ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°50 – Septembre 2013 **Bulletin d'information d'ISA-France**

Au sommaire de ce numéro :

Sur vos calendriers

Nancy– 17 octobre 2013 – Surveillance des procédés industriels Algorithmes de traitement et aides à la décision

Les exigences de sécurité, de disponibilité et d'optimisation des unités de production nécessitent de recourir à des systèmes numériques de contrôle-commande performants. Le risque existe cependant que l'opérateur n'ait pas une compréhension suffisante de l'information en provenance de ces outils. Il est essentiel que l'opérateur ne décroche pas par rapport à des techniques trop sophistiquées et garde en permanence la maitrise du procédé. Centré sur deux grands thèmes :

- **algorithmes de traitement de l'information – Diagnostics – Aides à la décision**
- **interfaces homme-machine**

le séminaire Nancy 2013 d'ISA-France, organisé avec le Centre de recherche en Automatique de Nancy – Université de Lorraine, fait suite aux séminaires de Lille, Marseille et Grenoble.

Renseignements sur contact@isa-france.org - Télécharger le programme.

Nashville (USA – TN) – 5-7 novembre 2013 – ISA Automation Week

La grande manifestation annuelle de l'ISA, l'**ISA Automation Week**, se tiendra à Nashville (Tennessee) – Convention Center - du **5 au 7 novembre** 2013. Elle sera ouverte par une conférence sur **« The cyber-threat to the Automation industry »** donnée par le Major Général Robert E. Wheeler.

Consulter le programme complet de cet événement sur www.isaautomationweek.org .

Au préalable, se tiendra du **1er au 5 novembre**, le **Leaders Fall Meeting** et le Council **of Society Delegates**, assemblée générale de l'association, ouverte à tous ses membres.

Dammam – 7 au 11 décembre 2013 – 2nd ISA EMEA Automation Conference

Faisant suite à la manifestation de Doha (Qatar) qui avait connu un vif succès en décembre 2012, la 2eme ISA EMEA Automation Conference, organisée sous l'égide du District 12, se tiendra du 7 au 11 décembre 2013 à Dammam (Arabie Saoudite) - Dammam Hotel & Towers.

Organisée sur le thème « Experience pour le futur », le programme de grande manifestation comprend un ensemble de conférences, une exposition et des séances de formation.

Pour plus d''informations, consulter www.isa-emea-expo.org

Retour sur : le Forum ISA-France des 26 et 27 juin 2013 "Cyber-attaques : comment faire face"

Le 6ème Forum ISA-France sur la cyber-sécurité des installations industrielles organisé à Paris les 26 et 27 juin 2013 a connu un très grand succès.

Le CD-Rom rassemblant l'ensemble des conférences est à présent disponible.

Commander le CD-Rom

Sommaire | Evénements | Standards | Technologie | Formation

Cyber-sécurité : le standard ISA-62443-3-3 devient norme ANSI

La série de standards **ISA-62443** (anciennement **ISA-99**), dont le développement est en cours d'achèvement au sein de l'ISA et qui a été repris mondialement par la CEI sous la référence **IEC 62433**, est conçue pour fournir à l'intention des développeurs, des fournisseurs, des intégrateurs et des exploitants de systèmes de contrôle un ensemble de règles et de méthodes leur permettant de prémunir les installations contre le risque d'attaques cyber-sécuritaires et d'en limiter les conséquences éventuelles.

Le dernier standard publié, **l'ISA-62443-3-3-2013** : *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels* a été approuvé le 13 août 2013 en tant que norme ANSI sous la référence ANSI/ISA-62443-3-3-2013. Il est en cours d'approbation par la CEI.

Ce standard est un élément essentiel du dispositif normatif relatif à la cyber-sécurité. Il fixe les **règles techniques** à observer pour permettre de sécuriser un système de contrôle, en *capability* pour un système générique et en *achievement* pour un système installé, et lui permettre ainsi d'atteindre un niveau de sécurité, caractérisé par le vecteur SL (Security Level), homogène avec celui que l'on veut atteindre au regard des risques encourus (SL-T). Le standard propose une liste d'une centaine de critères qui, selon que le système est conforme ou non à ces exigences, permettent de lui allouer un SL allant de 1 à 4 (par défaut 0), pour chacun des Fundational Requirements (FR) définis par la norme IEC 62443.

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓

Figure 1 : Extrait de la grille d'évaluation de l'ISA/IEC 62443-3-3.

