ISA France Section

ISA Flash

Setting the Standard for Automation™

ISA FLASH N°58 – Septembre 2015 **Bulletin d'information d'ISA-France**

Sommaire | Evénements | Standards | Technologie | Formation

Au sommaire de ce numéro :

- **Evénements** : Séminaire « Sûreté et sécurité de fonctionnement des systèmes critiques » – Le 20 octobre 2015 à Villeurbanne avec l'INSA de Lyon – L'ISA Fall meeting à Louisville (Etats-Unis) du 10 au 13 octobre 2015 – ISA-France partenaire de Smart Industries du 15 au 17 septembre 2015.
- **Standards : Deux nouveaux standards de l'IEC 62443 publiés par la CEI – L'ISA Security Compliance Institute – L'IEC 62443 (ISA 99) en route vers sa complétion –**
- **Technologie :**
  - La SEE publie un Livre blanc sur la cybersécurité des réseaux électriques intelligents
  - Un ouvrage de référence sur la cybersécurité des installations industrielles
  - When failure is not an option… par Steve Mustard
- **Formation :** Le programme de formation ISA-France 2015

Sommaire | Evénements | Standards | Technologie | Formation

Séminaire ISA-France/INSA de Lyon – Le mardi 20 octobre 2015 à Villeurbanne
« Sûreté et sécurité de fonctionnement des systèmes critiques »

Les systèmes de contrôle-commande des procédés industriels à risques (énergie, chimie, etc.) et les systèmes embarqués critiques (avionique, ferroviaire, etc.) relèvent, par l'importance des enjeux, d'une démarche de sûreté de fonctionnement tant au niveau de la conception, de la réalisation et de la mise en œuvre, qu'au niveau de la validation et de la maintenance.

Les problématiques de "criticité" de ces deux types de systèmes de commande sont similaires puisqu'elles impliquent la fiabilité et la disponibilité des matériels et des logiciels utilisés dans la réalisation des fonctions, la continuité de service s'avérant indispensable pour satisfaire des impératifs de sécurité et pour de simples motifs économiques. Cependant, dans le cas de certains systèmes embarqués, l'absence de position de repli sûre conduit à des exigences particulières

L'émergence très forte du **risque cybersécuritaire** amène à positionner la préoccupation de « security » au même niveau que les facteurs techniques dans l'analyse de la disponibilité.

En partenariat avec

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

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 cybersécuritaire ?

HIMA SAFETY NONSTOP

ANSYS ESTEREL Technologies

Télécharger le programme GO **– Le bulletin d'inscription** GO **Voir les résumés** GO
Inscription et paiement en ligne possibles sur www.isa-france.org
Renseignements : contact@isa-france.org **Tel : 01 41 29 05 05**

Samedi 10 au mardi 13 octobre 2015 – ISA Fall meeting à Louisville (USA)

La grande manifestation annuelle de l'ISA se tiendra cette année à Louisville (KY) aux Etats-Unis du samedi 10 au mardi 13 octobre 2015.
L'accès est libre et gratuit pour tous les adhérents de l'ISA. Une occasion unique d'échanger des informations et de confronter des points de vue avec d'autres membres de l'ISA, venus du monde entier.
Les réunions, et en particulier le Council of Society Delegates, se tiendront au Louisville au Marriott Downtown Hotel.
En savoir plus…

ISA-France partenaire de Smart Industries 2015 du 15 au 17 septembre à Paris

ISA-France sera partenaire de **Smart Industries 2015**, l'évènement dédié à l'Usine du Futur, qui se tiendra du 15 au 17 septembre à la Porte de Versailles à Paris hall N°2.
Sur 4 000 m², plus de 3 000 visiteurs viendront à la rencontre des 150 exposants pour 3 jours de business sur le thème de l'usine connectée intelligente. Vision et Transmission en seront les maîtres-mots.
Créer votre badge visiteur…

Sommaire | Evénements | Standards | Technologie | Formation

Deux nouveaux standards de l'IEC 62443 publiés par la CEI

La CEI a publié le 30 juin 2015 deux nouveaux standards qui s'inscrivent dans la série IEC 62443 (ISA99) relative à la cybersécurité des systèmes d'automatismes et de contrôle industriel.

