ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°56 – Mars 2015 **Bulletin d'information d'ISA-France**

Sommaire | Evénements | Standards | Technologie | Formation

Au sommaire de ce numéro :

- **Evénements** : Atelier ISA-France sur les drones le 8 avril à Paris – Conférence du District 12 les 15 et 16 mai à Tel Aviv – Séminaire Sûreté et sécurité de fonctionnement des systèmes critiques – Le 20 octobre 2015 à Lyon avec L'INSA de Lyon
- **Standards :** La cybersécurité des systèmes de contrôle : comparaison entre les approches ISA/IEC et ANSSI
- **Technologie :** Les automatismes industriels et l'Internet des objets
- **Formation** : Programme de formation ISA-France 2015

Sommaire | Evénements | Standards | Technologie | Formation

« Technologie des drones, pilotage et sécurité » Atelier ISA-France - Le mercredi 8 avril à Paris de 18h00 à 20h30

Les ateliers ISA-France sont l'occasion d'approfondir, dans le cadre convivial des Ateliers du Bac à Paris, un sujet technique ou économique de première importance, en venant écouter des spécialistes du domaine. Une occasion de parfaire ses connaissances et développer de nouveaux contacts.

L'atelier du mercredi 8 avril 2015 sera consacré aux drones.

Les drones ont été ces derniers mois à la une des quotidiens ; leur utilisation donne lieu à des « faits d'armes » spectaculaires. Mais la complexité d'un système de drones reste méconnue et cet atelier a pour objet d'approfondir certains aspects techniques du développement et de l'exploitation des drones. A travers trois interventions, il donnera une image scientifique de la réalité de ce marché, en regard des emballements médiatiques qui ne prennent pas toujours bien en compte certains éléments structurants.

Le programme :

18h00 – 18h30 : Accueil aux Ateliers du Bac - 69 rue du bac - 75007 PARIS

18h30 – 18h50 : Les drones, un univers diversifié dans lequel la communication masque souvent la technologie et l'expertise – Bertrand Ricque - Chef de programme - Optronics & Defence division – Sagem.

18h50 – 19h10 : L'insertion des drones dans l'espace aérien – Sylvain Pouillard - Ingénieur en chef drones – Sagem

19h10 – 19h30 : Conception, fabrication et exploitation de drones, des limites bornées par l'imagination –Jeremy GAYA - Industrialization Engineer – Infotron

19h30 – 20h30 : Questions-Réponses suivies d'un pot amical

Programme détaillé et bulletin d'inscription sur www.isa-france.org

Participation aux frais : membre ISA 40 € - Non membres ISA 60 € - Paiement possible en ligne

Conférence annuelle du District 12 - Les 15 & 16 mai 2015 à Tel Aviv

La conférence annuelle du District 12, rassemblant les sections d'Europe, du Moyen-Orient et de l'Afrique (EMEA) de l'ISA, se tiendra les 15 et 16 mai 2015 à l'hôtel Sheraton de Tel Aviv. Les membres de l'ISA-France intéressés à y participer sont invités à se rapprocher de l'ISA-France (contact@isa-france.org ou 01 41 29 05 09) pour tout renseignement relatif à cette importante manifestation (programme, inscription, réservation).

A noter : Sûreté et sécurité de fonctionnement des systèmes critiques – Le 20 octobre 2015 à Lyon

ISA-France organise avec l'INSA de Lyon, le 20 octobre 2015, un séminaire sur **la sûreté et sécurité de fonctionnement des systèmes critiques.**

Contrôle-commande des systèmes embarqués et des procédés industriels à risque : de la conception à la validation – Quelles spécificités ? Quelles convergences ? Quel impact peut avoir le risque cyber-sécuritaire ? Programme en cours de préparation – Renseignements : 01 41 29 05 09

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

La cybersécurité des systèmes de contrôle : comparaison entre les approches ISA/IEC et ANSSI

L'ISA a été pionnière en formalisant une approche graduée de cyber-sécurisation des systèmes numériques industriels, basée sur le concept de niveau de sécurité qui est noté en abrégé « SL » (Security Level) dans les documents constitutifs de le standard ISA99, aujourd'hui repris par la CEI en tant que norme IEC 62443.

Ce type d'approche est devenu un dénominateur commun dans le domaine des SI industriels et a été adopté par d'autres standards publiés depuis : dans le nucléaire (IEC 62645, NRC 5.71, AIEA NSS#17), dans d'autres référentiels de l'industrie (NIST 800-82 r2 en cours de finalisation) et par l'ANSSI dans deux documents essentiels : « *Méthode de classification et principales mesures* » et « *Mesures détaillées* » publiés en janvier 2014. Les grands groupes industriels qui ont initié des programmes de cybersécurité retiennent également ce type d'approche, souvent en déclinant l'un ou l'autre des référentiels.

Face à cette multiplication des référentiels, les équipementiers (actionneurs, automates, supervision…) et les intégrateurs s'inquiètent de savoir si ces approches sont compatibles entre elles et notamment avec les exigences françaises éditées par l'ANSSI. Plusieurs constructeurs d'automates ont étudié de près les exigences ANSSI pour les comparer à celles de l'ISA/CEI mais les résultats restent confidentiels. ISA-France et le groupe de travail SCADA du CLUSIF ont donc décidé de réaliser une étude similaire pour la partager publiquement : c'est l'objet du présent article qui traite des niveaux et critères de classification, avant de se pencher précisément sur la comparaison de certaines exigences.