L'IEC 62443-3-3 est le seul texte qui propose aujourd'hui une approche concrète, fondée sur des mesures techniques pratiques, pour sécuriser les systèmes de contrôle et évaluer le niveau de confiance qu'on peut leur accorder.

Il vient compléter l'**IEC 62443-2-1** qui définit les *Policies and Procedures* dont le respect est requis pour assurer, d'un point de vue organisationnel, la cyber-sécurité des systèmes, au niveau entreprise, site ou atelier. Ce dernier texte, dont la nouvelle version est en cours de finalisation, s'appuie sur les normes ISO 27000-1 et -2. Il est complété, pour les composants, par la l'**IEC-62443-4-2** dont le projet est en cours de circulation.

Jean-Pierre Hauet – jean-pierre.hauet@kbintelligence.com

Du côté du nucléaire… le lien avec les travaux ISA

Le projet de norme IEC 62645 (cyber-sécurité contrôle-commande réacteurs - centrales nucléaires) est passé cette année en CDV (Committee Draft fo Voting) au sein de l'IEC

Ce projet IEC 62645 reprend les principes de AIEA NSS #17 - *Computer Security at Nuclear Facilities* (téléchargeable sur http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf). Il définit une politique de défense graduée : les systèmes sont classés en différents degrés de sécurité et sont ensuite affectés à des zones physiques et logiques suivant ce degré, avec des règles de flux très spécifiques. Par exemple, une connexion réseau (ou liaison série) entre degrés est toujours à l'initiative de celui le plus critique ; des data-diodes (flux unidirectionnel d'information) sont recommandées vers le degré le plus critique. La notion de "zone" de l'AIEA est compatible avec celle définie par l'ISA et l'IEC dans l'ISA/IEC 62443.
A noter que l'IEC, comme d'autres acteurs, remplace le terme de « niveau » de l'AIEA par le terme degré, pour éviter la confusion avec les niveaux CIM au sens ISA (3 : supervision, 2 : contrôle…). On parle ainsi de « degrés de sécurité ».

L'AIEA NSS #17 préconise des règles générales de management de la sécurité et des mesures de sécurité par niveau ; d'autant plus strictes que le niveau de sécurité visé est élevé (figure 2). Le projet IEC 62645 comporte également des prescriptions concernant les IACS-SMS (systèmes de management de la cyber-sécurité dans les systèmes d'automatisme et de contrôle) ainsi qu'une vingtaine de clauses techniques, non détaillées, par degré de sécurité.

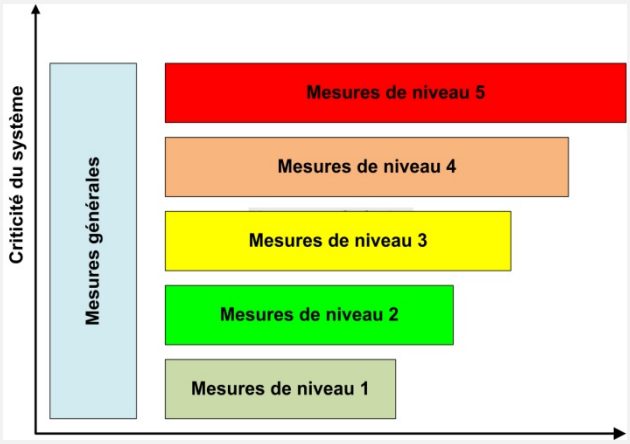


Figure 2 : Niveaux de sécurité selon l'AIEA

Lien avec les travaux ISA/IEC 62443

- Le standard ISA/IEC 62443-2-1 concerne typiquement dans sa nouvelle version, en cours d'élaboration, les IACS-SMS, avec des principes et des catégories de mesures de sécurité adaptées aux environnements industriels. Il repose sur les standards ISO/IEC 27001 et 27002 dont il reprend notamment l'articulation en 11 chapitres bien connue des professionnels de la sécurité des SIs. Il nécessitera, pour le nucléaire, quelques compléments spécifiques que pourrait apporter l'IEC-62645.
- le standard ISA/IEC 62443-3-3 approuvé par l'ANSI en août 2013, deviendra prochainement norme IEC. Le standard définit les mesures techniques de sécurité applicable aux systèmes désireux d'atteindre « en capacité » un niveau de sécurité donné (on y trouve donc définis les « SLs », Security Levels, initialement appelés "SALs", qui peuvent s'exprimer en « cible » (SL-T), « réalisation » (SL-A) ou « capacité » (SL-C)).