L'IEC TR 62443-2-3:2015 « Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment », est un rapport technique spécifiant les exigences pour les exploitants et les fournisseurs de systèmes d'automatisme et de contrôle industriel (IACS) relatives à l'établissement et à la maintenance d'un système de gestion des modifications. Ce rapport technique définit un format pour la distribution, par les fournisseurs d'IACS vers les exploitants des IACS, des informations relatives aux patches de sécurité. Il précise certaines des activités associées au développement de ces patches et à leur déploiement. Le format d'échange a été conçu pour les patches sécuritaires mais peut également être utilisé pour n'importe quelle mise à jour.

L'IEC 62443-2-4:2015 "Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers" est une norme issue des travaux du WIB (International Instrumentation Users Association, association d'origine néerlandaise). Cette norme contient les exigences applicables aux fournisseurs de services d'intégration et de maintenance dans le domaine des IACS.

Un fichier Excel est annexé la norme afin de faciliter son application. Le WIB offre par ailleurs en téléchargement partiellement libre un outil d'auto évaluation développé par WCK GRC permettant aux entreprises de se benchmarker.

L'IEC 62443 (ISA 99) en route vers sa complétion

En parallèle à la publication officielle des deux standards précités, a été mise en circulation au sein du Comité ISA99, pour approbation en tant que standard ISA, la partie **ISA/IEC 62443-3-2 « Security for industrial automation and control systems – Security risk assessment and system design »**.

Ce texte, longtemps attendu, constitue une brique essentielle du dispositif IEC 62443. Il définit un ensemble de règles d'ingénierie permettant de guider une organisation au travers du processus d'évaluation des risques et d'identification et d'application des contremesures de nature à ramener ces risques à un niveau acceptable. L'un des points-clés de ce texte réside dans les modalités d'application du concept de zones et de conduits introduit dans la partie ISA/IEC 62443-1-1.

Le standard concerne les exploitants d'IACS (Industrial Automation & Constrol Systems), les intégrateurs, les fournisseurs de produits et de services ainsi que les autorités en charge du respect des normes.

L'IEC 62443 (ISA99) franchit ainsi une nouvelle étape vers sa complétion. La figure ci-dessous récapitule l'état des différents textes au 31 août 2015.

