14 mars 2013

Cyber-sécurité des installations industrielles : la norme CEI 62443 (ISA-99) progresse

En publiant dès 2007 les premiers référentiels spécifiques à la cyber-sécurité industrielle, le comité 99 de l'ISA avait bien anticipé la nécessité, aujourd'hui avérée, d'assurer une solide protection des infrastructures critiques. Les attaques récentes (Stuxnet, Duqu, Shamoon, Gauss, Flame…) en attestent.

Les travaux de l'ISA99 sont à présent menés en harmonie avec ceux de la CEI et on parle aujourd'hui davantage de norme CEI 62443 que de norme ISA-99. Les deux ensembles normatifs ont fusionné allant ainsi au-delà de ce qu'il fut possible de faire pour l'ISA-84, la CEI 61508 et ses normes dérivées.

Cyber-sécurité et sécurité fonctionnelle constituent à présent les deux grandes préoccupations sécuritaires visant à parvenir à une situation sûre (safe) dans les systèmes E/E/PE (Electrical, Electronic, Programmable Electronic). La cyber-sécurité est un sujet complexe et le référentiel ISA/CEI comporte plusieurs volets, à l'instar des normes ISO 2700x ou des référentiels américains NIST 800-xx (qui ne sont pas normatifs).

Dans un premier temps, trois documents fondateurs de l'ISA-99 ont été publiés mais les événements survenus depuis 2010 réclamaient leur mise à jour et la publication des autres cahiers. L'ISA a pour cela constitué une dizaine de « working groups » pour mener en parallèle ces chantiers. La participation de consultants reconnus dans le domaine (Eric Byres, Joe Weiss…) et la contribution de très nombreux professionnels, constructeurs (Emerson, Invensys, Rockwell, Siemens, Yokogawa…), opérateurs (Dow Chemical, Shell, Aramco, Bayer…) et organismes compétents (NIST, INL, Exida…) permettent d'élaborer des documents de qualité, à la hauteur des enjeux de la défense des installations critiques et prenant en compte la réalité opérationnelle du terrain.

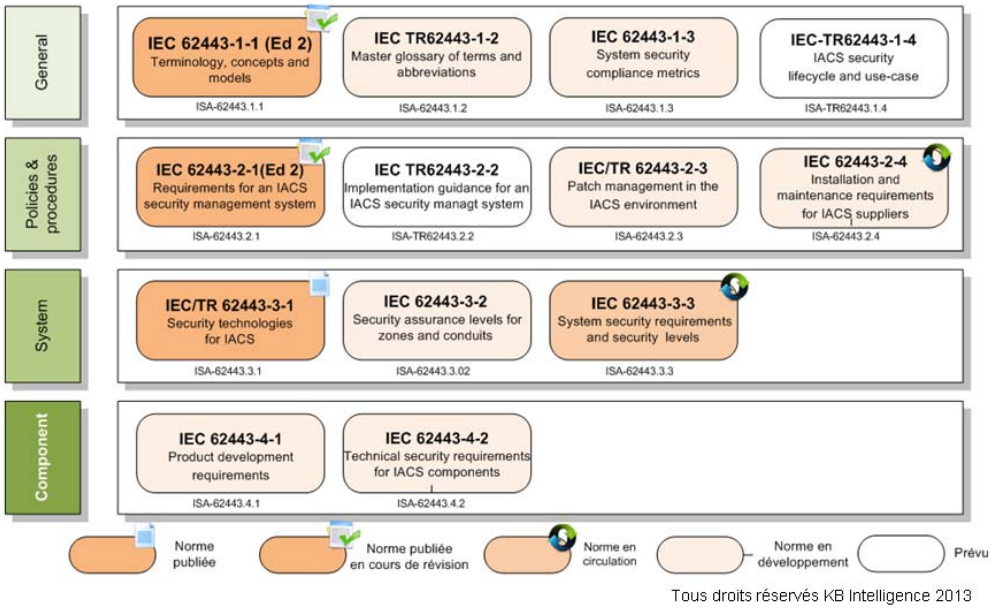
Un autre point important à mentionner est la prise en compte dans la révision des documents, et plus spécifiquement dans celle du 62443-3-1 relatif aux systèmes de management de la sécurité des systèmes de contrôle et d'automatismes (IACS-SMS en anglais), des normes ISO 27001 (Techniques de sécurité - Systèmes de management de la sécurité de l'information - Technologies de l'information - Exigences) et ISO 27002 (Techniques de sécurité - Technologies de l'information - Code de pratiques pour la gestion de sécurité d'information).