Les "niveaux" ISA/CEI et AIEA ne sont pas identiques mais il est possible d'établir une relation entre chaque catégorie pour qu'à un degré de sécurité IEC 62645 correspondent des mesures de sécurité d'un SL 62443-3-3.
Plusieurs comités nationaux suggèrent que l'IEC 62645, au lieu de développer à partir de zéro des chapitres dédiés au management de la cyber-sécurité d'une part et aux mesures techniques d'autre part, se réfère à des normes existantes et en particulier aux standards à l'ISA/IEC 62443-2-1 et -3-3.
Patrice Bock

Executive Order 13636 du président Obama

L'Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* signé le 12 février 2013 par le Président Obama a fait de la cyber-sécurité des grandes infrastructures l'une des priorités nationales aux Etats-Unis.

Il a mandaté le NIST (National Institute of Standards and Technology) pour proposer un référentiel incluant l'ensemble des standards, méthodologies et procédures qui permettront de mieux coordonner les approches technologiques et organisationnelles pour se prémunir des risques cyber-sécuritaires.

The White House
Office of the Press Secretary

For Immediate Release February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

Section 1. Policy. Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.

Figure 3 : Extrait de l'Executive Order du 12 février 2013

Une fois mis au point, normalement en début d'année 2014, les 16 secteurs critiques listés dans la Directive accompagnant l'Executive Order (énergie, transport, eau, santé, communications…), devront intégrer ce référentiel dans leur plan de protection.

L'ISA, dans le cadre de l'Automation Federation, participe activement aux travaux d'élaboration de ce référentiel, en particulier aux séminaires de travail organisés par le NIST dont le dernier s'est tenu à Dallas à la mi septembre 2013.

Six mesures pour contrôler la cyber-sécurité d'un système

La sécurisation des systèmes d'automatisme ne doit pas être une entreprise complexe

Par **Lee Neitzel** – Version française de **Christian Verney**

Résumé rapide

- L'objectif principal de la « cyber-sécurisation » d'un système d'automatisme est d'assurer la sécurité et la disponibilité, principalement en empêchant l'intrusion de logiciels étrangers, tels que les logiciels malveillants et les virus.
- Cet objectif peut être atteint en mettant en œuvre six mesures issues de la convergence des normes ISA/IEC/WIB. Ces étapes sont détaillées dans cet article.
- Les utilisateurs finaux peuvent améliorer la protection de leurs systèmes lors de l'exploitation et de la maintenance en collaborant avec des fournisseurs certifiés de matériel, de logiciels et de services

Si vous êtes comme la plupart des professionnels de l'automatisation de processus, vous êtes certainement conscient que vos systèmes d'automatisme ne sont pas aussi protégés qu'ils devraient l'être, et vous souhaitez apporter des améliorations. Mais vous êtes quelque peu perturbés par tous les discours en matière de sécurité industrielle et de normes ; vous cherchez une solution claire et précise pour une amélioration et non pas d'effrayants discours médiatiques.

L'objectif principal de la cyber-sécurité d'un système de contrôle est de protéger le site de fabrication et maintenir la production en état de marche. En revanche, la sécurité des systèmes d'information se concentre sur la protection des données, comme par exemple la prévention des vols de numéro de cartes de crédit. Dans les deux cas, la principale menace est le risque d'introduction de logiciels malveillants dans le système.

Un logiciel malveillant infecte habituellement un système par :

1- Les de mécanismes de transfert de fichiers, tels que les partages de fichiers et le protocole de transfert de fichiers (FTP) ;
2- L'exploitation de la vulnérabilité des réseaux face aux logiciels qui peuvent injecter du code dans le système ;
3- La copie automatique de fichiers dans le système a partir de médias portables, tels que les clés USB, les CD, les DVD et les téléphones cellulaires.

Pour faire face à cette menace, il faut suivre une approche en six étapes. Ces étapes sont issues des travaux du NIST, de l'ISA et des normes émergentes sur la cyber-sécurité qui sont désormais intégrées dans une seule norme internationale la série IEC 62443. Cette série de norme définit non seulement les mécanismes de sécurité d'un système de contrôle mais aussi la capacité des fournisseurs à durcir le système en place. En outre, des programmes de certification pour ces normes sont désormais en place pour les fournisseurs. Les activités de normalisation sont résumées dans la dernière partie de cet article.