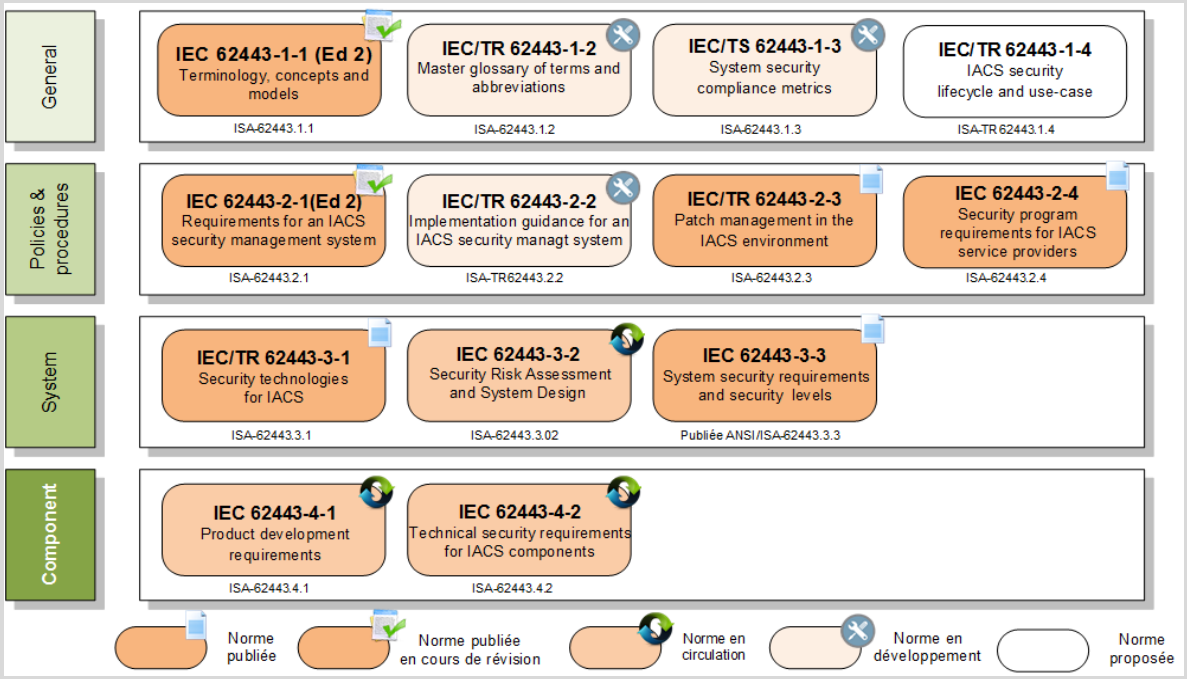


Figure 1 : Tableau d'avancement de la norme ISA/IEC 62443 au 31 août 2015.

ISA Security Compliance Institute ISASecure

L'ISA Security Compliance Insitute propose aujourd'hui trois certifications correspondant aux exigences de trois textes essentiels de l'IEC 62443 :

- IEC 62443-3-3: Requirements for System Security Assurance **(SSA) Certification**
- IEC 62443-4-2: Requirements for Embedded Device Security **Assurance (EDSA) Certification**
- IEC 62443-4-1: Requirements for Security Development Lifecycle Assurance **(SDLA) Certification**

Les cahiers des charges de ces certifications sont téléchargeables en ligne.

Sommaire | Evénements | Standards | Technologie | Formation

La SEE publie un Livre blanc sur la cybersécurité des réseaux électriques intelligents

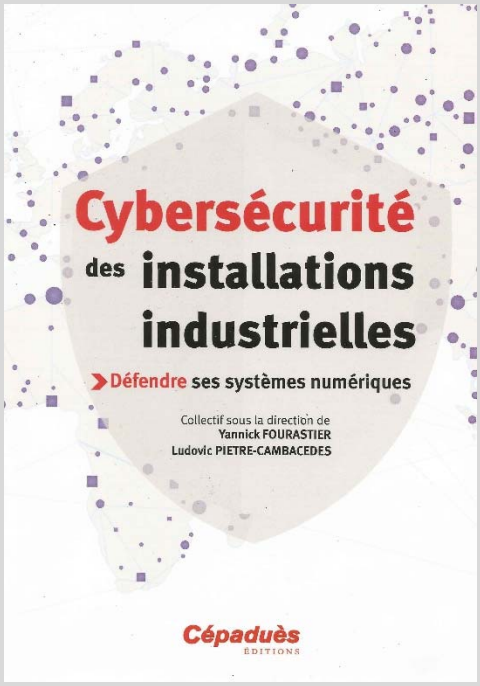
Dans le cadre de son Cercle des entreprises, la SEE vient de publier un Livre blanc sur la cybersécurité des réseaux électriques intelligents établi par un groupe de travail associant tous les grands acteurs du domaine : ANSSI, EDF, ErDF, RTE, Siemens, Alstom Grid, Atos, CEA, Gimelec, Institut Mines-Télécom, Orange. ISA-France était représenté au sein de ce groupe de travail par Jean-Pierre Hauet.

Ce Livre Blanc met à la disposition des acteurs intéressés par les REI des éléments d'information essentiels sur la problématique des REI. Il analyse le risque cybersécuritaire sous différents angles et notamment au regard des risques attachés aux aspects plus traditionnels de la sécurité, sûreté de fonctionnement en particulier. Il fait le point sur la réglementation et sur les normes applicables aux REI qui, bien qu'étant pour certaines encore en cours de finalisation, permettent à la plupart des acteurs de disposer d'un référentiel suffisant pour construire un système de gestion de la cybersécurité adapté à leurs besoins.

