ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°48 – Octobre 2012 **Bulletin d'information d'ISA-France**

Au sommaire de ce numéro :

- Sur vos calendriers : Diagnostic et tolérance aux fautes - Villeneuve d'Ascq – 25 octobre 2012
  ISA Automation Conference – Doha (Qatar) – 9 et 10 décembre 2012
- Evénements : ISA Fall meeting Orlando – District 12 DLC Nice
- Standards : formation du comité ISA 108 – Publication du rapport technique sur la gestion des alarmes
- Technologie : Eric Byres : Control System Security in a Post-Stuxnet World

Sommaire | Evénements | Standards | Technologie | Formation

Sur vos calendriers

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.**

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.

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 de finalisation 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 - Télécharger le prospectus pour sponsors et exposants.

En septembre

Orlando – USA – 22 au 24 septembre 2012

Du 22 au 24 septembre 2012, s'est tenu à Orlando (USA), l'*ISA Leaders Fall meeting* regroupant des délégations de l'ensemble des sections ISA, en conjonction avec l'Automation Week. Au cours de cette réunion, a été discuté le rapport intérimaire de la Task Force chargée de faire des propositions relatives à l'évolution de la structure de gouvernance de l'ISA. Ce rapport est disponible en cliquant sur l'image de droite. Chaque adhérent de l'ISA a la possibilité de faire connaître ses observations et suggestions en se rendant sur le site de l'ISA www.isa.org


Terry Ives Bob Lindeman

A l'issue du *Council of Society Delegates* (Assemblée Générale de l'ISA), Bob Lindeman a transmis le marteau à Terry Ives qui prendra les fonctions de Président à compter du 1er janvier 2013.
Au cours de la même assemblée, Bob Lindeman a remis à Jean-Pierre Hauet, Président d'ISA-France, un « award » en reconnaissance des services rendus comme District Vice President et comme membre de l'Executive Board.

Nice – 5 au 6 octobre 2012

La *District Leaders Conference* du District 12 de l'ISA (Europe, Moyen-Orient, Afrique) s'est tenue à Nice les 5 et 6 octobre 2012, sous la présidence de Jean-Pierre Hauet, en présence de Bob Lindeman, Président de l'ISA et avec la participation de représentants de Belgique, France, Grande-Bretagne, Irlande, Israël, Italie, Pays-Bas, Portugal, République Tchèque, Suède.
Cette réunion a permis de passer en revue le fonctionnement des sections ISA au sein du District 12 et débattre des questions intéressant le futur de la profession et de l'association.
Eric Byres, spécialiste canadien en cyber-sécurité de renommée mondiale, a donné une conférence sur le thème *Control System Security in a Post-Stuxnet World* dont on trouvera plus loin le texte.

Au cours du diner, Richard Lasjunies, MES Life Science development for SIEMENS, a prononcé une key-note address sur le thème *Integrating product and production lifecycle.*

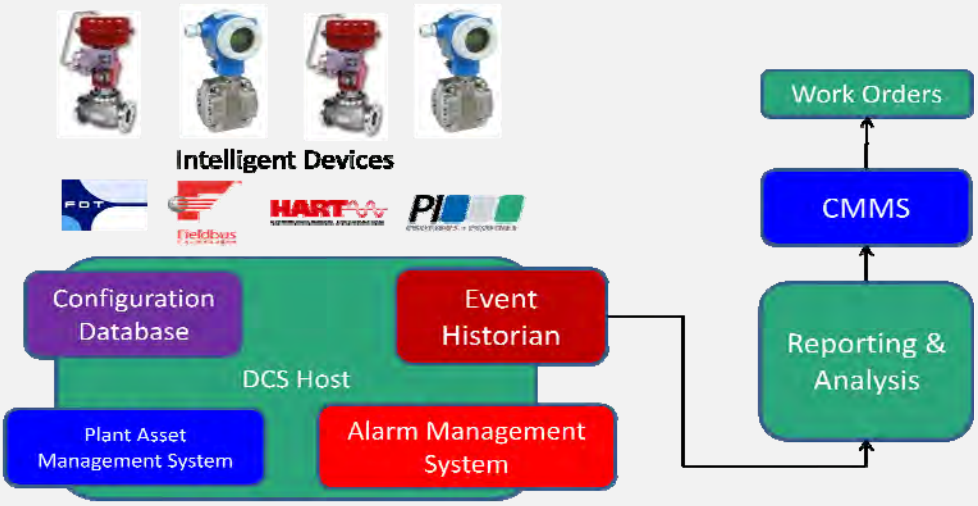
Sommaire | Evénements | Standards | Technologie | Formation

Formation du comité ISA108 : management des « intelligent devices »

Les « intelligent devices » (équipements de terrain intelligents) envahissent le monde du contrôle de procédé. Ils sont censés permettre une transformation complète de la façon dont est utilisée l'information qu'ils fournissent, en ce qui concerne les équipements eux-mêmes et le procédé qu'ils contrôlent. Ainsi, des équipements posant un problème de maintenance peuvent être détectés plus tôt et l'information véhiculée directement au système de contrôle, à un système de gestion des actifs (asset management) ou plus généralement à tout système ayant à en connaître.

Dans beaucoup de cas cependant, le résultat n'est pas au rendez-vous, souvent parce que le personnel utilise des vieilles méthodes de gestion de la maintenance alors que les équipements sont nouveaux. Les nouveaux équipements sont installés ainsi que les applications, mais les opérateurs et les techniciens restent avec leurs méthodes anciennes

traditionnelles de maintenance prédictive ou curative et ne tirent pas profit de la grande quantité d'information dont ils disposent.
Un nouveau comité de standardisation ISA, l'ISA108, a été formé et chacun peut y adhérer. Le comité se propose de définir des cadres de référence pour la conception, le développement, l'installation, l'utilisation du diagnostic et de toutes les autres formes d'information produite par les équipements de terrain intelligents dans les industries de procédé.



« Avec plus de 80 % des équipements intelligents dont les données ne sont pas utilisées ou qui ne sont même pas connectés à un système de gestion des données, il y a une perte de revenu considérable dans les industries de process » déplore Ian Verhappen, de Yokogawa Canada, responsable du comité ISA108. *« De là résulte clairement un besoin de disposer d'une série de standards définissant la façon d'intégrer ces données dans les systèmes de contrôle et dans les systèmes de gestion de l'information afin de tirer le meilleur parti de la maintenance « proactive ».*
Le Comité a pour mission d'élaborer des bonnes pratiques pour la mise en œuvre et l'exploitation des systèmes utilisant l'information provenant d'équipements de terrain intelligents. Des modèles et des bonnes pratiques, fonction des rôles dévolus au personnel, seront proposés. Ils viseront notamment à normaliser la formulation du flot d'information circulant au travers d'un système.
Les personnes intéressées à participer à ce comité peuvent contacter Ellen Fussell Policastro à l'ISA : efussell@isa.org
Télécharger ici le document de présentation du Comité 108 (ppt).

Gestion des alarmes : publication du rapport technique du Comité ISA18

Le rapport technique du Comité ISA18, ISA-TR18.2.6-2012, *Alarm Systems for Batch and Discrete Processes*,a été publié et est disponible sur www.isa.org/standards. Ce rapport technique a trait à l'application aux procédés batch et discrets des principes de gestion des alarmes définis dans le standard *ANSI/ISA-18.2-2009, Management of Alarm Systems for the Process Industries.*
Rappelons qu'un système d'alarme a pour objet d'alerter, d'informer et de guider les opérateurs en cas de situation anormale ou de dysfonctionnement d'un équipement.

Sommaire | Evénements | Standards | Technologie | Formation

Eric Byres, ISA Fellow, spécialiste mondialement reconnu dans le domaine de la cyber-sécurité des installations de contrôle, a bien voulu prononcer une conférence sur le thème ***Control System Security in a Post-Stuxnet World*** lors de la réunion du District 12 qui s'est tenue à Nice les 5 et 6 octobre dernier. Nous reproduisons ci-après, avec son aimable autorisation, le texte intégral de sa conférence.

Eric Byres
P. Eng., ISA Fellow
CTO and VP Engineering
Tofino Security Product Group, Belden Inc.
eric.byres@tofinosecurity.com
www.tofinosecurity.com

How the "Push for Productivity" degraded Pipeline SCADA Security

Anyone working with SCADA or industrial control systems (ICS) is aware of the pressure to increase productivity and reduce costs through network integration. For example, sharing real-time data from plant floor operations with management is standard practice for most companies. Similarly, the demand for remote support has made many control systems accessible via Internet-based technologies.

At the same time, SCADA systems themselves have changed radically. Proprietary networks have been replaced with equipment using Ethernet technology. Single purpose operator stations have been replaced with computers running Windows™, and IT software such as PDF readers; as well, web browsers are installed in every control room.

These new technologies are enabling companies to implement agile, cost-effective business practices. Unfortunately, they also come at a cost; many of the same security vulnerabilities that have plagued business systems now appear in SCADA systems. Industrial control systems are now exposed to cyber security threats they were never designed for.

Stuxnet - The Game Changer

Cyber attacks on automation systems were considered by many to be a theoretical problem until the discovery of the Stuxnet worm in July, 2010. At that moment the world changed, not only for manufacturing, energy and transportation companies, but also for automation vendors, hackers, criminals and even governments.

Stuxnet was specifically designed to attack Siemens automation products. It was capable of downloading proprietary process information, making changes to logic in PLCs, and covering its tracks. It used previously unknown vulnerabilities to spread. It was powerful enough to evade state-of-the-art security technologies.

Stuxnet's intended target was the uranium enrichment centrifuges used by Iran in its nuclear armaments program. Seizing control of the automation system, the worm was able to reconfigure the centrifuge drive controllers, causing the equipment to slowly destroy itself.

Stuxnet had a specific target, but like all attacks, cyber or conventional, there was collateral damage. Several companies in the US had PLCs that were reconfigured by Stuxnet, probably by accident. No real damage, but a lot of labor charges and shutdowns.

Even these problems soon stopped; software patches and anti-virus signatures soon drove Stuxnet into extinction. Unfortunately, the problem did not end there.

Stuxnet's Children Have Arrived

The real impact of Stuxnet began to appear after the worm itself was history. Thanks to Stuxnet's publicity, hackers, activists and criminals discovered that SCADA/ICS products are attractive targets. These systems soon became targets of choice for public security disclosures; in 2011 the US ICS-CERT released 104 security advisories for SCADA/ICS products from 39 different vendors. Prior to Stuxnet, only 5 SCADA vulnerabilities had ever been reported.

What was particularly concerning is that attack code was released for 40% of these vulnerabilities. This meant that the bad guys both knew where to find holes in SCADA/ICS products, and had the tools to exploit them.

Stuxnet also showed the world the power of a well-designed ICS worm. It could steal corporate secrets, destroy equipment and shut down critical systems. And while Stuxnet appeared to have been created for political reasons, the opportunities for corporate exploitation were obvious to governments and criminals alike. It was only a matter of time before someone reused the techniques from Stuxnet to go after other victims.

By February 2011, a new attack against industry was exposed. A paper titled *"Global Energy Cyberattacks: Night Dragon"* described cyber threat activity that was stealing sensitive data such as oil field bids and SCADA operations data from energy and petrochemical companies.

In early October 2011, a variety of sources announced the discovery of a new trojan named "Duqu". This targeted malware used a lot of the same source code as Stuxnet. Unlike Stuxnet, it is an information stealer and doesn't appear to directly target PLC systems. However, according to Symantec:

"Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers… The attackers are looking for information such as design documents that could help them mount a future attack on various industries, including industrial control system facilities."

At the end of October 2011, Symantec released details of a third attack directed at 25 companies involved in the manufacturing of chemicals and advanced materials. Calling these attacks the "*Nitro Attacks*" Symantec reported :

"The purpose of the attacks appears to be industrial espionage, collecting intellectual property for competitive advantage."

But not all cyber attacks are driven by industrial espionage motives. The recent Shamoon attacks, attributed to an activist group called the "Cutting Sword of Justice", targeted Saudi Aramco and other energy companies in the Middle East. This relatively unsophisticated piece of malware reportedly destroyed the data on 30,000 computers. If true, then the bar for effective disruption of a business has been lowered to the level of enthusiastic amateurs. Like the concerns governments have when they think of terrorists getting their hands on nuclear weapons, the proliferation of SCADA /ICS malware is a serious issue. No rules of engagement apply!

Why do they do it?

When most people consider the motivation of worm creators and hackers, they think of the destructive focus of early cyber events like the Slammer worm in 2003. That worm shut down vast portions of the Internet and affected companies around the world.

Today's new attacks show different focuses. Most often it is a subtle and persistent attempt to steal valuable information - information that can be used to make a counterfeit product, out-bid a rival for an oil exploration lease, or coordinate a short selling campaign against a company's stock.

Theft of operations information for commercial espionage has been around long before networks and cyber-security showed up. Check out the article "The Pizza Plot" for an example of how production data from a Kraft food plant was used by a competitor to reshape the $2.3 billion pizza market. Today the profit potential for SCADA information theft can be even bigger.

But clearly some attacks (like Shamoon) are intended to have long term destructive impacts on a company or industry. Even data stealing worms can also be precursors to later destructive attacks against automation systems. Clearly, the Stuxnet designers collected detailed process information on their victim prior to actually creating their worm. Could the Duqu worm be a forerunner to a more destructive attack?

It is worth noting that the goal of Stuxnet was to impact Iran's production rather than harm people. So it is possible that the goal of this next generation of malware is to quietly stop production at a utility or pipeline somewhere in the world. Impacting the production of a rival, short selling the shares of a company or extorting money under the threat of a disruption are all profitable activities for a criminal or nation-state group.

Why we can't keep Son-of-Stuxnet out of our Systems

Many security experts suggest the only solution is to go back to the days of completely isolated automation systems. Unfortunately, walling off a control system just isn't feasible today. As I explained in the article "#1 ICS and SCADA Security Myth: Protection by Air Gap," modern industry depends on a steady diet of electronic information from the outside world to operate. Cut off one source of data into the SCADA system and another (potentially riskier) "sneaker-net" source replaces it.

Industry and government can try to battle this trend by banning technologies and mandating procedures. We see this sort of strategy every time we try to board a plane and wait in long lines to take our shoes off. Frankly, I don't think it is effective security for air travel. It is even worse for companies that need to be profitable if they are going to stay in business.

The Way Forward

Is the situation hopeless? No, but security practices must improve significantly. First, industry needs to accept the idea that complete prevention of SCADA system infection is impossible. The article, *Cyber Security and the Pipeline Control System* (Feb 2009), showed that determined attackers have many pathways available to them, not just the obvious ones like Internet connections. As a result, no matter what we do, some SCADA assets will suffer compromise over the life of a system.

