ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°47 – Août 2012 **Bulletin d'information d'ISA-France**

Au sommaire de ce numéro :

Sommaire | Evénements | Standards | Technologie | Formation

Sur vos calendriers

Nice – France – 14 et 15 septembre 2012

- **Conférence annuelle du District 12 (DLC)** à l'Hôtel Westminster. Cette conférence est ouverte à tous les adhérents. Elle accueillera **Bob Lindeman**, Président de l'ISA et **Eric Byres**, spécialiste mondial de la cyber-sécurité **–** Voir le programme **–** S'inscrire

Villeneuve d'Ascq – France – 25 octobre 2012

- En coopération avec le **LAGIS** (Laboratoire d'Automatique Génie Informatique et Signal), **l'Ecole Centrale de Lille, l'université Lille1 et le CNRS**, journée d'études sur le **diagnostic et la tolérance aux fautes dans les systèmes de commande industriels.**

  Voir plus loin l'annonce détaillée et l'article du Docteur William M. Goble.

Sûreté de fonctionnement des systèmes critiques

Diagnostic et tolérance aux fautes

ISA France Section

Jeudi 25 octobre 2012

Villeneuve d'Ascq

LAGIS — Centrale Lille

ISA-France organise le 25 octobre 2012, par en coopération avec le LAGIS (Laboratoire d'automatique, génie informatique et signal) et l'Ecole centrale de Lille un séminaire dédié aux **systèmes de contrôle tolérant aux fautes** aptes à remplir leurs missions en toute sécurité en présence de défauts. Cette journée permettra d'aborder les concepts de disponibilité et de sécurité fonctionnelle sur le plan théorique et sur le plan applicatif en considérant des applications industrielles de systèmes de contrôle commande : procédés de production, systèmes embarqués.

Qui doit participer ?

La journée du 25 octobre 2012 s'adresse à tous ceux qui, à un niveau quelconque, ont la responsabilité de la performance et de la sûreté de procédés. Elle permettra de comprendre l'apport des technologies de base telles que les algorithmes de détection et de localisation de défauts (FDI) et les méthodes de tolérance aux fautes de type passif ou actif et de les situer dans le cadre normatif de l'IEC 61508/ISA 84 et IEC 61511. Elle sera l'occasion de faire le point sur les travaux universitaires dans ce domaine.

Voir le **programme** et le **bulletin d'inscription** - **Téléchargeables également sur www.isa-france.org**

Renseignements : **ISA-France** – Marjorie Demeulemester – Tél : + 33 1 41 29 05 05

contact@isa-france.org **–** Fax : +33 1 46 52 51 93

Conditions d'inscription préférentielles jusqu'au 15 septembre 2012 – Réduction membres ISA – Tarifs spéciaux universitaires et étudiants de l'ECN et de l'Université Lille 1.

USA – Orlando – 22 au 27 septembre 2012

- Du 22 au 24 septembre, **ISA Fall Leaders meeting,** Assemblée Générale de l'ISA, au Rosen Centre Hotel. Voir le programme.
- Du 24 au 27 septembre, **Automation Week 2012, Technology and Solutions Event,** à l'Orange County Convention Center. www.isaautomationweek.org

Doha - Qatar – 9 et 10 décembre 2012

- Sous l'égide du District 12 de l'ISA**,** ISA Qatar et ISA France organisent **l'ISA Automation Conference** qui se tiendra à l'hôtel Intercontinental de Doha (Qatar), les **9 et 10 décembre 2012**, Cette conférence regroupera des vendeurs, utilisateurs et spécialistes du Moyen Orient, d'Europe et d'Afrique.
- Programme en cours d'établissement. Les thèmes de la conférence seront la sécurité fonctionnelle et la cyber-sécurité, l'intégration des systèmes de contrôle et des systèmes de gestion, les techniques de régulation avancée. Renseignements et préinscriptions sur contact@isa-france.org

Sommaire | Evénements | Standards | Technologie | Formation

ISA99 et cyber-sécurité : les leçons de Stuxnet

Dans le cadre des travaux relatifs à la mise à jour de certains documents constitutifs du standard ISA99 relatif à la cyber-sécurité des systèmes de contrôle, l'ISA a mis en circulation cet été, pour approbation, un rapport technique, répertorié ISA-TR62443-0-3, relatif aux améliorations à apporter à la norme ISA/IEC 62443-2-1 (ex ISA 99-02-01) « Establishing an Industrial Automation Security Program », de façon que les installations respectant la norme soient à l'avenir mieux à même de faire face à des attaques du type Stuxnet.

Ce rapport est fondé sur une analyse des écarts (gap analysis) entre les exigences actuelles de la norme ISA/IEC 62443-2-1 et les protections à mettre en place pour faire face efficacement à des attaques « Stuxnet like ». On rappelle que l'attaque Stuxnet, décrite dans l'ISA Flash 40 de novembre 2010, a révélé une nouvelle dimension dans la menace cyber-sécuritaire. Cette attaque a démontré qu'il était possible, en utilisant notamment des canaux du type *sneakernet* telles que des clés USB, d'introduire dans un système ou dans les fichiers associés, des constructions informatiques malveillantes capables de s'y repérer, de s'y propager, de modifier des paramètres ou des données, de communiquer avec l'extérieur, le tout en utilisant des failles 0-day, jamais identifiées ou jamais patchées. Il en est résulté la nécessité de reconsidérer tous les standards, de quelque origine qu'ils soient, afin de renforcer leur résilience face à de telles attaques.

Le rapport technique ISA-TR62443-0-3 identifie quatre voies principales de renforcement des exigences normatives actuelles :

- améliorer la démarche d'analyse de risques afin de mieux distinguer menaces et risques, de façon notamment à ne négliger aucune menace ;
- améliorer les procédures de récupération d'un système et/ou de son back up dont les composants ou les données ont été ou sont susceptibles d'avoir été corrompus. Ceci débouche sur la nécessité de sécuriser la fourniture d'éléments-clés de substitution.
- étendre le management de l'environnement du système et de sa sécurité physique en prenant en compte les mouvements de media mobiles et le risque d'infiltration de media électroniques corrompus ;
- renforcer les exigences de segmentation des réseaux, avec obligation d'identifier zones et conduits, de lister toutes les communications entre zones et de désigner des responsables de sécurité pour chacune des zones. Cette exigence architecturale, qui s'inscrit dans une démarche de défense en profondeur, est essentielle pour assurer la robustesse du système.

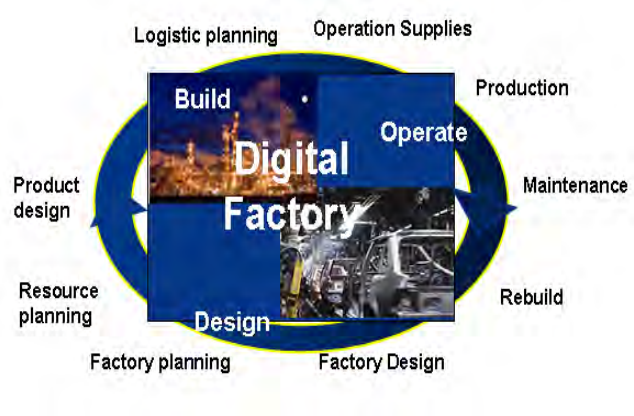
Dans l'attente d'une révision de la norme ISA/IEC 62443-2-1, le rapport ISA-TR62443-0-3 constitue une référence pertinente pour la mettre en œuvre de façon efficace. **Jean-Pierre Hauet** – jean.pierre.hauet@kbintelligence.com

Sommaire | Evénements | Standards | Technologie | Formation

L'usine numérique, mythe ou réalité ?

Le terme Digital Factory (usine numérique) est apparu dans le début des années 2000. L'usine numérique est constituée de l'ensemble des moyens numériques permettant de concevoir le processus de fabrication d'un produit. Mais qu'en est-il vraiment aujourd'hui ?
Cet article introduit les récentes activités du TC65 (Industrial-process measurement, control and automation) de la CEI concernant la normalisation des concepts de « Digital Factory ».

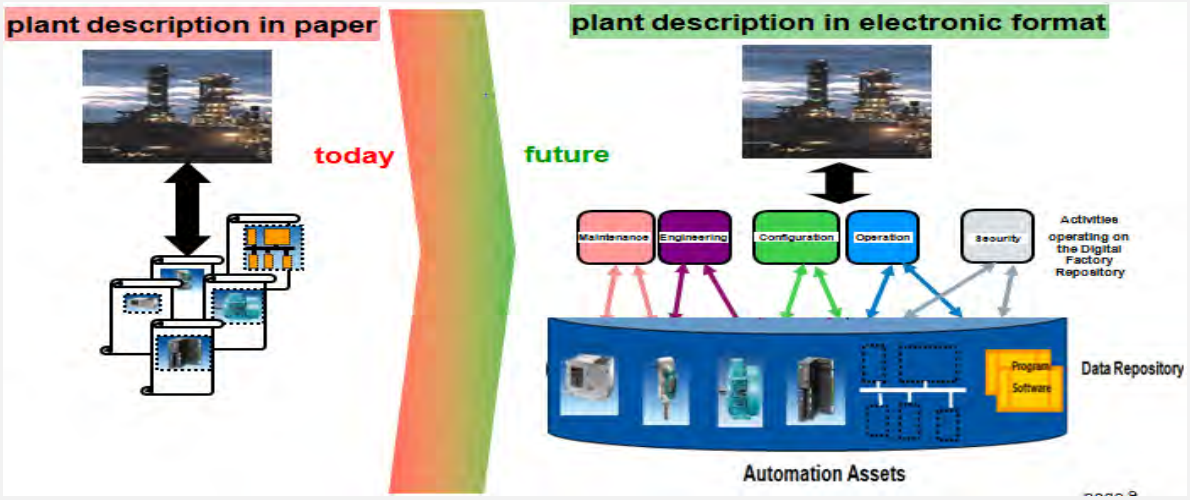
Digital Factory



Le cycle de vie d'une usine, c'est-à-dire la planification, la conception, la construction, le fonctionnement et la maintenance sont une combinaison de processus discrets qui exigent une haute intégration et une collaboration étroite des divers départements d'une entreprise avec des parties externes.
Dans le contexte de gestion du cycle de vie, on doit considérer une collection de systèmes et de méthodes participant au processus de réalisation pour le développement du produit final. L'usine numérique correspond à un environnement sans papier où les systèmes échangent des fichiers électroniques et des processus automatisés, cela ne signifie donc pas l'automatisation complète.

Digital Factory bénéficie des nouvelles technologies

L'échange de données entre les unités de production et l'entreprise était jusqu'à présent basé sur des documents papiers non normalisés. Désormais des normes définissent des formats d'échange de données sous forme de fichiers numériques qui sont placés dans une base de données. Ceci est illustré dans la figure ci-dessous :



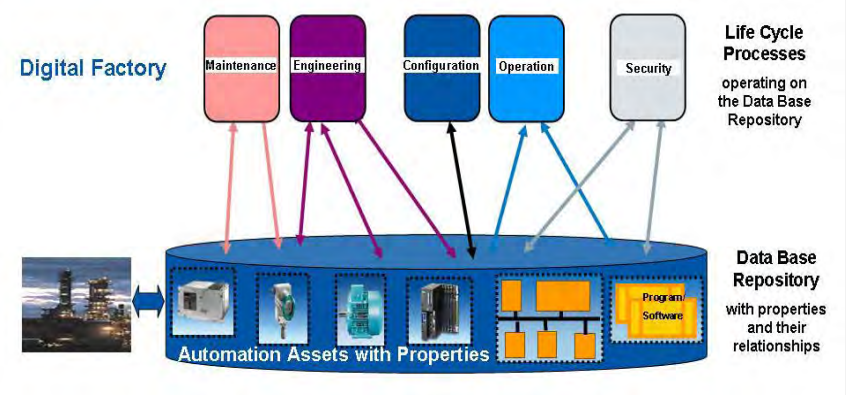
Les technologies actuellement disponibles favorisent le transfert immédiat de données et permettent aux entreprises une planification des ressources et l'utilisation des installations distribuées. Les nouvelles technologies rapprochent les ingénieurs de conception et de fabrication ; la facilité des échanges de données signifie qu'une modification de design peut être immédiatement répercutée à la fabrication ; ceci autorise de la flexibilité, améliore la qualité du produit et répond aux exigences des clients.

Dés lors que les systèmes communiquent, les opportunités d'automatiser des tâches abondent. Mais échanger des données n'est pas suffisant il faut que ces informations soient compréhensibles par les machines ; il faut donc partager leur signification afin que chaque système soit capable à l'aide de ces données d'exécuter des tâches de manière indépendante mais coordonnée.

Le pré-requis à cette entreprise numérique c'est que les propriétés des équipements, des systèmes et des applications soient normalisées pour être intégrées dans des bases de données.

Digital Factory et normalisation

Les informations électroniques disponibles sur une partie d'automatisation d'une usine sont stockées dans une base de données. Cette base de données mémorise toutes les informations concernant les dispositifs qui sont électroniquement décrits par "des propriétés" couvrant les aspects spécifiques de ces dispositifs (par exemple "les cotes" ou "le poids de dispositif"). Tout au long du cycle de vie de l'usine, des données sont ajoutées, supprimées ou modifiées dans la base de données afin d'avoir une description électronique à jour de l'usine.



Comme ces propriétés structurées sont la base du concept d'usine numérique, le besoin de normes définissant les structures des informations échangées est indispensable et un standard de l'industrie comme point de départ pour créer un modèle s'impose. Le périmètre du comité IEC SC65E (Devices and integration in enterprise systems) traite de la problématique du partage de données :

- le concept d'usine numérique consiste en données de structure normalisées stockées dans une base de données et c'est une des tâches du groupe de travail N°2 du SC65E qui s'emploie à classifier et normaliser les caractéristiques des dispositifs et des systèmes de commande de processus. Les données de structure normalisées sont définies comme les Listes de Propriétés (LOP) dans la série IEC 61987 ;
- le standard ISA95 aujourd'hui standard IEC/ISO (IEC 62264.x. Intégration du système de commande d'entreprise), développé par le groupe joint de travail N°5 du SC65E, est universellement reconnu car il s'applique à la plupart des environnements de production et de fabrication. Cette série de normes fournit un excellent cadre pour organiser les informations industrielles d'une activité industrielle.

Le modèle générique de Digital Factory

L'expression « Digital Factory » exprime la représentation informatique de toutes les ressources (assets) d'une configuration d'automatisme ainsi que leurs relations avec le procédé industriel. Cette représentation s'appuie sur un modèle générique simple permettant de décrire une installation industrielle à partir d'une description électronique de toutes les ressources d'automatisme qui la composent et ceci en s'appuyant sur les listes des propriétés de chacun des composants.

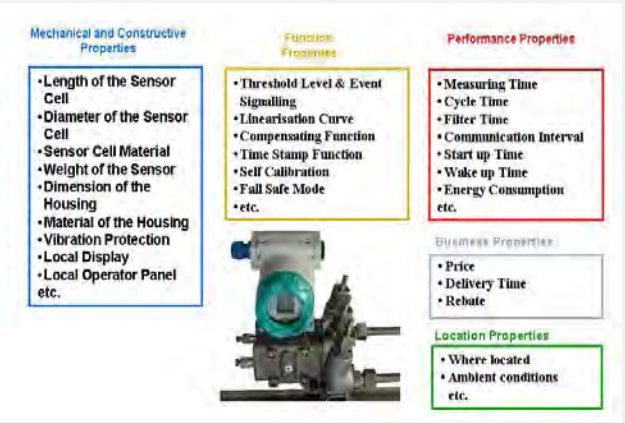
Le concept d'éléments de base est utilisé pour structurer les ressources d'automatisme et par la même l'unité d'automatisme. Le modèle repose sur les cinq éléments de base suivants:

- **Construction**, adresse toutes les données mécaniques et les propriétés de construction ;
- **Function,** reflète toutes les caractéristiques fonctionnelles de la ressource ;
- **Performance,** liée aux données fonctionnelles (par exemple : temps de cycle), à noter que les caractéristiques dédiées au management de l'énergie sont également prises en compte ;

Associés à ces éléments principaux deux autres éléments complémentaires sont souvent nécessaires :

- **Location,** indique la position de la ressource ;
- **Business,** reflète les aspects commerciaux de la ressource ou de l'unité d'automatisme.

La figure suivante donne un aperçu du modèle et son application pour décrire un capteur :



La spécification de ce modèle générique est un nouveau sujet d'étude qui a reçu l'approbation des comités nationaux du TC65. Un groupe de travail du TC65 s'appuiera sur un rapport technique récemment publié par un groupe d'experts internationaux qui présente les bases d'un modèle générique de référence pour « Digital Factory ». La présentation détaillée du modèle générique fera l'objet d'un article dans les prochains mois.

L'usine numérique, challenge pour de nombreuses entreprises pour les années futures, est en marche. Une dernière étape de normalisation des propriétés des équipements est nécessaire ; c'est le défi que relèvent de nombreux comités techniques de normalisation :

- TC 65 Industrial-process measurement, control and automation ;
- SC 17B Low-voltage switchgear and controlgear ;
- SC 22G Adjustable speed electric drive systems incorporating semiconductor power converters ;
- TC 57 Power systems management and associated information exchange ;
- TC 3 Information structures, documentation and graphical symbols.

…

Ce sont également d'importants travaux de la part des instances de normalisation (IEC, ISO) pour offrir l'accès aux utilisateurs à des bases de données normalisées (IEC 61360 - Component Data Dictionary (CDD - V2.0011.0002).

Christian Verney - Chairman IEC SC65E - cv@cverney.com

Fault Tolerance - The critical need for diagnostics and common cause strength

A l'occasion du Forum de Villeneuve d'Ascq du 25 octobre 2012 (voir ci-dessus) sur le diagnostic et la tolérance aux fautes, le **Docteur William M.Goble**, a bien voulu nous confier un éditorial sur les limites de la redondance dans les ystèmes d'automatisme à haute performance.

Le Dr Goble est Certified Functional Safety Expert et Principal Partner à l'EXIDA. Il dispose de 30 années d'expérience et est unanimement reconnu comme expert dans le domaine des systèmes électroniques, notamment dans celui des systèmes à haut niveau de sécurité et de disponibilité, dans le développement de nouveaux systèmes d'automatisme et dans l'analyse du marché. Il est à l'origine de beaucoup des techniques utilisées pour l'évaluation probabiliste des performances des systèmes d'automatisme fiables et sûrs.

Many designers believe the key to success in the design of systems with high availability/safety is redundancy. Some functional safety standards emphasize redundancy as the primary design attribute by prescriptive tables with minimum levels of redundancy. There was a time in the past when I believed that redundancy was all a design needed to achieve high availability, safety integrity or both. I recall the math textbook that explained how the probability of dual system failure equaled the probability of A failure times the probability of B failure. The calculation showed two or three orders of magnitude improvement in availability. I led a design team for a redundant process controller. I concluded that in the next twenty years of production of this new redundant controller I would never see a redundant system failure in the field! A logical conclusion for a naive engineer with no experience in redundant systems.

Then a redundant system failed in service. I was sent to do the field failure investigation. I learned that redundant systems can fail due to a common stress - a "common cause" failure. Then another failure of this redundant system occurred. I traced this failure to root cause and realized that the system output was coming from the bad unit because the automatic "diagnostics" did not identify the failure and the switchover circuitry did not select the good unit. Thus it became clear to me that both poor diagnostic coverage and common cause susceptibility were both capable of destroying the effectiveness of a redundant system. Redundancy depends on high coverage automatic diagnostics (95 % +) and high common cause strength.

High common cause strength comes from avoiding a common stress to the redundant parts of the system. One of the old design rules was physical separation. Redundant equipment should be in separate rooms, separate cabinets or at least separate p.c. boards. Alternatively redundant equipment can be designed with parts that are susceptible to the same stress. This concept is called "diversity" and strongly promoted in nuclear safety standards.

The redundancy concept continues to be used extensively by many designers in many different industries. But many of the designs do not come close to achieving the goals of high availability and/or safety. Many designers have yet to learn the techniques of high common cause strength and high coverage automatic self-diagnostics. As a Certification Body, EXIDA sees many of these redundant designs.

In one case a designer created triple redundant input circuits with a two out of three (2oo3) voting circuit. The design was implemented in one field programmable gate array (FPGA). This classical 2oo3 design concept has been used since the 1930s in relay logic circuits. The design concept has great merit. A 2oo3 design is especially effective in tolerating single channel failures in equipment with short mission times and a full functional test at the end of each mission. For longer mission times, repairable modules and automatic diagnostics are required to tolerate single channel failures as effectiveness is lost when one channel fails. Automatic diagnostics are relatively easy to implement via comparison of the three channel combinations (AB, AC and BC). This particular FPGA design was intended for

long mission times but did not implement channel comparison and did not have any means to repair a single channel. Most FPGA design tools do not give the designer any control over which gates are used internally. Even with this control the common cause susceptibility of multiple gates in the same integrated package is high. Given the likelihood of multiple failures due to a common stress and lack of effective diagnostics, the redundancy in this design adds very little to safety and availability of the product. This design did not pass functional safety certification.

In another case an integrated circuit manufacturer wanted to design a microcomputer subsystem to meet requirements of IEC 61508 SIL 3. Traditional design thinking would say this is not possible. However the manufacturer designed on chip redundancy combined with special techniques to minimize common cause susceptibility and high effectiveness automatic diagnostics. The result was a successful certification.

This SIL 3 microcontroller had the redundant parts of the system carefully oriented in different parts of the substrate at different orientations. Separate power sources, independent protection circuitry and other techniques were used. These design features provided much higher level of common cause strength. Of course this is only possible in fully custom integrated circuits where the designer has complete layout control. There is still common cause susceptibility and that was estimated in the probability of failure analysis but the design met SIL 3 requirements.

The redundant microcontroller design had automatic self-diagnostics with coverage ratings greater than 95%. This rating was obtained using various techniques including comparison of redundant subsystems, error detection and correction bits in memory and various other techniques. It was clear to the EXIDA assessors that this design was carefully implemented to meet the reality of effective redundant system designs.

There are many other examples of good designs. System designers today benefit greatly from functional safety standards like IEC 61508 because awareness of the methods of effective redundant system design is included in that standard and the many industry specific standards derived from it. In the 1990's, information about common cause failures seemed to be only in papers published by the nuclear industry and NASA. Today this information has spread into multiple industries including not only process control but even automotive. Redundant architectures have evolved into combinations of classical dual and triple designs with reasonable common cause strength and very effective diagnostics. Valid redundant designs have been done not only with the microcontroller based logic solvers but sensors and even mechanical final elements.

Redundancy can be a very effective means to achieve high availability/safety in any system design. But the designers must understand that the job is not as simple as duplicating or triplicating identical sets of parts. Common cause susceptibility must be evaluated and designs must be sufficiently strengthened. Automatic self-diagnostics must be carefully designed into the system. I hope that today's designs will not see the failure of a redundant system in twenty years of production. Or at least very few redundant system failures.

Sommaire | Evénements | Standards | Technologie | Formation

ISA-France - Programme de formation 2012

Code	Désignation	Calendrier 2011	
		Lieu	Date
JPH1	ISA-100 et les applications nouvelles des radiocommunications dans l'industrie - Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	5 et 6 mars 2012 9 et 10 mai 2012 17 et 18 septembre 2012 10 et 11 décembre 2012
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	7 mars 2012 11 mai 2012 19 septembre 2012 12 décembre 2012
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	27 et 28 février 2012 14 et 15 mai 2012 24 et 25 septembre 2012 17 et 18 décembre 2012
JVI6	Manufacturing Intelligence : Construire la Performance dans l'Entreprise	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	2 et 3 mars 2012 21 et 22 mai 2012 26 et 27 septembre 2012 19 et 20 décembre 2012
BRI1	ISA-84 - Sûreté de fonctionnement avec les normes IEC61508 et IEC61511- Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	15 et 16 février 2012 2 et 3 mai 2012 12 et 13 septembre 2012 3 et 4 décembre 2012
JPD1	ISA/CEI 62443 (ISA99) - Cyber-sécurité des systèmes de contrôle - Un jour	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	2 mars 2012 4 mai 2012 7 septembre 2012 5 décembre 2012
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	23 et 24 février 2012 20 et 21
BDC1	Normalisation dans le domaine de l'automation - Deux jours	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	13 et 14 février 2012 10 et 11 septembre

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 - Marjorie Demeulemester
- 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