Le Livre blanc est téléchargeable gratuitement en ligne.

Un ouvrage de référence sur la cybersécurité des installations industrielles

Les **Editions Cépaduès** viennent de publier un consacré à la « **Cybersécurité des installations industrielles** ». Ce livre est le résultat d'un travail collectif mené sous la direction de Yannick Fourastier (Airbus Group) et Ludovic Piètre-Cambarécès (EDF). Parmi les auteurs des 16 chapitres de ce volume de 528 pages, on retrouve les noms de la plupart des spécialistes qui œuvrent dans le domaine de la cybersécurité des systèmes industriels, en particulier, outre ceux des deux coordinateurs, ceux de Gérôme Billois (Solucom – Administrateur du CLUSIF), Stéphane Meynet (ANSSI), Pierre Kobes (Siemens), Frédéric Guyomard (EDF R&D), Patrice Bock (ISA-France) et bien d'autres.



Cet ouvrage est exemplaire à plus d'un titre et doit figurer dans les bibliothèques de tous les responsables, ingénieurs et techniciens appelés à traiter de la cybersécurité. Dès le premier chapitre, le lecteur, même non spécialiste, prend conscience de la réalité et de l'enjeu de la question. Il montre en quoi le problème des installations industrielles est spécifique et nécessite une réponse appropriée face à des attaques dont l'ampleur et la technicité sont décrites en termes impressionnants : les cyberattaques ne sont plus l'affaire d'étudiants désireux de se singulariser mais d'organisations criminelles internationales qui agissent pour elles-mêmes ou pour compte de tiers : « Hackers for hire » et « Payloads as a service ». Les grandes attaques qui ont émaillé ces dernières années : Stuxtnet, Duqu, Flame, Gauss, Dragonfly… sont décortiquées avec une précision glaçante.

Mais l'industrie n'est pas sans ressources face à ces menaces. L'ouvrage explique de façon très didactique comment la cybersécurité peut être construite autour de mesures organisationnelles et de mesures techniques déterminées à partir d'une analyse de risque minutieuse. Des chapitres très documentés sont consacrés à la sécurisation des réseaux, à la détection des intrusions et, plus généralement, à l'offre technologique en cybersécurité industrielle : systèmes de contrôle d'accès, pare-feu, filtres, systèmes de détection d'intrusion, diodes… en mentionnant les produits aujourd'hui disponibles sur étagère.

L'ouvrage accorde une large place aux questions liées à la sûreté de fonctionnement et à ses similitudes avec la cybersécurité. Cette analyse est particulièrement intéressante l'amène à comparer l'approche de l'ISA84 (et donc des IEC 62508 et 62511) avec celle de l'ISA99 (IEC 62443). Les convergences mais aussi les différences sont clairement mises en évidence tant au plan des principes qu'au niveau de la mise en œuvre. La conclusion, souvent méconnue, est que si la causalité des dommages potentiels reste fondamentalement différente, les conséquences des atteintes au bon fonctionnement du système revêtent nécessairement un important tronc commun qui doit se retrouver au niveau des analyses de risque. Quant aux solutions, elles ne sont pas nécessairement exclusives et la question de la redondance, par exemple, est discutée avec beaucoup de pertinence.

L'ouvrage aborde la question des référentiels et du corpus normatif. Sa lecture aidera le lecteur à s'y retrouver entre les multiples organismes qui coexistent sur le marché : ISO, IEC, NIST, NERC, etc. Sans contraindre le lecteur à un choix, la pertinence de chaque référentiel au regard du problème à traiter est analysée avec le recul suffisant. L'accent est mis sur l'IEC 62443 (ISA99) qui fait l'objet d'un chapitre particulier. L'IEC 62443 est ainsi présentée comme « présentant une position centrale dans les échanges entre acteurs des SNI (Systèmes numériques industriels). Elle est le seul référentiel à portée internationale avec l'ambition d'être multisectorielle… »

La « Cybersécurité des installations industrielles » apparait in fine comme un ouvrage de référence, incontournable pour les professionnels de la cybersécurité industrielle. Qu'on le lise de façon linéaire ou qu'on y entre de façon ponctuelle sur des sujets choisis, l'ouvrage apparait comme le prolongement idéal de la session de formation proposée par l'ISA-France sur la cybersécurité des installations industrielles (voir le programme de formation de l'ISA-France sur www.isa-france.org).

Il est souhaitable que cet ouvrage fasse l'objet de mise à jour régulière, tant les questions de cybersécurité sont aujourd'hui évolutives. Il faudra en particulier l'enrichir d'un chapitre consacré spécifiquement aux communications sans fil et plus particulièrement aux réseaux de capteurs qui constituent la première implémentation de l'Internet industriel des objets. Il faudra également traiter des perspectives ouvertes par les modules de sécurité, composants cryptographiques matériels inviolables solidaires des équipements, dans lesquels sont stockés tous les éléments, tels que les clés de chiffrement et d'authentification, relatifs à leur sécurité. Une telle approche permettra-t-elle de disposer de composants intrinsèquement sûrs, quelle que soit la robustesse de la protection périphérique à la zone dans laquelle ils seront installés ? Autant de sujets à suivre attentivement

When failure is not an option… par Steve Mustard

A l'occasion du séminaire de Villeurbanne, **Steve Mustard**, President & CEO de National Automation, Inc, expert reconnu dans le domaine de la cybersécurité des installations industrielles, très actif au sein de l'ISA et l'Automation Federation, nous livre ses impressions sur l'absolue nécessité de mener une politique plus active de lutte contre les cyberattaques, en s'appuyant, notamment, sur l'approche de l'IEC 62443. ISA-Flash le remercie vivement de sa contribution.

When failure is not an option

Eur Ing **Steve Mustard**, BEng CEng FIET CAP

National Automation, Inc

Houston, Texas, USA

Abstract

Mission critical operations are heavily dependent on the use of reliable and robust Industrial Automation and Control Systems (IACS). In recent years a number of factors have altered the direction of IACS development and deployment. These include the integration of IACS with business systems, the adoption of commercial and open source products, the increased threat of cybersecurity attack and an aging workforce not being replaced by suitably skilled individuals.

This paper will consider these factors and highlight the tools and resources available to help keep IACS-based operations safe and reliable.

Background

Mission critical operations are heavily dependent on the use of reliable and robust Industrial Automation and Control Systems (IACS). Over the past 50 years these systems have evolved to meet the specific needs of mission critical operators. At the same time, the people involved have developed a broad skill base necessary to maintain the safe and reliable operation of these systems.

In recent years a number of factors have altered the direction of IACS development and deployment:

- The integration of IACS with business systems – demands for access to real time production information require that IACS equipment be connected to IT equipment ;
- The adoption of commercial and open source products – cost pressures and calls for the use of IT-based techniques and services have driven vendors to use commercially available components in their solutions ;
- The increased threat of cybersecurity attack – cybersecurity has traditionally been seen as an IT problem but events over the past 15-20 years show that IACS operations can be severely impacted by such an attack ;
- An aging workforce not being replaced by suitably skilled individuals – the workforce that evolved the current understanding of how IACS needs to work is reaching retiring age. To date there is a shortage of suitable academic and career paths to ensure that the vacancies are filled.

Technology convergence

Industrial Automation and Control Systems (IACS) have always been designed for safe and reliable operation in robust environments. The very first PLC, the MOdular DIgital CONtrol or Modicon, was designed to be rugged with no on/off switch, fans or any other moving parts [1]. Over time, PLCs and other IACS components have evolved to provide increased reliability, resilience and functionality through the use of specific designs and parts. A rugged controller, for example, might have a specialist real-time operating system such as QNX and may run on a higher-specification processor designed to operate at environmental extremes of temperature, vibration and shock. Once installed this equipment would be expected to run unattended for 10 years or more.

With IT products, standardization of core components such as the Windows operating system together with widespread adoption has driven costs down. It is very common for IACS equipment to be used for over a decade or more. IT equipment however, is typically replaced every 2 to 3 years. High availability and rugged operation are not key factors in IT system design.

As IT equipment costs have reduced and functionality has increased, the adoption of IT-standard components in IACS was inevitable. This adoption has been driven by three key factors:

- Lower cost of ownership ;
- Familiarity and ease of use ;
- Ease of integration with business systems.

The cost for vendors to design, develop and maintain specialist equipment for decades is very high. There are significant cost reductions from the use of standardized

components. In addition, as the workforce has become more familiar with IT it is easier for users to learn to use IACS equipment based on similar products. Using standard components provides access to protocols and services that makes the integration of IACS with business systems easier.

The need for product certification

The adoption of IT-standard components has created new issues for IACS users. Consider the following examples:

- As various IACS product vendors incorporated complete Web servers to enable diagnostics, remote access and other features, they incorporated core libraries such as OpenSSL, even if these were not required. In 2014, a vulnerability in OpenSSL known as "Heartbleed" was identified. Few IACS users would have thought that their systems were vulnerable to an issue that allowed users to bypass encryption protection and get access to confidential information such as usernames and passwords [2].
- A relatively new SCADA system vendor actively promotes the fact that their product is built around Java, despite the fact that Java is known to be a major security risk. A serious security vulnerability was discovered early in 2013 resulting in the US Department of Homeland Security (DHS) advising users to disable Java in their web browsers. In addition to the introduction of security vulnerabilities from Java, the ability to rapidly deploy new SCADA applications in the user environment through the Java environment creates a major change control issue.

The advent of the Industrial Internet of Things (IIoT) will only exacerbate this problem. Vendors with less experience in IACS development will be producing products using IT-standard components and mission critical operators will need to be much more careful about the choices they make.

The development of compliance laboratories specializing in IACS certification is essential if mission critical operators are going to be able to procure the right products. ISASecure is a conformance certification program run by the ISA Security Compliance Institute (ISCI). ISASecure independently certifies IACS products and systems against ISA/IEC62443 to ensure that they are robust against network attacks and free from known vulnerabilities. ISCI also offers an ISASecure organization process certification for product development organizations [3].

Cybersecurity threats

In 2005, reports indicated a 10-fold increase in the number of successful cyber-attacks on infrastructure control systems since 2000 [4]. By 2015, reports indicated a 100 % increase in attacks on IACS installations in 2014 compared with the previous year [5].

The increased connectivity to the business environment already discussed has exposed new vulnerabilities that can be targeted by attackers. The connection between industrial (or Operational Technology – OT) and IT systems has created problems for both types of systems. For instance:

- In one of the biggest data breaches to date, over 40 million target customers had their information including credit card details compromised. This incident was found to have originated through the HVAC vendor's network [6].
- In Germany in December 2014, a steel mill was attacked and the blast furnace suffered major damage. The origin of the attack was the business network from where the attackers were able to navigate to the control system network and disrupt the emergency shutdown systems that are designed to prevent major damage to plant [7].

ISA/IEC62443, the international standard for Industrial Automation and Control Systems Security, provides details of the recommended cybersecurity mitigations for IACS implementations [8]. This standard is referenced extensively throughout the US NIST Cybersecurity Framework [9]. This framework is a higher-level outline document designed to help mission critical organizations define and manage their cybersecurity management program.

Although these cybersecurity standards and frameworks exist, mission critical operators have been slow to adopt

them. These organizations have made a significant investment to embrace the necessary occupational safety culture needed to avoid repeats of the Piper Alpha [10] and Texas City [11] disasters. In contrast, recognition that cybersecurity is a major driver in process safety is still lacking in many places. For example:

- If a worker in refinery were to walk upstairs without holding the handrail, he would be stopped and the incident could be reported as a near miss. However, if the same worker were to put a USB drive in an IACS workstation without running a virus scan, there is a high likelihood that he would not be stopped and it would not be seen as a near miss.
- Change control in many mission critical organizations have not been updated to take into account the effect of any changes to cybersecurity. As a result, a change can be made that introduces new vulnerabilities without appropriate mitigating or compensating controls being applied. This problem is exacerbated by the rapidly changing technology already noted above.

Threats from remote and mobile access

Another major cybersecurity factor is the increase in the use of remote and mobile access in IACS installations. By providing internal technicians and external product vendors with full access to systems to allow them to diagnose and resolve issues, a faster response should be achieved. In addition there can be a lower risk to personnel, for example, remote working avoids the need for a helicopter transfer to an offshore platform.

However, providing this full access to systems creates significant new vulnerabilities:

- It may be possible to obtain credentials and access the systems from an unauthorized device. This is a particular problem if the remote access is performed over a public Wi-Fi network;
- If a device is lost or stolen it may be possible to use this to gain access ;
- An increased reliance on firewall configuration to secure the IACS system often managed by business IT ;
- Anecdotal evidence suggests that more weight is placed on the ability to respond quickly rather than safely ;
- Mission critical organizations support their technicians accessing IACS equipment whilst on vacation in locations such as Las Vegas ;
- Routine changes are made to IACS equipment from remote locations such as central offices, home, or even whilst traveling.

The risks of an incident caused by impaired decision-making or poor communications should far outweigh the benefits of a rapid response.

Remote and mobile access to IACS environments needs careful consideration and a thorough risk assessment process. The North American Electric Reliability Corporation (NERC) develops and enforces compliance with mandatory

reliability standards for the US electricity sector. V5 of their standard [12], slated for legislation in 2016, includes a requirement, part of the Electronic Access Control (EAC) R2.1. which "denies [remote] access by default".

Fault tolerance: the expectations and the reality

IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Systems* [13] and IEC 61511, *Functional safety - Safety instrumented systems for the process industry sector* [14] both provide extensive details on how to design components and systems that form part of IACS environments. These use Safety Integrity Levels (SIL) to quantify the safety demands on those components and systems.

It is well understood that the major difference between IT systems and OT systems is the relative order of priorities: In IT systems confidentiality is the main concern, however, in OT systems availability is the priority. What is often overlooked in this philosophical detail is that availability is of paramount importance because the failure of these systems can affect the safety of personnel, the public and the environment. In addition, system unavailability can impact production, a major financial issue for many mission critical businesses.

As previously mentioned, the move towards the use of standard components has created a challenge. When using standard components, the system developers may not have access to the features necessary to implement a truly rigorous design. Even if they do, the sheer volume of code that may be provided by default in these standard components may make exhaustive test and validation difficult, if not impossible.

For example, despite the need to follow rigorous aviation design and development standards, Boeing has had numerous problems with its 787 Dreamliner. One of these problems resulted in an Airworthiness Directive (AD) from the US FAA instructing Boeing to perform a repetitive maintenance task on all 787 airplanes [15]. This AD addressed an issue where the airplane would lose all AC power due to the Generator Control Units going into failsafe mode after 248 days of continuous operation. This issue was a result of a programming error where a register was incorrectly sized.

There are many similar programming error examples in IACS components, some of which have been formally identified and some of which have been fixed by vendors. However, deployment of a vendor fix to an IACS component is generally much more challenging than with IT components and so it is often the case that these vulnerabilities continue to exist in many mission critical facilities. In December 2013 researchers identified three major vulnerabilities in a SCADA product used in an estimated 7,600 facilities worldwide [16]. By March 2014 the vendor issued advice to its customers "to immediately update to the latest version of the application … and patching it to resolve the vulnerabilities" but there is no requirement for the end users to do this. In many cases such an update may require a shutdown of the facility and it may not be possible to schedule this for many months, or even years.

A shortage of skilled professionals

There is an acute shortage of suitably qualified and experienced individuals to work in mission critical systems design and operation. If we are to keep our businesses, and our national critical infrastructure safe, we will need a new generation of specialists who understand the importance of the phrase ***"failure is not an option".*** Coupled with the technology changes already discussed, this presents a real risk to the future of reliable and safe mission critical operations.

The National Consortium for Mission Critical Operations (NCMCO) strives to be a national center of excellence and an ambassador for the mission critical operations field [17]. The NCMCO was awarded a $23 million federal grant in 2013 to fund two-year degree programs in "Mission Critical Operations" at four North Carolina colleges and one college in Georgia. As part of the program, the International Society of Automation (ISA) has been tasked with creating a new Certified Mission-Critical Professional (CMCP) certification program that will test graduates based on the skills and body of knowledge taught through the Mission Critical Operations curriculum and degree programs [18]. The program is available starting in September 2015, with a target to offer the program's first graduates in 2017.

The Automation Federation (AF) is an association of member organizations with the same goal of promoting the profession of automation around the world. The AF has worked with the US Department of Labor to produce an

Automation Competency Model (ACM) [19]. This model is to help:

- Identify specific employer skill needs ;
- Develop competency-based curricula and training requirements ;
- Develop industry-defined performance indicators, skill standards, and certifications ;
- Develop resources for career exploration and guidance.

It will take several years for the first generation of mission critical professionals to complete their training but organizations such as AF and NCMCO are working to close the gap and increase the availability of suitably skilled individuals.

Conclusion

Mission critical operations are heavily dependent on the use of reliable and robust Industrial Automation and Control Systems (IACS). In recent years a number of factors have altered the direction of IACS development and deployment. The result is a significant number of concerns that mission critical operators must address if they are to continue to have safe and reliable systems:

- The integration of IACS with the business environment creates new vulnerabilities that must be mitigated ;
- The use of IT-standard components introduces IT-standard risks that may be difficult to mitigate in an OT environment ;
- There is demand for mobile and remote access with insufficient consideration of the risks this creates ;
- There are a wide number of cybersecurity and safety standards that have been introduced to provide guidance and to assist with securing IACS. The adoption and use of these standards is not always consistent or comprehensive leading to potentially serious vulnerabilities in mission critical components ;
- The use of commercial standard components makes product validation more difficult due to the increased scope and complexity of the components ;
- The use of open source products allows for the introduction of code and associated vulnerabilities that should not be present in IACS environments ;
- The loss of experienced personnel due to retirement, and the lack of suitably trained replacements will leave a knowledge gap that will take time to fill.

To address these concerns mission critical operators need to:

- Rigorously apply all relevant standards ;
- Make cybersecurity a part of their operational culture ;
- Demand third party certification of products ;
- Adopt competency models as a means to assess and develop personnel.

Failure is not an option: mission critical operators must take action

Acknowledgements

The author wishes to thank **David Boyle**, who provided valuable comments and ideas to this paper.

About the author

Steve Mustard is a process control consultant with over 25 years experience in wide variety of areas such as embedded systems, military applications and remote monitoring and control of energy and utility, manufacturing and transport systems. He is a UK registered Chartered Engineer (CEng), a European registered engineer (Eur Ing) and an ISA Certified Automation Professional (CAP). He is the former chairman of the Institution of Engineering and Technology's (IET) Americas Regional Board and is a current member of the Automation Federation's (AF) Government Relations Committee. He can be contacted at steve.mustard@au2mation.com

References

[1] Ernie Hayden, *An Abbreviated History of Automation & Industrial Controls System and Cybersecurity* (SANS Institute, 22 January 2015). https://www.sans.org/reading-room/whitepapers/physical/abbreviated-history-automation-industrial-controls-system-cybersecurity-35697

[2] Chris Bronk, *What Heartbleed means for critical infrastructure* (Forbes, April 23 2014). http://www.forbes.com/sites/thebakersinstitute/2014/04/23/what-heartbleed-means-for-critical-infrastructure-2/

[3] ISASecure. http://www.isasecure.org/en-US/Certification

[4] E.J. Byres and J. Lowe, *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems* (ISA, October 2004). https://www.tofinosecurity.com/professional/myths-and-facts-behind-cyber-security-risks-industrial-control-systems

[5] