ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°63 – Août 2017 Bulletin d'information d'ISA-France

Au sommaire de ce numéro :

29 juin 2017 : Assemblée générale de l'ISA-France

Le 29 juin 2017 s'est tenue à paris l'assemblée générale de l'ISA-France. Le rapport d'activité et les comptes de l'énnée 2016 ont été approuvés à l'unanimité. Jean-Pierre Hauet a été reconduit dans ses fonctions de président de l'association ainsi que Bernard Dumortier, secrétaire et vice-président, Patrice Noury, trésorier et vice-président, et Jean Vieille, vice-président.

La cyberattaque contre les réseaux ukrainiens : l'analyse d'ISA-France diffusée dans le monde entier

Dans le numéro 62 de l'ISA-Flash, nous avons publié le résumé de l'étude effectuée par Patrice Bock, avec la participation de Jean-Pierre Hauet, sur la cyberattaque menée contre les réseaux de l'Ouest ukrainien en décembre 2015 et renouvelée en décembre 2016.. Cette étude a été publiée dans la revue Intech de l'ISA et reprise dans le monde entier y compris en Ukraine. Cette analyse permet de mettre en évidence les faiblesses du système qui ont rendu possible cette attaque Elle montre que le respect d'un niveau de sécurité **SL2** selon le standard **IEC 62443** aurait très probablement permis de l'éviter. L'article démontre le caractère opérationnel du standard ISA/IEC 62443-3-3 pour évaluer la cybersécurité d'un système de contrôle et définir les mesures de protection à mettre en oeuvre pour atteindre un niveau de sécurité donné.

L'article peut être téléchargé gratuitement ICI

ISA-France présente à la journée EXERA du 28 septembre 2017

Notre partenaire **EXERA** organise à Paris le 28 septembre prochain, à Paris (gare de l'Est) une journée technique consacrée à « **la cybersécurité des systèmes industriels** ».
ISA-France y participera sous forme de deux présentations :

- l'une de Jean-Pierre Hauet sera consacrée à « **la norme IEC 62443 et les évolutions à prévoir pour répondre aux besoins nouveaux (IIoT notamment**) »
- l'autre de Patrice Bock sur « **les retours d'expérience et la surveillance des réseaux industriels critiques** »

Le programme et le bulletin d'inscription peuvent être téléchargés ICI

Ugo Baggi (Italie) élu Vice President Elect du District 12

Lors de la conférence annuelle du District 12, organisée par la section Italie les 7 et 8 juillet 2017, à Milan, **Ugo Baggi**, président de la section Italie, a été élu Vice President Elect du District 12. Il succèdera à David O'Brien (Irlande) à compter du 1er janvier 2019. Nous lui adressons toutes nos félicitations et nos vœux de réussite.
Cette DLC faisait suite à la 4e conférence sur l'automation, placée sous l'égide du District 12, et organisée cette année au Castello Di Belgioioso par la section italienne. Cet « **Automation Instrumentation Summit »** a connu un très grand succès et s'inscrivait dans le cadre d'une Technology Week du 3 au 9 juillet 2017 s'achevant par la DLC du District 12.
Le lecteur pourra visionner une excellente **vidéo** mis en ligne par les organisateurs.

Ugo Baggi lors de l'Automation Instrumentation Summit

28 au 31 octobre 2017 : 2017 ISA Fall Leaders Meeting à Tampa (Floride)

La grande conférence annuelle de l'ISA se tiendra cette année du 28 au 31 octobre à Tampa (floride). Rappleons que cette conférence est l'occasion pour tous les membres de l'ISA intéressés de rencontrer leurs homologues venant des 129 sections réparties dans le monde qui consituent aujourd'hui l'ISA.
Une occasion unique de nouer des contacts et de se tenir au courant de l'actualité dans le monde de l'automation.
Tous les détails sont sur le site de **l'ISA**.

Sommaire | Evénements | Standards | Technologie | Formation

Le point sur la normalisation de la gestion des alarmes (ISA18.2)

A la suite de la publication en 2009 d'une première version de la norme **ISA 18.2,** le comité technique a travaillé sur l'édition de rapports techniques afin de faciliter sa mise en œuvre. Sept rapports techniques avaient été mis en chantier. Trois ont été publiés en 2012 :

- ISA TR 18.2.4-2012 Enhanced and Advanced Alarm Methods
- ISA TR 18.2.5-2012 Alarm System Monitoring Assessment and Auditing
- ISA TR 18.2.6-2012 Alarm Systems for Batch and Discrete Processes

Un autre a été publié en 2015, un cinquième en 2016 et un sixième en 2017 :

- ISA TR 18.2.3-2015 Basic Alarm Design
- ISA TR18.2.2-2016 Alarm identification and Rationalization
- ISA TR 18.2.7-2017 Alarm management when Utilizing Packaged Systems

Ces textes sont disponibles sur le site de l'ISA

Il reste donc encore un rapport technique à terminer, il devrait être publié cette année :

- ISA TR 18.2.1-2017 Alarm Philosophy

En parallèle avec le travail sur ces rapports techniques le comité a travaillé sur une nouvelle édition de la norme de façon à être homogène avec la norme internationale IEC. Cette nouvelle version a été publiée en 2016 :

- ANSI/ISA 18.2-2016 Management for Alarm Systems for the Process Industries

Les évolutions de la norme avaient pour objectif de prendre en compte le retour d'expérience depuis la première publication de 2009 et d'harmoniser le vocabulaire et les concepts avec la norme IEC 62682. La nouvelle version offre une meilleure définition des termes et renforce les exigences de fonctionnalités afin d'être conforme à la norme IEC.

Cependant cette mise à niveau pose un problème pour les rapports techniques. Les définitions des différents documents ne sont pas homogènes, certains se réfèrent encore aux définitions de l'ancienne norme et quelques fois proposent leurs propres définitions. Seuls les deux derniers rapports sont homogènes avec la nouvelle version. Pour les autres rapports techniques, le travail reste à faire.

La publication du rapport technique TR 18.2.1 Alarm Philosophy sera importante. Ce rapport clarifiera comment mettre en œuvre la gestion des alarmes d'un procédé industriel afin d'éviter les interprétations particulières de la norme qui doit rester générique.
Il est maintenant possible de mettre en œuvre et d'exploiter un système d'alarmes performant et efficace à l'aide de la norme ISA 18.2-2016.
Patrice Noury

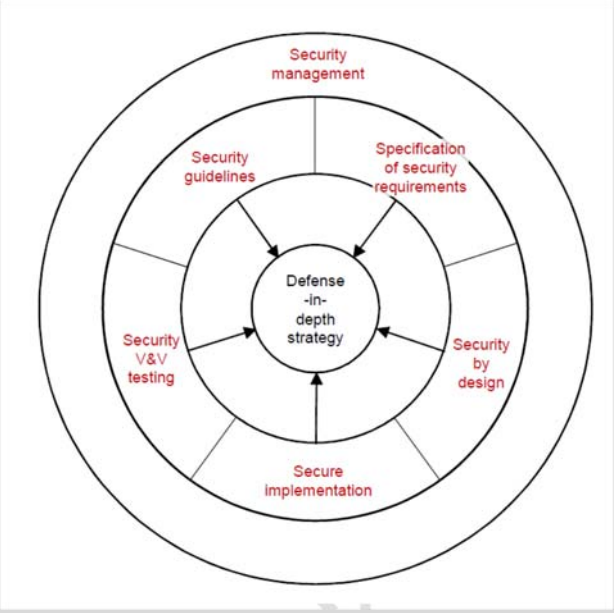
Cybersécurité : le standard ISA/IEC 62443-4-1 prochainement approuvé par l'ISA

Un nouvelle étape importante vient d'être franchie dans la complétion de la norme ISA/IEC 62433 relative à la cybersécurité des systèmes de contrôle industriel.

En effet, le texte fnal du standard ISA/IEC 62443-4-1 « **Product security development life-cycle requirements** » a été mis en circulation en juillet 2017 au sein du Comité ISA99 pour approbation définitive. Le texte diffusé est le texte parvenu à l'état de FDIS (Final Draft International Standard) au sein de l'IEC et n'appelle plus d'observations techniques. Sa ratification par l'ISA99 devrait intervenir d'ici la fin août.

Ce texte est important : il définit les exigences à satisfaire tout au long du cycle de vie des **produits** destinés aux systèmes d'automatisme et de contrôle indusriel (IACS) : développement, maintenance et fin de vie des produits matériels ou logiciels, nouveaux ou existants. Ces exigences s'appliquent aux entités en charge du développement et de la maintenance des produits mais pas aux intégrateurs ni aux exploitants qui relèvent d'autres standards (notamment IEC 62443 2-4).

Le document listent 47 exigences qui sont regroupés en huit chapitres, illustrés par la figure 1, qui permettent de s'assurer, au niveau du cycle de vie, de l'aptitude d'un produit à participer à une politique de défense en profondeur.



Ces huit pratiques comprennent en premier lieu, Les exigences relatives au management de la sécurité qui s'appliquent à l'ensemble des pratiques sécuritaires.
On trouve ensuite des pratiques spécifiques aux différentes étapes du cycle de vie :

- la spécification des exigences de sécurité, telles que les capacités d'authentification, de chiffrement, d'audit, auxquelles doit satisfaire le produit ;
- la conception du produit et de toutes ses interfaces ;
- les pratiques d'Implémentation (y compris règles de codage et outils d'analyse de code) ;
- les pratiques de vérification et de validation (notamment face aux menaces identifiées) ;
- le management des problèmes de sécurité lorsqu'ils surviennent ;
- la gestion des mises à jour (gestion des patches…) ;
- la gestion de la documentation et la façon de mettre en œuvre le produit compte tenu du contexte (Security guidelines).

Figure 1 : Les exigences listés dans la norme IEC 62443-4-1 visent à intégrer dans le cycle de vie d'un produit l'objectif de défense en profondeur

La norme IEC 62443-3-3 donne lieu à **certification** aux Etats-Unis par l'ISA Security Compliance Institute et en Europe par l'EXIDA selon la méthode SDLA (Secure Development Life-cycle Assessment). Des centres de développement de Schneider-Electric et d'Honeywell sont dès à présent certifiés. Les TUV allemands ont également mis en place des certifications IEC 62443-4-1.
Jean-Pierre Hauet

Utiliser OPC UA…

Utiliser OPC UA (OLE for Process Control Unified Architecture) pour répondre aux exigences de sécurité des sites industriels

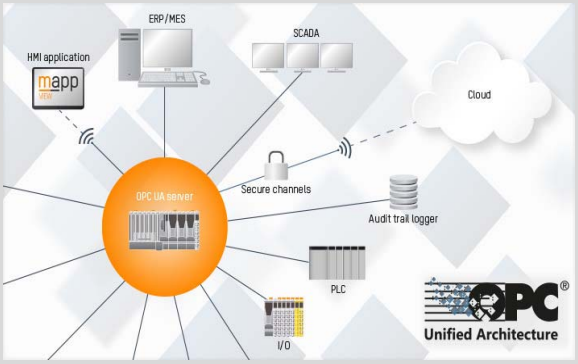
par Christian Verney

ISA-France Technology leader

Retour sur OPC UA

Les systèmes de contrôle industriel exploitent la dernière architecture unifiée OPC (UA), qui offre une interopérabilité inter-plateformes entre les logiciels applications et les équipements. La criticité des systèmes de contrôle industriels (SCI) et la volonté de rendre les informations process et commerciales disponibles à tous, n'importe où, et à tout moment, imposent pour les sites industriels des règles de sécurité pour protéger les informations échangées entre les parties intéressées.

Les normes OPC UA sont conçues pour répondre à ces exigences de sécurité tout en maintenant le niveau de flexibilité et de contrôle que les administrateurs des sites industriels réclament.



Le standard OPC est apparu au milieu des années 90 pour faciliter les échanges entre le monde des automatismes et celui de la supervision basée sur PC.

OPC Unified Architecture (OPC UA) est un protocole de communication, indépendant des constructeurs, dédié aux applications d'automatisation industrielle. Il est basé sur le principe client-serveur et permet une communication transparente, des capteurs-actionneurs aux systèmes ERP ou au nuage. OPC UA permet les échanges de données en temps réel, l'émission d'alarmes, de statuts et des historiques, et beaucoup d'autres types de données.

Le protocole est indépendant de la plate-forme et intègre de base des mécanismes de sécurité. Flexible et complètement indépendant, OPC UA est considéré comme le protocole de communication idéal pour la mise en œuvre de l'Industrie 4.0. OPC UA établit un pont entre le monde de l'IT et celui de la production.

OPC UA est un protocole de communication universel et sécurisé, particulièrement adapté à la communication entre machines. Il peut être appliqué à n'importe quel support physique (câble, liaison sans fil ou autres), à tout type de système d'exploitation et il peut être aussi bien installé sur une machine à forte capacité de calcul que sur de modestes objets connectés.

OPC UA est un ensemble de spécifications qui composent désormais la norme internationale IEC 62541 développée par le TC 65 (Industrial-process measurement, control and automation) de la CEI.

- IEC 62541-1, OPC unified architecture – Part 2: Overview and concepts
- IEC 62541-2, OPC unified architecture – Part 2: Security model

- IEC 62541-3, OPC unified architecture – Part 3: Address space model
- IEC 62541-4, OPC unified architecture – Part 4: Services
- IEC 62541-5, OPC unified architecture – Part 5: Information model
- IEC 62541-6, OPC unified architecture – Part 6: Mappings
- IEC 62541-7, OPC unified architecture – Part 7: Profiles
- IEC 62541-8, OPC unified architecture – Part 8: Data Access
- IEC 62541-9, OPC unified architecture – Part 9: Alarms and condtions
- IEC 62541-10, OPC unified architecture – Part 10: Programs
- IEC 62541-11, OPC unified architecture – Part 11: Historical access
- IEC 62541-12, OPC unified architecture – Part 12: Discovery
- IEC 62541-13, OPC unified architecture – Part 13: Aggregates

Sécurité, principes essentiels et menaces majeures

Les principes essentiels de la sécurité sont rappelés brièvement ci après :

- **les audits** : ils permettent la traçabilité de toutes les actions systèmes dans le but d'identifier qui a effectué l'action, quand et à quelles fins et de connaitre toutes les tentatives qui ont été faites pour compromettre le système ;
- **l'authentification** : un système de contrôle industriel (SCI) se compose d'équipements, d'applications logicielles et d'exploitants. Chaque composante doit décliner son identité pour être considéré comme un élément de confiance ;
- **l'autorisation** : même si une partie est reconnue fiable, elle ne doit disposer que des autorisations minimales nécessaires pour exercer sa fonction. C'est-à-dire la capacité de lire, d'écrire et/ou d'exécuter des actions pour réaliser une tâche ;
- **la disponibilité** : elle garantit que le SCI est pleinement opérationnel en limitant les facteurs qui peuvent avoir une incidence sur son exécution
- **la confidentialité** : les informations échangées doivent être visibles et partagées seulement par les parties de confiance. Cela impose de la part de l'expéditeur le chiffrement des informations et pour le destinataire la faculté de déchiffrer les données reçues selon un algorithme convenu ;
- **l'intégrité** : les informations échangées entre les parties de confiance ne doivent pas pouvoir être modifiées. Les informations reçues doivent être celles qui ont été initialement envoyées.

Pour atteindre ces objectifs, il est impératif d'identifier les principales menaces qui pourraient compromettre la sécurité. De nombreuses menaces sont potentielles et, parmi les plus courantes, voici celles qui ont frappé les SCI ces dernières années :

- **la violation des droits utilisateurs** : elle se produit lorsqu'un attaquant usurpe l'identité d'un utilisateur en obtenant par des moyens électroniques ou physique son nom d'utilisateur, son mot de passe ou d'autres droits ;
- **les écoutes indiscrètes, l'espionnage** *(eavesdropping)* : une partie non autorisée intercepte des informations pour un bénéfice personnel ou pour préparer de futures attaques ;
- **les messages malveillants** *(malformed messages)* : en recevant des messages dont il ne perçoit pas le caractère malveillant, le récepteur effectue des traitements inappropriés qui peuvent nuire au bon fonctionnement du SCI ;
- **l'altération de messages** et **l'usurpation** *(spoofing)* : un attaquant, sous l'identité d'une partie autorisée, manipule ou créait un message entre les applications et les périphériques dans le but nuire ;

- **la saturation de requêtes** *(message flooding)* : un attaquant cible une application ou un périphérique en déclenchant de fréquentes communications avec de grandes quantités de données, dans le but de mettre le récepteur hors ligne et d'impacter sa disponibilité ;
- **le renvoi de message** *(message replay)* : en capturant des messages authentifiés et en les utilisant, un attaquant peut exécuter des opérations à des moments inappropriés. Ces messages peuvent tromper les utilisateurs du système en faisant croire que tout fonctionne normalement, alors que l'état du système est défaillant ;
- **le profilage** *(profiling)* : un attaquant utilise ses connaissances sur les vulnérabilités concernant la sécurité d'une version particulière d'une application ou d'un dispositif. Ces vulnérabilités peuvent avoir été communiquées par le fournisseur dans le but de sensibiliser le public aux lacunes antérieures et aux efforts faits pour les corriger ;
- **le vol ou détournement de session** *(session hijacking)* : quand un attaquant est capable d'interférer dans les applications et/ou les périphériques en cours d'exécution et d'exécuter la session d'une partie autorisée.

En mettant en œuvre une stratégie de sécurité pour un site, un administrateur peut contrecarrer ces menaces et atteindre les objectifs de sécurité nécessaire à la protection des infrastructures :

- la plupart des sites possède un système qui gère la sécurité et répond aux exigences en matière de protection. Cela passe par l'adoption d'une politique de sécurité pour la protection des bâtiments et des ressources électroniques, la mise en place d'audits et de procédures de vérification, de prévention et d'intervention ;
- afin de répondre aux menaces identifiées, une évaluation des risques pour la sécurité est faite et des mesures de sécurité appropriées sont définies pour mettre en œuvre une stratégie de défense efficace basées sur plusieurs niveaux de protection ;
- une telle démarche est nécessaire car il n'existe pas de solution universelle pour se protéger contre toutes les menaces ; de nombreuses mesures spécifiques doivent être déployées pour protéger en profondeur le site. C'est une association de pare-feu, de systèmes de détection/prévention des intrusions, une gestion des mises à jour systèmes ainsi que la définition des règles informatiques précisant notamment pour le système, ce qui est permis et ce qui ne l'est pas.

La sécurité, une exigence principale lors du développement d'OPC UA

Les règles majeures

- **L'authentification et l'attribution d'autorisations aux utilisateurs** : pour établir une connexion, l'utilisateur s'identifie par des certificats X.509, un nom d'utilisateur et un mot de passe. Tous les systèmes d'administration d'utilisateurs sont supportés. De plus, les droits d'accès (par exemple l'accès aux données en lecture et en écriture) peuvent être spécifiés pour chaque utilisateur ;
- **L'intégrité** : la signature de messages empêche un tiers d'en modifier le contenu ;
- **La confidentialité** : la confidentialité des informations échangées est assurée par le chiffrement des messages. On utilise pour cela des algorithmes modernes et reconnus sûrs. Différents niveaux de sécurité peuvent être sélectionnés selon les exigences de l'application concernée. Pour certaines applications, il suffit de signer les messages afin de prévenir les changements apportés par des tiers tandis que le chiffrement des messages est nécessaire dans d'autres cas pour ne pas autoriser la lecture ou la modification de l'application.

- **Authentification et autorisation des applications** : les applications OPC UA s'identifient elles-mêmes (d'une manière similaire à un utilisateur) via des «software and application instance certificates ». Avec l'aide de ces certificats logiciels, il est possible d'accorder, à certaines applications client, un accès étendu à l'information sur un serveur OPC UA, par exemple pour l'ingénierie du serveur.

L'architecture de sécurité OPC UA

Grâce à son modèle de sécurité flexible, OPC UA peut s'adapter aux contraintes de sécurité du site et permettre à l'administrateur de contrôler complètement la configuration et la gestion des communications.

L'architecture client/serveur d'OPC UA propose également une stratégie de défense élaborée, car les applications OPC UA offrent une interface qui limite la quantité des informations exposée ou manipulée entre les différents niveaux de communication d'un site.

Pour lutter contre les menaces à la sécurité, OPC UA offre une architecture conçue sur trois niveaux : une couche d'application, une couche de communication et une couche de transport.

- La plupart des fonctionnalités OPC UA sont traitées dans le contexte de la couche d'application. C'est là que les processus information des clients et des serveurs, comme la lecture, l'écriture et la navigation sont exécutés. C'est également à ce niveau qu'OPC UA propose les processus d'authentification et d'autorisation des utilisateurs basés sur le concept de session entre un client et les instances de serveur.
- Chaque session échange des informations sur un canal sécurisé géré par la couche de communication. Le canal sécurisé qui constitue la couche de communication offre des fonctionnalités permettant l'authentification des applications, la confidentialité et l'intégrité des données échangées. Un niveau approprié de chiffrement et se déchiffrement est proposé afin de préserver la confidentialité des messages transmis, les messages sont signés pour assurer l'intégrité des données cependant que des certificats numériques permettent une authentification des applications.
- Les données sécurisées qui en résultent sont ensuite transmises à la couche de transport pour un traitement ultérieur. La couche de transport gère l'envoi et la réception des données de l'infrastructure de communication. Le mécanisme de transport utilisé (OPC UA Binary ou XML via HTTP) impacte la mise en œuvre du canal sécurisé géré par la couche de communication.

Comment cela fonctionne

Chaque application OPC UA possède un certificat numérique unique (X.509) appelée certificat d'instance application, attribué lors de l'installation. Ce certificat est créé par l'application au moment de l'installation, mais peut être remplacé par l'administrateur du site par un certificat jugé plus approprié.

Ce certificat est composé d'une clé publique qui peut être partagée avec les autres parties de confiance, ainsi qu'une clé privée connue seulement par l'instance application. Ces clefs ont une taille variable, plus la clef est complexe et plus il est difficile pour un tiers de la déchiffrer.

Lorsqu'une application client se connecte à un serveur, un canal sécurisé est créé. Ce processus nécessite que le client et le serveur échangent des clés publiques pour les communications. Le canal sécurisé sera établi uniquement si l'administrateur a configuré le client et le serveur pour faire confiance aux certificats de chacun.

Ceci permet l'authentification de l'application. Afin de fournir l'identité de l'utilisateur d'une application, le client crée une session qui exploite le canal sécurisé pour les communications. Les applications peuvent utiliser ces informations utilisateur pour limiter ou restreindre l'accès à certaines opérations, fournissant ainsi le niveau d'autorisation approprié à l'utilisateur.

À partir de cet instant, le client chiffre toutes les informations qu'il envoie au serveur avec la clé publique du serveur, et signe chaque message avec sa propre clé privée. Lors de la réception d'un message, le serveur testera l'intégrité du message en validant la signature au regard de la clé publique du client et déchiffre le message avec sa propre clé privée. Cela garantit que tous les messages sont restés confidentiels et n'ont pas corrompus.

OPC UA : une arme pour lutter contre les menaces sécuritaires

- Par l'utilisation des clés publiques/privées et du chiffrement pour assurer l'authentification, la confidentialité et l'intégrité des communications, OPC UA protège contre les écoutes, la falsification ou la modification des messages, le vol de session, et la détection électronique des informations d'identification utilisateur. Pour certaines autres menaces, des contre-mesures supplémentaires sont nécessaires et sont gérées par la conception, les spécifications et les recommandations d'OPC UA.
- OPC UA limite les actions qu'un client à la possibilité d'effectuer sur un serveur avant qu'il ne soit authentifié. Ces actions se limitent à l'obtention des règles de sécurité du serveur et à la création d'un canal sécurisé. Pour ce qui concerne la sécurité des connexions, ces informations changent rarement après le déploiement et occasionne peu de temps de traitement sur le serveur.
- Si trop de demandes de création de canaux sécurisés échouent, le serveur différe intentionnellement le traitement des futures demandes afin de minimiser l'impact d'une attaque potentielle.
- Les serveurs doivent également permettre aux administrateurs de limiter le nombre de connexions qu'ils gèrent à un moment donné, afin de lutter contre la saturation délibérée du serveur (message flooding) ;
- OPC UA permet de limiter les actions qu'une partie non authentifiée peut accomplir ce qui minimise le profilage du serveur par un attaquant ;
- Chaque message échangé contient un ID pour la session, un ID pour le canal sécurisé, un ID pour la demande, l'horodatage et les numéros de séquence. Comme ces messages ne sont pas modifiables, les applications peuvent valider ces valeurs pour s'assurer qu'un attaquant n'a pas intercepté un message qu'il utilisera à l'avenir. Les clients et les serveurs valident également chaque message pour s'assurer qu'il est de la forme appropriée. Cela élimine les préoccupations entourant la rediffusion des messages et les messages malveillants.

En résumé

OPC UA fournit à l'industrie une interopérabilité entre les applications logicielles et les matériels de divers fournisseurs. Cette interopérabilité permet l'échange d'informations essentielles pour tout système de contrôle industriel, ainsi que pour l'ensemble de l'entreprise.

Dans le but de favoriser la prise de décisions opérationnelles et commerciales, la capacité d'obtenir des informations de n'importe où dans le monde est essentiel. Étant donné que cela demande la transmission des données sur des domaines publics, il faut le faire en toute sécurité pour protéger l'authenticité, l'intégrité et la confidentialité de l'information. L'utilisation des principes OPC UA et des techniques informatiques aujourd'hui largement répandues permettent de répondre à ce défi.

Code	Actions de formation	Calendrier de fin d'année 2017	
		Lieu	Date
JPH1	Les solutions nouvelles de radiocommunication dans l'industrie - L'IEC 62734 (ISA-100) - Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	3 et 4 octobre 2017 20 et 21 novembre 2017
JPH3	La norme ISA/IEC 62443 (ISA-99) et la cybersécurité des systèmes de contrôle - Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	5 et 6 octobre 2017 18 et 19 décembre 2017
JPH4	L'Internet industriel des objets - Les futures architectures de systèmes d'automatisme et de contrôle – Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	9 et 10 octobre 2017 22 et 23 novembre 2017
JVI1	ISA-88 : Conception fonctionnelle des automatismes des systèmes cyber-physiques de l'Industrie 4.0- Un jour	**Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY**	11 septembre 2017 13 novembre 2017
JVI2	ISA-95 : Conception fonctionnelle et interopérabilité MES/MOM - un jour	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	12 septembre 2017 14 novembre 2017
JVI4	B2MML : Spécification des Interfaces XML entre applications informatiques Industrielles - Un jour	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	13 septembre 2017 15 novembre 2017
JVI6	Intelligence et performance des systèmes Industriels - Un jour	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	13 septembre 2017 15 novembre 2017
JVI7	Transformation digitale des systèmes industriels - Un jour	**Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY**	15 septembre 2017 17 novembre 2017
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	18 septembre 2017 20 novembre 2017
BRI1	ISA-84 - Sûreté de fonctionnement avec les normes IEC 61508 et IEC 61511- Deux jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	19 et 20 septembre 2017 21 et 22 novembre 2017
BRI2	Modélisations et calculs de fiabilité pour IEC 61508/IEC 61511/S84- Un jour	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	21 septembre 2017 23 novembre 2017
BRI3	IEC 61508 - Théorie et pratique de la maîtrise des systèmes techniques - Trois jours	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	11 au 13 octobre 2017 27 au 29 novembre 2017

ISA-France est un organisme indépendant et qualifié de formation des ingénieurs et techniciens du monde de l'automation. (enregistrement auprès de la préfecture d'Ile de France sous le N° 11754084175).

Pour tout renseignement :

- 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 au format Word

Informations et bulletins d'adhésion à l'ISA 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
Siège social : 17 rue Hamelin – 75016 Paris

Retrouver nous sur LinkedIn