Les concepts fondamentaux

Les classes de l'ANSSI

L'ANSSI a défini trois classes de cybersécurité[1] pour des installations ou parties d'installations. A ces trois classes, numérotées de 1 à 3, on pourrait ajouter une « classe 0 » correspondant aux systèmes que l'on considère comme non critiques et pour lesquels les exigences de sûreté permettent à minima de se prémunir contre les menaces liées à la négligence.

Le niveau d'exigence va croissant de quelques dizaines de recommandations pour la classe 1 à plus de 100 directives pour la classe 3. Les mots « recommandations » et « directives » ont leur importance ici car ils soulignent le caractère obligatoire ou non de l'exigence.

Les exigences sont regroupées dans les documents précités de l'ANSSI en deux chapitres principaux[2] (chapitre 3 – Mesures de sécurité organisationnelles et chapitre 4 – Mesures de sécurité techniques), au sein desquels on trouve une dizaine de sous-chapitres regroupant les exigences en sous-domaines. Elles portent donc sur des aspects organisationnels (responsabilité et organisation de la sécurité, intégration de la cybersécurité dans le cycle de vie des projets…) et techniques (mesures de sécurité : par exemple, gestion de mots de passe, segmentation des réseaux...) soit tout le spectre typique d'exigences.

Les SL (security levels) de l'ISA/IEC 62443

Le niveau de protection qui doit être apporté à un système ou une zone d'un SI industriel[3] est définit au travers des « Security Levels » (SL). Quatre niveaux de SL sont définis avec pour objectif de renforcer le niveau de robustesse des mécanismes de sécurité au fur et à mesure que l'on accroît le SL du système.

Le document 62443-3-3 définit des exigences techniques pour des systèmes, classées selon les sept « Functional requirements » (FR) retenus par la norme. Ces FR couvrent tout le spectre des mesures techniques, depuis le FR1 « Identification & Authentification » jusqu'au FR7 « Disponibilité ».

L'approche est plus complexe que celle des classes ANSSI, car le niveau de sécurité SL n'est pas nécessairement identique d'un FR à l'autre, ce qui conduit à caractériser le niveau de sécurité par un « vecteur SL « à sept composantes.

La notion de niveau de sécurité s'applique à trois objectifs distincts mais complémentaires :

[1] Document « Méthode de classification et principales mesures», publié en janvier 2014, disponible sur le site de l'ANSSI.

[2] Document « Mesures détaillées », publié par l'ANSSI en janvier 2014, disponible sur le site de l'ANSSI.

[3] Le découpage en zones et conduits est abordé dans le document introductif 62443-1-1, dans l'annexe A du standard 62443-3-3 et dans le document 62443-3-2 en cours de finalisation.

1. la détermination d'un niveau cible à atteindre pour un système donné: on parle alors de SL-T (T pour target = cible) ;
2. l'évaluation du niveau de sécurité effectivement atteint : c'est le SL-A (A pour achieved = atteint) que l'on mesure via un audit par rapport au référentiel IEC 62443-3-3 ;
3. l'aptitude d'un composant ou d'un système à permettre l'obtention d'un niveau de sécurité donné : c'est le SL-C (C pour capability = capacité). Ce niveau peut être variable suivant le FR. Ainsi un composant donné peut être SL- C (3)=4 pour le FR3 (Integrity) mais SL-C (5)=2 pour le FR5 (Data flow control c'est-à-dire le contrôle des flux de données).

La logique de l'approche est donc de définir un SL-T pour un système (a priori commun à tous les FR) puis de concevoir le système en combinant des composants qui ont des capacités au moins suffisantes pour ce SL, ou alors de palier un SL-C trop faible (par exemple vis-à-vis du contrôle de flux de données) en rajoutant un équipement de contre-mesure (par exemple un pare-feu) d'atteindre un SL-A ≥ au SL-T.

Dans le cadre de notre comparaison avec la classification de l'ANSSI, comme celle-ci traite des installations et a minima des systèmes au travers des classes, nous nous concentrerons sur le niveau « système » et donc sur le concept de SL-T, pour lequel l'IEC 62443-3-3 définit des exigences, en les comparant à celles de l'ANSSI au niveau système. Une approche similaire peut être conduite au niveau « composant » pour lequel les exigences ISA/CEI sont définies par l'IEC 62443-4-2.

Les principales différences entre les deux approches

Affectation des systèmes à des classes (ANSSI) ou à des SL (ISA/CEI)

Une méthode d'affectation à une classe est suggérée dans le document de l'ANSSI et est conforme à l'esprit « High-level risk analysis »[4] de l'ISA/CEI, à savoir une prise en compte à la fois de l'impact en cas de cyber-attaque réussie (sur les personnes, les biens, l'activité économique et l'environnement) et d'une estimation de sa probabilité sur la base d'un modèle prenant en compte les type de systèmes, la connectivité, l'accessibilité et le type d'attaquants.

Pour l'ANSSI comme pour l'ISA/CEI, l'approche est aujourd'hui plutôt qualitative, guidée par des scénarios. L'ISA/CEI mentionne (annexe A de 62443-3-3) qu'avec l'augmentation des connaissances et des modèles mathématiques sur les attaques, risques et les incidents, on peut espérer à terme avoir des modèles plus quantitatifs, basés sur des approches statistiques.

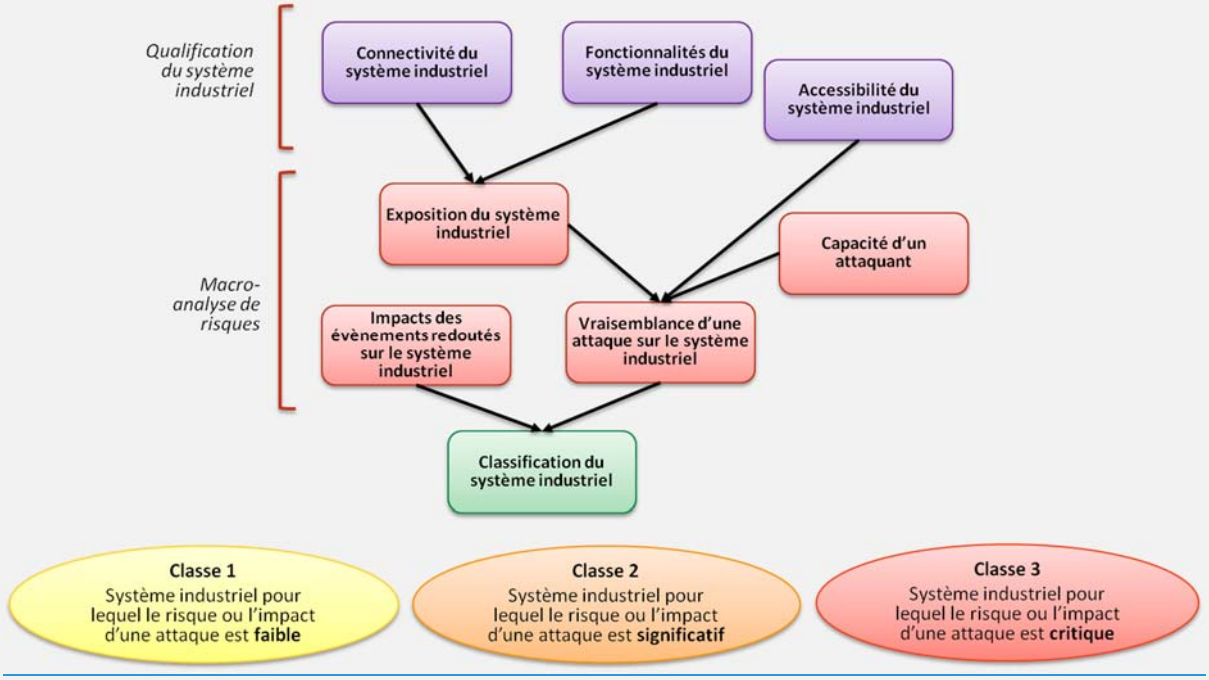

Figure 1 : Logique d'affectation à une classe selon l'ANSSI.

[4] Le document IEC 62443-2-1 prescrit deux niveaux d'analyse de risque, dénommés respectivement analyse de haut niveau et analyse détaillée.

L'ISA/CEI ne traite pas encore, dans les documents publiés, de la manière d'attribuer un SL-T à un système, notamment parce que le concept de SL est plus récent que la plupart des documents déjà publiés. On peut cependant noter que :

- 62443-2-1 décrit le principe d'une analyse de risque « High-level », avec évaluation d'impact et de probabilité ;
- 62443-3-2[5] explicite la manière de réaliser une « High-level risk analysis », ainsi que le regroupement de systèmes en zones et les règles de communication entre zones. La dernière étape, consistant à attribuer un SL-T à l'ensemble des systèmes d'une zone, serait du ressort de l'opérateur.

L'ISA/CEI établit un lien entre chaque niveau SL et le niveau des attaquants contre lesquels on cherche à se prémunir :

- SL1 : accès accidentel au système et erreurs. SL1 permet d'assimiler à des sources de menaces malveillantes les erreurs humaines non prévues par les analyses de sûreté et pouvant avoir des impacts de sécurité ;
- SL2 : attaquants utilisant des moyens simples, dotés de ressources faibles, de compétences générales et ayant une motivation faible ;
- SL3 : attaquants très actifs, utilisant des moyens sophistiqués, dotés de ressources et d'une motivation modérées et de compétences spécifiques ;
- SL4 : attaquants très actifs, dotés de moyens sophistiqués, de ressources étendues, de compétences spécifiques et d'une motivation élevée.

Il existe un lien entre le type d'attaquants et les objectifs visés : les attaquants SL1 ne cherchent pas a priori à nuire et donc ne peuvent toucher que des systèmes exposés peu sensibles tandis que les attaquants SL4 visent les systèmes les plus critiques dans le but de détourner leurs fonctionnalités (type de menaces les plus inquiétantes en SI industriels). L'intérêt de cette approche, par les moyens et connaissances nécessaires pour réaliser l'attaque, est d'apporter une certaine cohérence entre le niveau des attaquants et le niveau de robustesse des mesures.

La gradation dans les exigences telles que définies par l'ANSSI abordent aussi bien les mesures de sécurité organisationnelles que techniques. Dans le cas de l'ISA/CEI par contre, la différenciation en niveaux n'existe que pour les mesures de sécurité techniques listées dans le document 62443-3-3 pour les systèmes et dans le document 62443-4-2 pour les composants. Pour les mesures de sécurité organisationnelles, l'ISA/CEI reprend dans le document 62443-2-1, dont la nouvelle version est en cours de finalisation, les exigences des normes ISO 27001 et 27002 en les adaptant au cas des systèmes de contrôle et d'automatisme.

Les exigences de l'ANSSI en matière de sécurité dans les projets impliquent la mise en place d'une organisation projet et des tests techniques pour s'assurer d'une prise en compte efficace de la sécurité. Dans le corpus de l'ISA/CEI, on retrouve ces deux types d'exigences dans le 62443-2-1 d'une part et dans le 62443-3-3 et le 62443-4-2 d'autre part, avec pour ces derniers documents une hiérarchisation selon les SL.

Pour la compréhension de ces références, la figure 2 en fin d'article décrit le plan documentaire de la norme ISA/IEC 62443 en distinguant les quatre niveaux : General, Policies and Procedures, System, Component.

Communications entre systèmes de classes et SL différents

L'ISA a dès 2007 introduit le concept de zones de sécurité correspondant à des regroupements physiques et/ou logiques de système, sous-systèmes ou composants présentant des exigences similaires en matière de cybersécurité. Ces zones sont reliées par des conduits qui regroupent des canaux de communication que ce soient les réseaux, des personnes ou des media amovibles. Un SL-T est ainsi assigné à chacune des zones.

Les conduits relient les zones et qui sont des cas particuliers de zones de sécurité. Ils doivent donc également recevoir un SL-T.

L'ANSSI inclut de son côté dans ses exigences techniques des contraintes sur les communications entre systèmes ou installations de classes différentes, requérant par exemple d'utiliser une "data diode" pour imposer un flux unidirectionnel depuis les systèmes de classe 3 vers les systèmes de classe 2.

Les deux référentiels exigent la segmentation des réseaux, entre production, développement, Wi-Fi, etc.

[5] Document est en cours de finalisation, le working draft 5 est accessible sur le site de l'ISA.

Conclusions

Les deux approches de l'ANSSI et l'ISA/CEI procèdent de la même philosophie et sont dans l'ensemble compatibles, y compris en termes de niveaux : bien qu'il y ait trois classes d'un côté et quatre niveaux de sécurité de l'autre. Si on considère les niveaux d'attaquants, la classe 1 peut correspondre aux SL 1 et 2 et les classes 2 et 3 respectivement aux SL 3 et 4.

Dans sa démarche, l'ANSSI reste cependant plus prescriptive sur le choix des solutions alors que l'ISA/CEI se limite à une approche normative de formulation d'exigences.

Les expériences pilotes en 2014 menées par certains industriels sur l'application de la classification ANSSI ont montré les limites d'une approche générale de classification. Il serait sans doute préférable que chaque secteur industriel, voire chaque opérateur, se dote d'une méthode d'affectation en classes ou SL, en cohérence avec les autres méthodes de gestion des risques industriels déjà en œuvre.

Il serait par ailleurs possible d'avoir une approche totalement cohérente, en termes de classification, entre les approches ISA/CEI et ANSSI. Concernant les exigences techniques précises, une étude plus précise est nécessaire, exigence par exigence : dans la mesure où les exigences précises pour les OIV des différents secteurs sont en cours de définition, cette comparaison pourra être effectuée une fois les arrêtés effectivement publiés. A la date de publication du présent article, on sait seulement que les exigences pourront s'écarter de celles présentes dans le document « Mesures détaillées » de 2014.

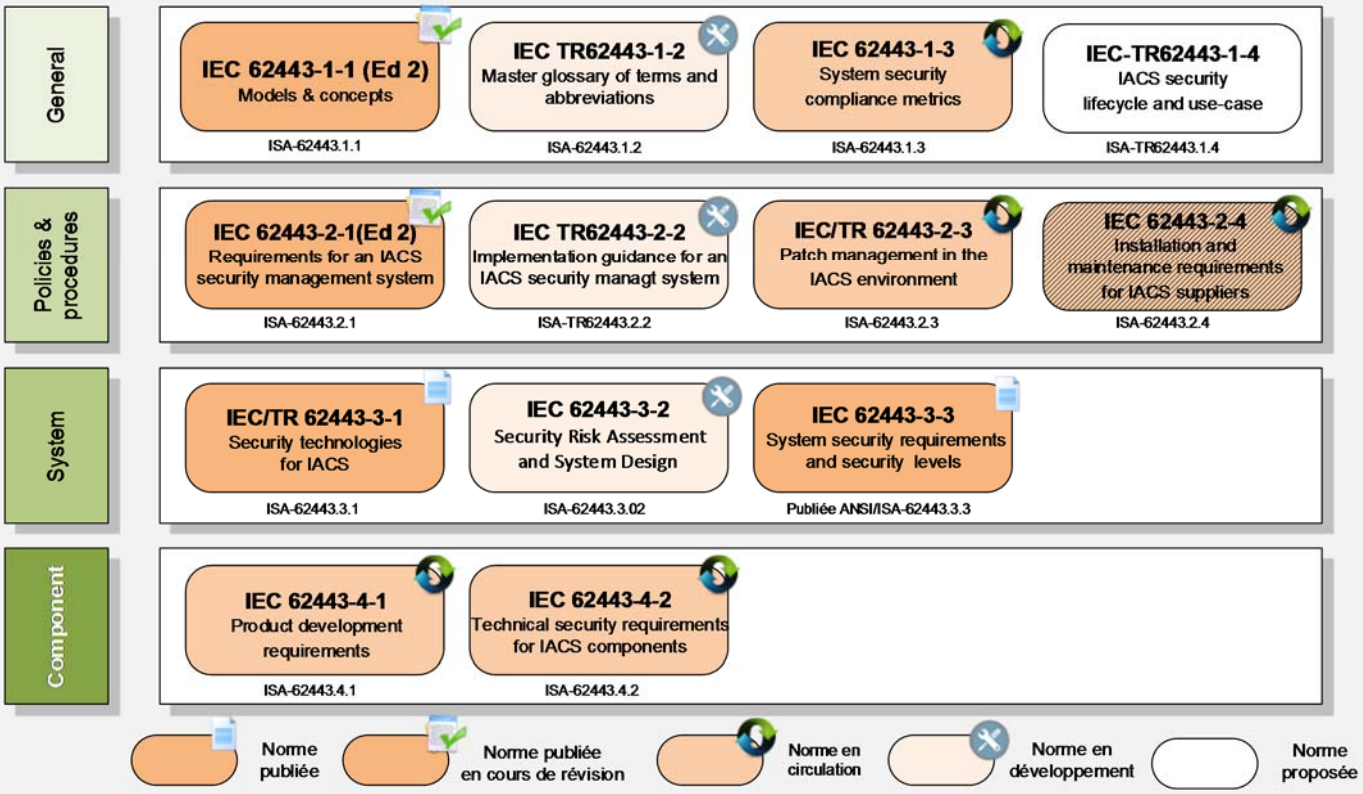

Figure 2 : Structure documentaire de la norme IEC 62443 (ex ISA99). Nota : le standard IEC 62443-2-4, marqué en hachuré, est d'origine WIB.

Les auteurs

Patrice Bock, patrice.bock@isa-France.org , **Jean Caire**, **Orion Ragozin**, avec la participation de Jean-Pierre Hauet, jean-pierre@hauet.com

Les automatismes industriels et l'Internet des objets

Christian Verney

Introduction

Le concept de l'internet des objets (Internet of Things ou IoT) entraine depuis quelque temps beaucoup d'agitation dans l'industrie informatique et dans celle des communications. Mais qu'en est-il de ces concepts dans le monde des automatismes industriels ?

Sans aucun doute, les technologies de l'information joueront un rôle plus important dans les processus de production que par le passé, afin d'augmenter la productivité, la flexibilité et la réactivité.

Les grandes entreprises industrielles veulent profiter d'une meilleure connectivité des produits pour offrir à leurs clients de nouveaux services à valeur ajoutée. De nouveaux modèles économiques tels que «Industrie 4.0 », « L'usine connectée » émergent et l'Internet des objets est ainsi une technologie clé du projet Industrie 4.0.

Qu'entend-on par l'Internet des objets?

L'Internet des objets consiste à connecter ce qui ne l'est pas. L'Internet des objets bénéficie des innovations techniques de ces dernières années et des innombrables déploiements des technologies du protocole Internet et des protocoles de sécurité associés.

Les applications d'automatismes industriels commencent à explorer l'utilisation de ces concepts afin de construire des architectures systèmes plus flexibles et plus efficaces et de parvenir à des process de production plus réactifs et à une meilleure intégration des systèmes de l'entreprise.

L'objectif principal est de faciliter, via la communication par Internet, l'interaction entre les différents équipements d'automatismes d'une unité de fabrication : capteurs, actionneurs, robots, interfaces homme/machine, y compris les smartphones, les tablettes… afin d'accroitre la productivité.

Cela implique l'identification précise de chaque équipement, une infrastructure capable de déployer en toute sécurité de nombreux dispositifs de communication et des standards ouverts pour soutenir l'innovation dans des environnements divers.

Les défis et les enjeux pour les automatismes industriels

Le véritable défit est de réussir la convergence entre les technologies de l'information et les technologies du contrôle industriel.

Pour bénéficier du concept de l'IoT, trois axes sont à considérer qui vont changer la façon dont les systèmes d'automatisation industriels sont conçus et déployés :

- des normes sont indispensables ;
- une puissance de calcul accrue est nécessaire ;
- la facette « sécurité » est prioritaire.

1er axe à considérer : des normes sont indispensables

Pour parvenir à un véritable Internet industriel des objets, il faut que les divers dispositifs et systèmes aient la possibilité de partager des informations et d'interagir. Mais actuellement la plupart des systèmes d'automatisation industrielle sont basés sur une collection de technologies et de réseaux propriétaires disparates. De tels systèmes ne peuvent pas bénéficier de l'apport de l'IoT. Ils doivent évoluer en s'appuyant sur des normes offrant interopérabilité, flexibilité et évolutivité.

De nombreuses initiatives pour créer de telles normes ont été lancées et souvent l'industriel ne sait pas quel groupe il doit rejoindre, quelle norme choisir et avec qui s'associer. Les organisations PLCopen, la Fondation OPC et l'ISA, ainsi que les organismes internationaux de normalisation (IEC/ISO) collaborent et proposent désormais un socle de normes pour relever le défi :

- La technologie OPC UA offre une solution de communication sécurisée et transparente indépendante du réseau, c'est le fondement d'une nouvelle ère de la communication pour le contrôle industriel ;
- PlCopen fournit la technologie pour rendre l'information des contrôleurs accessible d'une manière harmonisée. Cela signifie que la communication sur le site de production est grandement facilitée. PLCopen permet également la communication machine-to-machine (M2M), ainsi que la communication machine-to-cloud, afin de relier le contrôleur industriel au monde extérieur et vis et versa ;

- L'initiative B2MML (Business To Manufacturing Markup Language) permet de coupler plus étroitement le monde de la fabrication et celui de l'entreprise. B2MML est développé par un comité ad hoc au sein du WBF « The Forum for Automation and Manufacturing Professionals » rattaché à l'ISA au travers de l'Automation Federation.
- Les normes ISA/IEC proposent des solutions pour renforcer la sécurité.

OPC UA

OPC UA (OLE for Process Control Unified Architecture) s'inscrit dans le paradigme de l'Internet des objets afin de servir une gamme d'applications, y compris l'automatisation industrielle.

La conception et les spécifications d'OPC UA en font une technologie adaptée au développement d'infrastructures multifournisseurs, de multiplateformes sécurisées et à une interopérabilité fiable pour les automatismes industriels et les domaines connexes.

OPC UA est une architecture sécurisée évolutive dont la communication sécurisée et cryptée s'appuie sur :

- les normes de l'industrie informatique (IP et les services Web) ;
- les contrôles d'accès nécessaires pour lire et écrire les données et les métadonnées associées à l'objet d'automatisme de plus bas niveau ou pour échanger avec les systèmes de gestion de la fabrication et ceux de l'entreprise.

OPC-UA prône l'utilisation des services Web pour les communications systèmes et l'interaction avec tous les périphériques en réseau. Le World Wide Web Consortium (W3C), principale organisation internationale de normalisation pour le Web, définit un service Web comme « un système logiciel conçu pour soutenir l'interaction machine-to-machine sur un réseau".

Les spécifications d'OPC UA sont en libre accès et forment depuis 2011 une norme internationale (la série IEC 62541-x), c'est à dire un standard ouvert pour les communications et l'intégration des périphériques et des applications.

Les sept premières parties définissent les caractéristiques et les propriétés de base d'OPC UA. Les parties 8 à 11 appliquent ces propriétés de base aux types d'accès spécifiques tels que l'accès aux données (DA), les alarmes et les événements (A & E) et l'accès aux données de l'historique (HDA).

OPC UA est utilisé dans les centrales nucléaires, les plates-formes pétrolières, les unités de traitement des eaux, les usines automobiles (chaines de fabrication), les usines de retraitement.

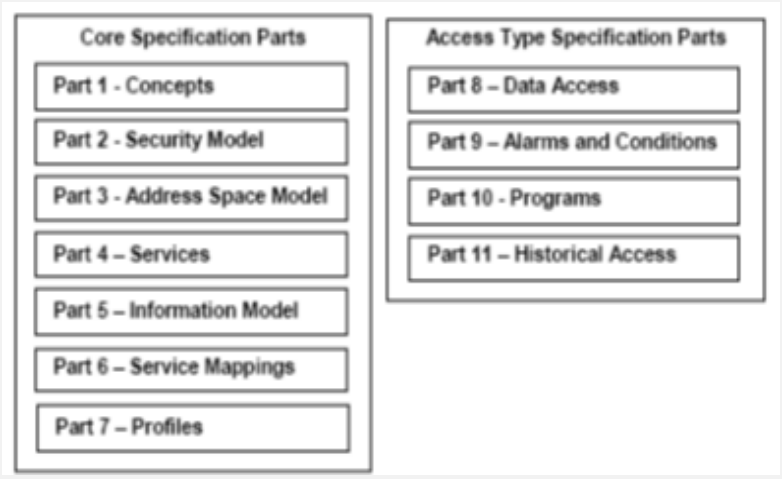

Figure 1 : OPC UA (IEC 62541-x) Multi-Part Specification.

PLCopen integrated Web services

Aujourd'hui, les nombreux protocoles propriétaires d'échange de données n'offrent pas d'interopérabilité permettant de transporter les informations entre les contrôleurs, les systèmes, les entreprises et le cloud.

PLCopen et la Fondation OPC collaborent depuis quelques années et ont contribué à la spécification de l'IEC 61131-3, PLCopen blocs fonctionnels qui intègrent OPC UA. Avec les blocs fonctionnels PLCopen OPC UA, l'industriel dispose désormais d'une solution de communication universelle, sûre et fiable qui permet à un contrôleur, à l'aide du modèle d'information du serveur OPC-UA basée sur la norme CEI 61131-3, d'échanger horizontalement des structures de données complexes avec d'autres contrôleurs, indépendamment du bus de terrain ou verticalement avec d'autres périphériques ERP/ MES et le cloud.

Les nouveaux blocs fonctionnels permettent aux programmeurs d'automates (PLC) et aux utilisateurs de contrôleurs certifiés PLCopen d'exposer les informations avec une sémantique normalisée pour échanger de manière transparente des données entre le contrôleur d'acquisition de données, les systèmes d'exécution de fabrication (MES), l'Enterprise Resource Planning (ERP) et les divers automates programmables.

Business To Manufacturing Markup Language (B2MML)

La nécessité de coupler efficacement la production avec la chaine logistique est un élément essentiel pour améliorer la dynamique industrielle.

B2MML (Business To Manufacturing Markup Language) est un vocabulaire XML permettant de décrire l'information échangée entre les systèmes de gestion, tels que l'ERP (Enterprise Resource Planning) ou le SCM (Supply Chain Management), les systèmes de PLM (Product Lifecycle Management) de gestion des actifs et de la maintenance, avec les systèmes industriels, tels que les DCS (Digital Control Systems), les SCADA (Supervisory Control And Data Acquisition) ou le MES (Manufacturing Execution Systems).

B2MML est une implémentation XML des modèles de données des normes ISA88/IEC 61512 et ISA95/IEC/ISO 62264 pour le développement des interfaces de communication qui consiste en une série de schémas XML conformes au langage XML Schema (XSD) du W3C (World Wide Web Consortium).

- L'ISA88/ISO/IEC 61512 « Contrôle-commande des processus de fabrication par lots » est une norme internationale relative au contrôle batch qui définit les modèles et la terminologie s'appliquant à l'exploitation des installations de fabrication par lots et qui spécifie les structures de données et les règles générales relatives aux langages.
  Cette norme fournit plus spécifiquement une terminologie normative ainsi qu'un ensemble cohérent de concepts et de modèles relatifs au contrôle commande de processus de fabrication par lots, qui permettent d'améliorer la communication entre les parties concernées.
- L'ISA95/ISO/IEC 62264 est la norme internationale pour l'intégration des systèmes d'entreprise et de contrôle ; visant à assurer l'interopérabilité de la production avec la planification, en clair, la connexion des systèmes de contrôle avec les ERP. C'est un modèle fonctionnel constituant un guide précieux pour la cartographie et la définition des besoins fonctionnels dans les projets « MES ». Au-delà des aspects spécifiques de la communication et de la définition fonctionnelle de la gestion de production, la norme ISA95 complète la norme ISA88 pour offrir un ensemble de modèles de description spatio-temporel du système de production particulièrement pertinents pour développer une approche d' architecture de production capable de soutenir les efforts d'évolution permanente de l'entreprise.

Alors que les normes définissent des modèles structurels ne proposent pas de taxonomie rigoureuse ni des types de données suffisants pour la communication humaine, B2MML vise à définir des structures de données totalement typées et rigoureusement nommées comme base de construction de messages intelligibles par des machines.

2ème axe à considérer : une puissance de calcul accrue est nécessaire

Une architecture d'automatisme plus distribuée

De nombreux dispositifs de radiocommunications sont déjà utilisés dans l'industrie. Les capteurs basés sur les standards ISA100-11a, WirelessHART ou WIA-PA sont des dispositifs IP compatibles avec l'IPv6 qui offrent des méthodes d'adressage et de routage appropriées. L'emploi d'IP dans les architectures d'automatismes de fabrication permet de distribuer davantage de fonctions dans les nouvelles générations de contrôleurs industriels surpuissants. Les capteurs/actionneurs dotés de processeurs intégrés prennent en charge les commandes locales, optimisent l'exploitation des données et produisent des analyses et des diagnostics.

L'architecture de ces nouvelles installations est différente de celle des systèmes fermés du passé, cette révolution transférant l'intelligence à la périphérie du système. Ces nouvelles capacités éliminent le besoin de logiciel de niveau intermédiaire lourd, coûteux et difficile à maintenir.

Des volumes de données à traiter

Cette approche IoT génère de grandes quantités de données qui changent la façon dont les industriels planifient leurs opérations et gèrent le processus de fabrication. La prochaine étape de l'optimisation des processus sera atteinte en tirant parti de la collection de mesures actuellement inutilisées par des dispositifs de détection largement distribués avec de meilleures capacités analytiques.

Les entreprises manufacturières doivent envisager une stratégie d'hébergement en cloud (privé/public/hybride) pour traiter la quantité de données à partir du nombre exponentiel de dispositifs IoT qui se connecteront sur le réseau. Les systèmes logiciels de l'entreprise (ERP/MES de contrôle/supervision et d'acquisition de données [SCADA]) devront être mis à niveau avec des algorithmes d'auto-apprentissage pour analyser ces données, déterminer les tendances et prendre les décisions nécessaires pour augmenter l'efficacité.

3ème axe à considérer : la facette « sécurité » est prioritaire

L'utilisation d'Internet en tant que plate-forme de communication commune permettra aux entreprises de connecter plusieurs systèmes, des machines, des capteurs et des dispositifs de contrôle pour servir efficacement les nouvelles stratégies commerciales.

Mais en s'écartant des systèmes d'automatisation cloisonnés, il devient nécessaire d'intégrer les approches sécurité des technologies de d'information. Cet impératif va transformer la façon dont les systèmes d'automatisation sont conçus et déployées. Il est indispensable d'améliorer la sécurité de l'accès au réseau de l'usine sans toutefois dégrader les performances temporelles ni complexifier les procédures de fabrication.

ISA 99/IEC 62443

Par le passé, un certain nombre d'entités ont travaillé de manière séparée pour élaborer des normes de cybersécurité. Ces groupes se sont réunis pour créer une norme commune qui simplifie grandement la mise en œuvre et les contrôles de conformité. L'organisation américaine du NIST participe à cet effort et son rôle a été renforcé le 12 Février 2013 par la publication du décret présidentiel intitulé «Amélioration de la cybersécurité des infrastructures critiques ».
Il y a dix ans l'ISA a lancé le projet ISA99 « Automatisation industrielle et sécurité des systèmes de contrôle » afin de développer une gamme complète de normes de cybersécurité pour l'industrie de l'automatisation. Le résultat des travaux, qui sont en voie d'achèvement, a été soumis pour normalisation à l'IEC sous la référence IEC 62443-x dont la structure est présentée dans la figure 2 de l'article qui précède.

En parallèle mais de façon indépendante de l'élaboration de la norme, des méthodes de certification du niveau de sécurité ont été développées:

- Les certifications ISA Secure (EDSA, SSA et SDLA) qui traitent des produits, systèmes et processus de développement ;
- La certification Achille de Wurldtech (a GE Company) qui traite des communications.

Ces procédures s'appuient sur la série IEC 62443 (ISA99).

En résumé, Il y a aujourd'hui convergence de l'industrie autour de la norme IEC 62443. Cette norme fournit un ensemble très complet de règles pour la cybersécurité industrielle avec des normes pour les organisations, les systèmes, les composants et l'intégration et la maintenance. Les programmes de certification existants demeurent, mais feront désormais référence aux normes IEC 62443 plutôt qu'à des spécifications propriétaires.

Conclusion

Le transfert du concept d'Internet des objets dans le monde des automatismes industriels sera plus délicat et plus long que celui observé pour le milieu de l'informatique et de la communication. Le marché industriel est un segment complexe pour ce nouvel écosystème. Les cas d'utilisation et les types d'équipements sont variés et nombreux, le niveau de connectivité et d'interopérabilité des données des équipements est faible, les normes et les bonnes pratiques sont digérées lentement et les contraintes temps réel demeurent un énorme défi. Mais la transformation du secteur industriel a commencé, des objets connectés de production sont développés et de nombreux leaders d'opinion prévoient une croissance spectaculaire du nombre des équipements industriels connectés (figure 3).

Le rapport de IHS Technology prévoit une croissance annuelle de 30 % des objets industriels connectés jusqu'en 2025. La figure 3 illustre l'importance du concept d'internet des objets et explique pourquoi de grands fabricants et de nombreux opérateurs industriels ont décidé d'utiliser la technologie IP.

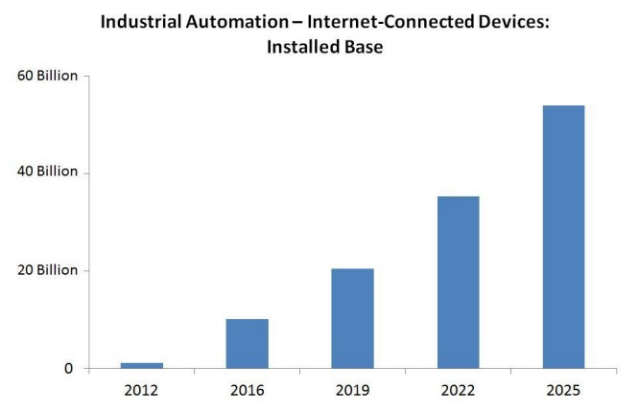

Figure 3 : Prévision d'évolution de la base installée de l'Internet industriel des objets – Source : IHS Technology.

Christian Verney - cv@cverney.com

ISA secure: http://www.isasecure.org/
OPC Foundation: https://opcfoundation.org/
PLC Open: http://www.plcopen.org/
W3C (World Wide Web Consortium): http://www.w3.org/
IHS technology: https://technology.ihs.com/

Code	Désignation	Calendrier 2015	
		Lieu	Date
JPH1	**L'IEC 62734 (ISA-100) et les applications nouvelles des radiocommunications dans l'industrie - Deux jours**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	17 et 18 juin 2015 14 et 15 octobre 2015 16 et 17 décembre 2015
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	Sur demande
JPH3	**La norme ISA/IEC 62443 (ISA-99) et la cyber-sécurité des systèmes de contrôle - Un jour**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	19 juin 2015 16 octobre 2015 18 décembre 2015
JVI1	**ISA-88 : Conception fonctionnelle automatismes et contrôle des procédés industriels - Deux jours**	**Fontainebleau**	8 et 9 juin 2015 5 et 6 octobre 2015 7 et 8 décembre 2015
JVI2	**ISA-95 : Conception fonctionnelle et interopérabilité MES/MOM - Deux jours**	**Fontainebleau**	10 et 11 juin 2015 7 et 8 octobre 2015 9 et 10 décembre 2015
PNO1	**ISA-18.2 - Gestion d'alarmes : un outil efficace au service de l'opérateur - Un jour**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	16 juin 2015 13 octobre 2015 15 décembre 2015
BRI1	**ISA-84 - Sûreté de fonctionnement avec les normes IEC 61508 et IEC 61511- Deux jours**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	1er et 2 juin 2015 28 et 29septembre 2015 30 novembre et 1er décembre 2015
BRI2	**Modélisations et calculs de fiabilité pour IEC 61508/IEC 61511/S84**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	3 juin 2015 30 septembre 2015 2 décembre 2015
BRI3	**Développement d'applications de sécurité IEC 61508 / IEC 61511 / ISA-84**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	25 au 28 mai 2015 21 au 24 septembre 2015 23 au 26 novembre 2015

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 09
- 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 GO au format Word GO