Le tableau ci-aprèsrécapitule l'ensemble des cahiers ISA/IEC 62443 publiés à ce jour ou en cours de révision ou de développement. Les professionnels désireux de disposer de davantage de précisions sur les normes ISA/IEC 62443 peuvent se rapprocher de l'association ISA-France (contact@isa-france.org) qui organise périodiquement ou sur demande des formations sur le sujet.

Les documents **IEC 62443-2-1** (révision 2013) **et IEC 62443-3-3** (nouveau document) ont fait récemment l'objet de votes positifs au sein de l'ISA et ont entamé la dernière ligne droite avant publication (prise en compte des commentaires, ajustements mineurs, transfert et validation par l'IEC TC65 – Technical Committee 65 de la CEI).

L'IEC 62443-2-1, basé sur les normes ISO 27000, définit un modèle de système de management de la sécurité (IACS-SMS) et un catalogue de recommandations pour l'établissement de « *policies and procedures* » adaptées aux environnements du contrôle et des automatismes, avec une structure selon les 11 chapitres de l'ISO 27002. Comme les autres référentiels dédiés aux systèmes industriels (NIST 800-82, AIEA NSS #17…), les chapitres concernant la formation (8.8.2), la gestion de la sous-traitance (10.2) et les achats et recette (12.1), prennent en compte les spécificités des usines et installations critiques.

Structure documentaire CEI-62443 (2013)
Ancienne référence : ISA 99



Il faut cependant noter que les problèmes très spécifiques aux environnements industriels, à savoir la gestion des configurations et des mises à jour et l'organisation de la maintenance, feront l'objet de cahiers spécifiques de la série 62443, respectivement -2-3 (en cours de finalisation) et -2-4, (en cours de développement).

L'IEC 62443-3-3, également voté en comité ISA99 et donc en cours de finalisation, définit en termes techniques précis les mesures de sécurité à mettre en œuvre dans un IACS (Industrial Automation Control system) pour permettre aux installations qui en seront équipées d'atteindre un niveau de sécurité donné (selon l'échelle des SL, ou « *Security Levels* », allant de 1 à 4, le niveau 0 étant réservé aux systèmes n'offrant pas les garanties minimales pour être classés 1).

Ce document est essentiel dans la série. Il bénéficiera de l'apport des autres documents mais peut être utilisé indépendamment. Les mesures de sécurité y sont définies avec des exigences croissantes selon les « SL », sur la base d'une centaine d'exigences regroupées selon les sept « foundational requirements » de l'ISA/IEC 62443 : identification & authentification, contrôle d'usage, intégrité des systèmes, confidentialité des données, contrôle des flux de données, réponse en temps approprié aux événements, disponibilité des ressources (nota : traduction non officielle des termes anglais).

Ces mesures de sécurité prennent en compte les exigences temps-réel (priorité aux tâches de contrôle par rapport aux tâches de sécurité) et de l'organisation du travail (par exemple notion de travail en équipes pour cadrer l'usage d'identifiants communs). Elles sont encadrées par une logique donnant la primauté aux fonctions « essentielles » (essentiellement la sécurité fonctionnelle), avec des indications sur la manière de concilier éventuellement des exigences a priori contradictoires.

Les autres documents de la série -3, viendront compléter cette approche technique. En particulier :

- Le -3-1 : solutions techniques de sécurité. Ce document a été publié en tant que rapport technique sous la référence « ANSI/ISA-TR99.00.01-2007 ». Il définit les notions de zones et conduits et décrit les contremesures techniques relevant de l'état de l'art pouvant être mises en œuvre pour assurer la cyber-sécurité d'un IACS. Sa mise à jour vient d'être lancée afin d'y inclure les techniques les plus récentes (filtrage applicatif sur les protocoles industriels etc.).

- -3-2 : définition et règles pour le découpage en zones (segmentation de réseaux industriels), règles d'évaluation des besoins de sécurité cible (SL-T – security level - target). Ce document sera probablement renommé « Risk Assessment and Design ».

  L'analyse de risque joue en effet un rôle essentiel dans la définition des Security Levels assignés à chaque zone. C'est la combinaison de la probabilité de réalisation d'une menace avec l'évaluation de ses conséquences éventuelles qui détermine la criticité du risque et donc le niveau de protection (SL) à mettre en place. Si la norme définit des lignes générales pour définir des échelles de criticité, il reste de la responsabilité de chaque responsable de définir son échelle de risques, en fonction de la nature de ses acticités et de l'environnement dans lesquels il est plongé. Cette échelle de risques doit ensuite être mise ne relation avec l'échelle des niveaux de sécurité.

Les publications du nouveau cahier -2-1 et du cahier -3-3 sont prévues d'ici la fin 2013.