Avant de déployer ces six mesures de sécurité, vous devez vous assurer que vous avez mis en place une politique de sécurité pour le système de contrôle. Si ce n'est pas le cas vous pouvez consulter et vous inspirer de la politique de sécurité mise en place par les services informatiques. Votre politique de sécurité doit supporter chacune des mesures décrites dans les paragraphes suivants afin de protéger votre système contre tous les logiciels non autorisés.

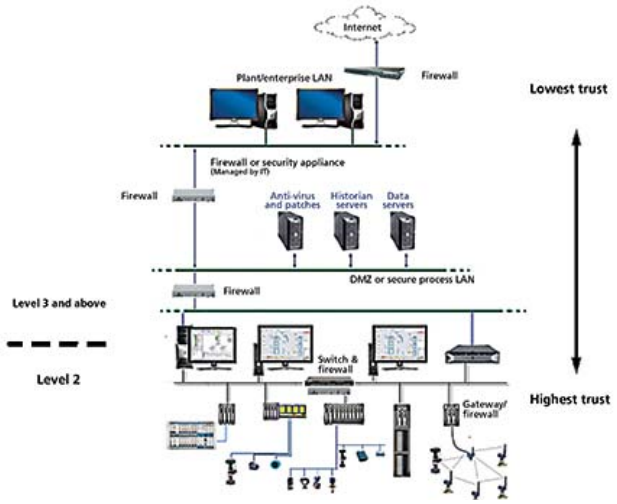
Six mesures pour la sécurité

Les mesures décrites dans cet article confirment qu'un bon niveau de sécurité ne peut être obtenu simplement en achetant un système de contrôle doté des fonctions de sécurité appropriées. La sécurité résulte autant du process que de la technologie. La mise en place de ces mesures s'adresse aux menaces de code malveillant mais également à toutes les autres attaques dont peuvent être victime les systèmes de contrôle.

Ces mesures peuvent être mises en œuvre de manière progressive, la sécurité peut être améliorée au fil du temps. L'évolution de la sécurité est définie par un modèle de maturité spécifié dans la norme IEC 62443. Cela devrait vous encourager à vous engager sur la voie de la sécurité et non plus considérer cette dernière comme une problématique effrayante difficile à résoudre. L'application de ces nouvelles normes de sécurité s'apparente à la mise en place laborieuse des ceintures de sécurité que nous refusions dans nos véhicules avant de reconnaitre plus tard les bienfaits quelles ont apportés

Mesure N°1: établissement d'un périmètre de sécurité autour des réseaux de communication

La première mesure consiste à établir des périmètres de sécurité pour les réseaux de communication afin de limiter les points d'accès par lesquels les logiciels malveillants peuvent pénétrer dans le système d'automatisme. Comme le montre le schéma ci-dessous, les réseaux de communication entre l'entreprise et les unités de production se situent au niveau 3 ou au dessus, tandis que les réseaux de contrôle du système sont au niveau 2 et en dessous.



Des pare-feux sont utilisés pour segmenter en interne le système de contrôle et l'isoler du niveau 3 et des réseaux externes. Vous devez vous assurer que tout le trafic vers/à partir du système de commande est crypté et traverse au moins un pare-feu. De plus, en aucun cas le poste de travail du niveau 2 ne doit avoir un accès direct à Internet ou une adresse IP qui lui permette d'être directement accessible à partir de l'Internet.
Dans le système de contrôle, les pare-feux doivent être utilisés pour isoler les contrôleurs, les réseaux d'appareils sans fil et les réseaux SIS des postes de travail du niveau 2. En outre, les commutateurs avec des ports qui se verrouillent doivent être utilisés pour empêcher les périphériques non autorisés de se connecter au système de contrôle.

Ces pare-feux et ces commutateurs, en conjonction avec les pare-feux entre le niveau 3 et le niveau 2 créent une superposition de périmètres de sécurité, le plus bas degré de confiance étant attribué au niveau 3 et le niveau le plus élevé au niveau 1.
Les composants qui ne sont pas critiques du point de vue de la sécurité et de la disponibilité, comme les serveurs d'historiques ou de données, doivent être installés à un niveau supérieur de la hiérarchie, avec moins de protection mais avec en conséquence un accès plus facile, de façon que le personnel de fabrication puisse visualiser les données et effectuer les interventions nécessaires.
Une fois que les pare-feux et les commutateurs sont installés, ils doivent être maintenus pendant toute la durée de vie du système afin de rester efficaces. Les règles de filtrage doivent être à jour pour refléter les modifications contre les nouvelles menaces apportées aux IT et aux systèmes de contrôle et de protection. Les ports de commutateur non utilisés doivent être contrôlés régulièrement pour s'assurer qu'ils sont toujours verrouillés.

