les méthodes mises en place pour lutter contre les attaques de déni de service).

A chacune de ces exigences est associé un niveau de sécurité. Ce dernier s'obtient en calculant la probabilité d'occurrence du risque (estimée en considérant la probabilité d'attaque et la vulnérabilité du système) puis en la combinant à la criticité des conséquences liées à ce risque. Il en résulte une note de 1 à 4, dont voici la signification :
1 Les fonctions ne sont pas critiques pour la mission et ne sont pas susceptibles de faire l'objet d'attaques ;
2 Les fonctions ne sont pas critiques pour la mission mais peuvent faire l'objet d'attaques ;
3 Les fonctions sont critiques pour la mission et peuvent faire l'objet d'attaques. Elles ne nécessitent pas de réponse immédiate mais leur défaillance peut conduire à des impacts importants en termes de performance et de résultat financier du fait de la perte totale des capacités opérationnelles du système ;
4 Les fonctions sont critiques pour la mission et peuvent faire l'objet d'attaques. Elles exigent une réponse immédiate pour assurer la sécurité publique et environnementale du fait du risque de perte des capacités opérationnelles du système ou même de pertes humaines.

Enfin, on notera qu'il existe quatre types de vecteurs SAL différents selon que l'on considère le niveau de sécurité à obtenir (SAL-C pour *Target*), le niveau de sécurité d'une installation à l'état de projet (SAL-D pour *Design*), le niveau de sécurité d'une installation déjà en fonction (SAL-A pour *"Achieved"*) ou encore le niveau de sécurité d'un composant (SAL-C pour *Capability*).

le vecteur SAL. On espère que cela sera bientôt le cas. En attendant, les industriels et les experts en cybersécurité peuvent utiliser les quelques outils déjà disponibles sur le marché. On peut citer le *Cyber Security Evaluation Tool* (CSET) proposé par les autorités américaines, ou encore l'outil CS2SAT (*Control System Cybersecurity Self Assessment Tool*), développé par *Idaho National Lab*. Ce dernier se conforme à des standards comme le SP800-53 du *National Institute of Standards and Technology* (NIST) ou le standard CIP du *North American Electric Reliability Corporation* (NERC). Même s'ils ne sont pas encore harmonisés vis-à-vis de l'ISA-99, qui est plus complet que le SP800-53 ou le CIP, ces outils permettent d'avoir une bonne idée du niveau de sécurité d'une installation. Et nous avons bon espoir que la plupart des outils se conforment au standard de l'ISA une fois que celui-ci sera entièrement passé à l'état de norme.

Mesures. Les outils vont donc s'adapter progressivement au standard. Mais ce décalage entre cadre normatif et réalité du terrain ne pose-t-il pas problème dans le domaine de la cybersécurité, où les pirates sont toujours en avance par rapport aux technologies de protection informatique ?
Je reconnais qu'il est assez difficile de se protéger contre des attaques dont on ne connaît pas encore la nature. Il ne faut pas baisser les bras pour autant, surtout qu'il suffit d'appliquer des règles de base du standard ISA-99 pour limiter la propagation de la plupart des virus, qu'ils soient connus ou inconnus. L'exemple de Stuxnet illustre bien ce principe. Certes, il aurait été impossible de se protéger totalement contre l'invasion de ce virus, étant donné sa complexité et le fait qu'il utilise simultanément plusieurs failles de sécurité de Windows encore inconnues jusqu'alors (on les appelle failles *Zero-Day*). En revanche, on ne peut pas dire qu'on ne pouvait rien faire pour l'empêcher de se répandre à l'intérieur des usines. Pour cela, les règles de base de l'ISA-99 auraient suffi. Les textes renferment de nombreuses recommandations sur les moyens de verrouiller des accès. Certaines pourront peut-être sembler triviales, toutefois nous nous rendons compte que dans une grande partie des usines, ce n'est pas fait. L'ISA-99 insiste notamment sur le fait de remplacer le mot de passe par défaut de chaque logiciel par un mot de passe personnalisé, et sur le fait de changer ces mots de passe régulièrement. C'est indispensable pour certains systèmes comme la supervision, car les pirates peuvent se servir de ces applications comme autant de points d'entrée pour pénétrer à l'intérieur du système.
Pour résumer, le standard ISA-99 préconise une "défense en profondeur". Partant du principe qu'on ne peut pas empêcher les attaques, il faut éviter à tout prix leur propagation à l'intérieur de l'entreprise. Ce principe est assez ancien, puisqu'il remonte à la gestion des réseaux de puissance : il faut que les réseaux soient correctement isolés de manière à limiter l'impact d'une panne de courant. On peut parfois se permettre de perdre une zone, mais il faut à tout prix éviter que tout le réseau ne s'effondre.
A ce propos, nous nous inquiétons des attaques qui pourront toucher les "smart grids", ces systèmes automatisés qui associent réseau électrique et réseau informatique. Lorsque des millions d'usagers seront reliés ensemble par un seul et même système, les conséquences d'une attaque pourraient être catastrophiques. Si aux Etats-Unis la sécurité des "smart grids" fait l'objet de nombreux débats, en France les gestionnaires de ces réseaux restent encore très réservés sur le sujet.

Mesures. Vous disiez qu'il faudra attendre 2014 pour que l'ISA-99 devienne une norme, et pour que les outils logiciels soient harmonisés avec la norme. Quel conseil donnez-vous aux industriels qui veulent mettre en place dès maintenant une politique de cybersécurité ?
Il est vrai qu'il faudra attendre quelques années avant qu'un écosystème de solutions conformes à l'ISA-99 ne soit disponible. Les aspects méthodologiques de l'ISA-99 sont déjà figés, et il ne reste plus aux groupes de travail qu'à se mettre d'accord sur les aspects métriques du standard. C'est seulement une fois que ces métriques seront clairement définis que l'on pourra voir émerger les premiers outils et les premiers réseaux d'experts qui proposeront leurs services aux industriels. Car il faut être réaliste : les documents de l'ISA-99 s'adressent avant tout à des spécialistes. On voit mal le dirigeant d'une PME se plonger dans les 900 pages du standard. Pour l'instant nous cherchons avant tout à sensibiliser le plus grand nombre, c'est pourquoi nous évoquons des méthodes de protection compréhensibles par tout le monde. Mais lorsque des experts en cybersécurité étudieront une installation, ils iront beaucoup plus loin dans les aspects techniques.

Mesures. A quand selon vous la création d'un réseau d'experts ISA-99 ?

Des méthodes de protection concrètes

Phoenix Contact

Les premiers textes de l'ISA-99, déjà publiés par l'ANSI, introduisent les aspects méthodologiques du standard. Bien qu'ils soient toujours à l'état de projets, les autres textes décrivent avec davantage de précision les outils à mettre en place.
Outre les recommandations à apporter aux PC sous Windows (ports USB et lecteurs de disques à désactiver, par exemple), le standard va jusqu'à donner des préconisations pour le paramétrage des pare-feu, et met l'accent sur quelques technologies innovantes. Parmi les règles à retenir pour sécuriser les communications dans une zone donnée, on peut citer le *whitelisting*. Par opposition au *blacklisting*, qui consiste à écarter volontairement tout programme identifié comme dangereux (c'est le mode de fonctionnement des logiciels antivirus), on cherche ici à ne laisser passer que le code autorisé au préalable. Seuls les exécutables validés et disposant d'une signature numérique fiable pourront être exécutés. Intéressante pour les systèmes qui évoluent peu, cette technologie revient à mettre tout ou partie du système sous cloche, afin qu'aucune nouvelle instruction ne vienne perturber son fonctionnement. Le *whitelisting* est intégré à certains pare-feu de *Core Trace*, *Industrial Defender* ou encore *Phoenix Contact* qui a acquis en 2008 la société *Innominate*.
Autre technologie intéressante : la "data diode". A la manière d'une diode électronique qui ne laisse passer le courant que dans un sens, une diode réseau ne laissera passer les données que dans un seul sens. Certains produits industriels, comme les routeurs et les passerelles de *Waterfall Security Solutions*, de *Fox DataDiode* ou encore de *Owl Computing Technologies*, sont spécialement conçus pour garantir le caractère unidirectionnel des communications. On les utilisera principalement pour éviter que des pirates ne puissent piocher des informations dans un réseau d'entreprise.

En France, Jean-François Pacault, haut fonctionnaire de défense et de sécurité au Minefe (ministère de l'Economie, des Finances et de l'Emploi) et moi-même aimerions que cela se fasse le plus tôt possible. Avec un réseau d'experts accrédités ISA France, les industriels auraient l'assurance d'une certaine qualité de service, d'un certain respect de la norme. Seulement il n'y a pas encore de véritable marché, les industriels n'étant pas prêts à payer des sociétés d'audit pour étudier leurs systèmes automatisés. A mon avis, les Etats-Unis, qui sont en avance par rapport à nous sur ces questions de cybersécurité, devraient voir apparaître ce type de services d'ici peu. Bien sûr, les choses peuvent s'accélérer s'il y a d'autres attaques de grande envergure dans les mois à venir. Mais en tout cas nous considérons que nous avons parcouru plus de la moitié du chemin vers la normalisation de l'ISA-99…

Mesures. Quelle serait pour vous la meilleure preuve que le standard a réussi à s'imposer ?
Dans l'absolu, nous aimerions que l'ISA-99 connaisse le même succès que le modèle CMMI dans le domaine de la qualité logicielle. Il existe d'ailleurs des analogies dans les démarches de cybersécurité et de qualité logicielle, car dans les deux cas certains aspects ne peuvent pas être quantifiés, ou évalués de manière totalement objective (les questions n'attendent ni un oui ni un non, mais plutôt une appréciation). Même les sociétés qui ont atteint le plus haut niveau CMMI doivent se remettre en cause en permanence, et c'est ce vers quoi nous voulons aller avec l'ISA-99. Nous évoquions tout à l'heure le fait que l'on mesure le vecteur SAL d'une installation par rapport à un vecteur cible. Une fois que le niveau de sécurité cible est atteint, nous souhaitons que l'industriel recommence son analyse avec des objectifs plus ambitieux. A terme, l'analyse d'un système automatisé devra donc être faite de manière itérative, pour devenir une démarche d'amélioration continue de la cybersécurité.

Propos recueillis par Frédéric Parisot