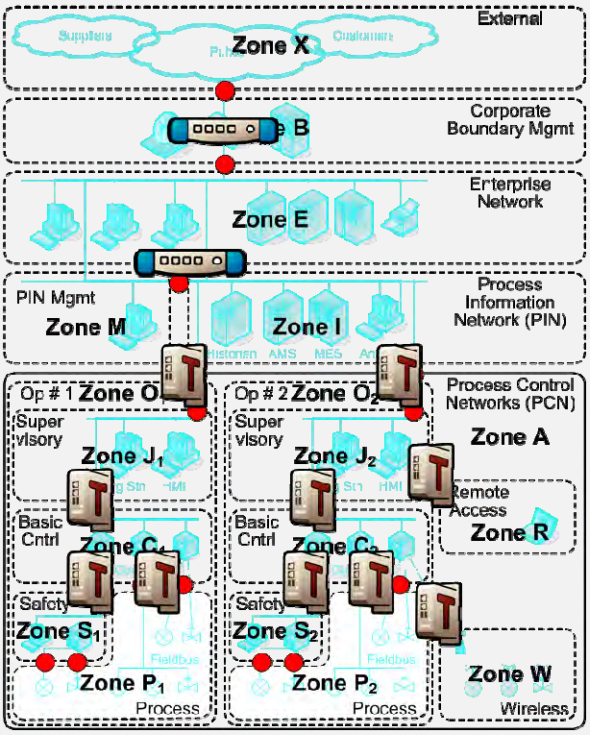
The only solution is to do what the human body does to defend against nasty viruses. It can't keep them all out (you do have to breath), so it has excellent systems for the rapid detection of a hostile entity. It does not just monitor what passes through your mouth – it monitors your entire body. Once something bad is detected, the immune system immediately goes to work to isolate and control it.

Similarly, for effective SCADA security pipeline operators need to:

- Consider all possible infection pathways and have strategies for managing each one. Don't just focus on the obvious like the corporate firewall or USB thumb drives.
- Aggressively sub-divide ICS networks to limit the consequences of a compromise. The ISA/IEC-62443 standards (formerly called ISA99) call this building a zone-based defense.

- Define choke-points (called conduits in the ISA and IEC standards) between zones, where you can control or even shut off network traffic in cases of emergency. Figure 1 shows a zone and conduit model deployed in a large North American refinery.
- Look beyond traditional IT firewalls for your SCADA zone controls, toward firewalls capable of deep packet inspection of industrial protocols. This is important because worms like Stuxnet have shown how easy it is to piggy-back on valid traffic to escape detection.
- Focus first on securing mission critical systems, particularly safety integrated systems (SIS).
- Include security assessments as part of periodic maintenance processes.
- Work to improve the culture of security amongst management and technical teams.

Implementing these changes will improve the "*defense-in-depth*" posture for any SCADA /ICS system and help protect your operation from cyber espionage. Better SCADA security is needed urgently; waiting for the next worm may be too late.



Zone and Conduit Strategy Secures Refinery

References and Further Reading:

#1 ICS and SCADA Security Myth: Protection by Air Gap:
http://www.tofinosecurity.com/blog/1-ics-and-scada-security-myth-protection-air-gap
Stuxnet Central:
http://www.tofinosecurity.com/stuxnet-central
US Industrial Control Systems Cyber Emergency Response Team (ICS-CERT):
https://www.us-cert.gov/control_systems/ics-cert/
Global energy Cyber Attacks "Night Dragon":
https://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf
W32.Duqu - The precursor to the next Stuxnet:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf
The Nitro Attacks - Stealing Secrets from the Chemical Industry:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf
Shamoon Attacks Saudi Aramco:
Shamoon Malware and SCADA Security – What are the Impacts?
The Slammer Worm:
http://en.wikipedia.org/wiki/SQL_Slammer
The Pizza Plot:
http://www.tofinosecurity.com/sites/default/files/Pizza%20Plot.pdf

Sommaire | Evénements | Standards | Technologie | Formation

ISA-France - Programme de formation fin 2012 (programme 2013 en cours d'établissement)

Code	Désignation	Calendrier 2012	
		Lieu	Date
JPH1	**ISA-100 et les applications nouvelles des radiocommunications dans l'industrie - Deux jours**	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	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	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	17 et 18 décembre 2012
JVI6	Manufacturing Intelligence : Construire la Performance dans l'Entreprise	**Rueil-Malmaison** KB Intelligence 10, rue Lionel TERRAY	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	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	5 décembre 2012

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