Mesure N°2 : durcissement des postes de travail

La deuxième mesure a trait au durcissement des postes de travail du système de contrôle afin de rendre plus difficile l'accès au système par les logiciels malveillants. Cinq actions primordiales pour ce durcissement doivent être effectuées :

- Tout d'abord pour définir les politiques de sécurité du poste de travail, il faut appliquer le modèle de durcissement « Center for Internet Security (CIS)" ;
- Deuxièmement, les postes de travail doivent être consacrés uniquement à des fonctions d'ingénierie et d'exploitation et, à ce titre, toutes les applications, les services et les ports qui ne sont pas utilisés pour ces fonctions doivent être supprimés ou désactivés pour que les vulnérabilités connues ou inconnues qu'ils peuvent véhiculer ne puissent être exploitées ;
- Troisièmement un logiciel anti-virus doit être installé pour détecter et supprimer les logiciels malveillants connus avant qu'ils infectent le poste de travail. De plus les versions d'anti-virus doivent être mises régulièrement à jour pour faire face aux nouveaux virus qui circulent ;
- Quatrièmement, les fichiers systèmes doivent être configurés pour permettre uniquement aux utilisateurs autorisés d'accéder aux fichiers sensibles. Le principal défaut est de permettre aux utilisateurs avec des privilèges d'administrateur d'accéder à tous les fichiers d'un poste de travail. Les utilisateurs doivent être sérieusement identifiés et doivent seulement avoir accès aux fichiers et répertoires dont ils ont besoin.
- Cinquièmement, les clefs USB, les CD et les lecteurs de DVD doivent être verrouillés lorsqu'ils ne sont pas utilisés à des fins autorisées. En outre, il convient de rappeler aux utilisateurs que l'utilisation de médias portables est un moyen classique d'infecter un système. Il n'est pas rare pour un attaquant de déposer les clés USB infectées dans l'espoir que quelqu'un les branchera sur un poste de travail.
- Enfin pour se protéger essentiellement contre les infections mémoire, ces actions pour durcir le système peuvent être complétées par un redémarrage régulier du poste de travail. Certaines attaques plus sophistiquées et plus difficiles à détecter reposent sur l'installation de logiciels malveillants résidant en mémoire. Les postes de travail qui fonctionnent 24h/24 et 7j/7 sont la cible de ce type d'attaques ; le redémarrage de ces postes de travail lorsque c'est possible supprimera ce type d'affectation.

Mesure N°3 : gestion des comptes utilisateurs

La troisième mesure s'adresse à la gestion des comptes utilisateurs. Il faut accorder aux utilisateurs uniquement les privilèges dont ils ont besoin. Leurs mots de passe doivent être suffisamment longs et l'emploi d'une combinaison de trois des quatre critères suivants doit être exigée : majuscules, minuscules, chiffres et caractères spéciaux. L'octroi d'un ensemble limité de privilèges restreint la capacité d'un logiciel externe ayant infecté le programme d'un utilisateur d'utiliser des privilèges élevés pour accomplir un acte malveillant.

L'utilisation de mots de passe complexes rend la tâche des pirates plus difficile pour découvrir ou reconstruire les mots de passe. La politique de sécurité doit définir la période de validité d'un mot de passe et empêcher la réutilisation des dernières combinaisons.

La protection par des mots de passe lutte contre les logiciels malveillants qui veulent accéder au système, mais protège également contre les pirates qui essaient de se connecter au système.

Si un logiciel malveillant s'exécute dans un programme utilisateur il est en mesure d'acquérir le mot de passe d'un administrateur et faire démarrer un autre programme utilisant les informations d'identification de l'administrateur. Ces techniques sont couramment utilisées par des logiciels malveillants pour accroitre leurs privilèges.

Mesure N°4 : mise à jour des patches de sécurité

Cette mesure concerne la mise à jour des logiciels (patches) du système d'exploitation et des logiciels du système de contrôle. Ces mises à jour suppriment les vulnérabilités des logiciels pouvant être infectés. En effet des outils gratuits disponibles sur Internet permettent aux pirates de rechercher les vulnérabilités d'un poste de travail et ensuite d'injecter automatiquement les logiciels malveillants qui démarrent des exécutables de commande ou téléchargent des codes pirates sur le poste de travail.

Evidemment les mises à jour doivent être préalablement testées afin de vérifier qu'elles ne perturberont pas le logiciel du poste de travail. Pour valider tous les correctifs de sécurité des systèmes il est recommandé de collaborer avec des fournisseurs certifiés.

Mesure N° 5 : sauvegarde et restauration

La cinquième mesure a trait à la mise en œuvre d'un plan de sauvegarde et de récupération. Une sauvegarde efficace et un plan de relance permet de restaurer dans l'état initial les données de configuration et les logiciels d'un système infecté. Les fournisseurs certifiés sont tenus d'avoir une stratégie de sauvegarde et de récupération qui définit et spécifie quand et comment restaurer un système dans un état stable même s'il n'y a aucun signe d'infection. Ceci est important car les logiciels malveillants sophistiqués sont indécelables et sommeillent jusqu'au moment propice.

Mesure N° 6 : surveillance des mesures de sécurité et des risques

La sixième mesure concerne la surveillance des activités suspectes et l'évaluation des risques. Des solutions de sécurité d'inspecter et d'analyser l'historique des connexions aux stations de travail, aux pare feux, aux commutateurs et aux divers appareils afin de détecter la présence de logiciels étrangers. Certaines packages de surveillance inspectent le trafic réseau, ainsi que l'utilisation du processeur et de la mémoire, à la recherche d'anomalies. En l'absence de plans de surveillance automatisés, un examen manuel des journaux d'événements et du trafic réseau doit être effectué pour rechercher des activités suspectes, par exemple une augmentation inattendue du trafic réseau lors des heures creuses

L'évaluation des risques doit être effectuée lors de la conception initiale, avant la mise en service et pendant le cycle de maintenance du système pour s'assurer que les changements apportés au système n'altèrent pas la sécurité. Les mesures prises après une évaluation des risques peuvent inclure de nouvelles règles pour les pare-feux, le verrouillage de nouveaux ports de commutation, une politique concernant les mots de passe plus contraignante, la suppression des logiciels inutilisés et de meilleures procédures de gestion de la connexion des périphériques externes comme les clés USB.

Une convergence des normes pour simplifier la conformité

Par le passé, plusieurs entités différentes ont travaillé de manière séparée pour formuler des normes de sécurité, mais ces groupes se sont réunis pour créer une norme commune, ce qui va simplifier grandement la mise en œuvre d'une conformité. Le NIST participe également à cet effort ; sa participation a été renforcée le 12 Février 2013 par un « Executive Order » intitulé «Amélioration de la cyber-sécurité des infrastructures critiques."

Il y a dix ans, l'ISA a créé le projet ISA99 « Sécurité des automatismes et des systèmes de contrôle » pour développer une gamme complète de normes de sécurité pour l'industrie des automatismes. Le résultat de ce travail a été proposé à la CEI ; c'est ainsi que les spécifications ISA sont à l'origine de la série IEC 62443.

En parallèle, l'Association néerlandaise « International Instrument Users », désormais connue sous l'appellation WIB, a créé une norme de sécurité définissant « les bonnes pratiques des fournisseurs de systèmes de contrôle ». Cette norme complète la suite ISA 99 et est venue intégrer la série IEC 62443.

Toujours en parallèle, deux normes pour la certification du niveau de sécurité des produits ont été développées, l'ISA SecureDevice et le « Wurldtech's Achilles Communication Certification » ; ces normes complètent la suite ISA 99 et sont en cours d'intégration dans la série IEC 62443.
En résumé, Il y a une convergence de l'industrie autour de la norme IEC 62443. Cette norme fournira un ensemble très complet de standards pour la cyber-sécurité industrielle avec des normes pour les organisations, les systèmes de contrôle, les composants, la mise en œuvre et la maintenance. Les programmes de certification existants demeurent, mais ceux-ci feront désormais référence à la série de normes IEC 62443 plutôt qu'a des spécifications propriétaires.

Conclusion

La sécurité industrielle est beaucoup plus qu'une simple affaire de matériel ou de logiciel. Les responsables de projet et les personnes en charge du personnel ont la responsabilité de promouvoir la prise de conscience cyber-sécuritaire. Ils doivent s'assurer qu'il est possible de durcir les systèmes de contrôle en appliquant la politique de sécurité définie pour le site.
Les normes émergentes et la convergence autour de l'IEC 62443 créent de nouvelles exigences pour les fabricants de systèmes/composants de contrôle et pour les fournisseurs de services d'exploitation et de maintenance. Dans le cadre de l'IEC 62443, les programmes de sécurité doivent suivre un processus d'évolution afin d'être toujours plus efficaces.
Enfin, un certain nombre de constructeurs/fournisseurs ont obtenu les certifications qui attestent de leur engagement à contrôler la sécurité système. La collaboration avec des constructeurs et des fournisseurs de services certifiés réduit les coûts et les risques, la conformité est plus rapide lors de la mise en œuvre mais également sur l'ensemble du cycle de vie du système d'automatisation.

ISA-France - Programme de formation novembre 2013

Code	Désignation	Calendrier 2012	
		Lieu	Date
JPH1	ISA-100 et les applications nouvelles des radiocommunications dans l'industrie - Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	26 et 27 novembre 2013
JPH2	Réseau maillé ISA-100 - Approfondissement et mise en œuvre- Un jour *Le suivi préalable de la formation JPH1 est recommandé*	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	28 novembre 2013
JPH3	ISA/CEI 62443 (ISA99) - Cyber-sécurité des systèmes de contrôle - Un jour	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	25 novembre 2013
JVI1	ISA-88 - Conception fonctionnelle du contrôle-commande industriel		Nous consulter
JVI2	ISA-95 - MES et intégration ERP/Exécution		Nous consulter
JVI3	ISA-88/95 - Architecture d'entreprise - Système de production industriel		Nous consulter
JVI4	B2MML/BatchML - Pratique des interfaces entre systèmes informatiques industriels		Nous consulter
JV15	ISA-88/ISA-95/B2MML : Spécification fonctionnelle et interopérabilité en informatique industrielle - Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	20 et 21 novembre 2013
JVI6	Manufacturing Intelligence : Construire la Performance dans l'Entreprise	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	22 novembre 2013
BRI1	ISA-84 - Sûreté de fonctionnement avec les normes IEC61508 et IEC61511- Deux jours	**Rueil-Malmaison** KB Intelligence	12 et 13 novembre 2013

		10, rue Lionel TERRAY	
RCY1	**IS0-CEI-G.UM. : Estimation et calcul de l'incertitude de mesure dans l'industrie - deux jours**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	18 et 19 novembre 2013
BDC1	**Normalisation dans le domaine de l'automation - Deux jours**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	14 et 15 novembre 2013

ISA-France est reconnue comme un organisme indépendant et qualifié de formation des ingénieurs et techniciens du monde de l'automation dans les pays francophones d'Europe ou du Maghreb (Enregistrement auprès de la préfecture d'Ile de France sous le N° 11754084175). Ses programmes, conçus sur la base des standards ISA, couvrent les problèmes d'actualité du secteur de l'automation : wireless, cyber-sécurité, conception et sécurité fonctionnelles, intégration, instrumentation et mesure, normalisation.

Il est également possible d'accéder aux cours dispensés par l'ISA (USA) selon les modalités décrites sur le site www.isa.org ou d'organiser des sessions de formation intra-entreprises (Pendre contact avec ISA-France sur contact@isa-france.org ou au +33 (0)1 41 29 05 09).

Pour tout renseignement sur les stages ISA-France

- Tel : +33 (0)1 41 29 05 05 – Sandrine Taisson
- Fax : +33 (0)1 46 52 51 93
- contact@isa-france.org
- Télécharger un bulletin d'inscription (à retourner par fax ou par courrier électronique)
  au format PDF au format Word

Adhérer à l'ISA et à l'ISA-France, c'est :

- **Accéder à des conditions préférentielles à 150 standards reconnus mondialement et à plus de 2500 documents techniques,**
- **Bénéficier de réductions importantes sur les manifestations ou formations organisées par l'ISA ou l'ISA-France,**
- **Accéder à une base documentaire de milliers de documents**
- **Entrer dans un réseau de 25 000 professionnels de l'automation**
-

Informations et bulletins d'adhésion sur www.isa-france.org et www.isa.org

Pour toute demande de renseignements : Tel +33 1 41 29 05 09 ou contact@isa-france.org

Direction de la publication : Jean-Pierre Hauet – ISA-France 10 rue Lionel Terray 92500 Rueil-Malmaison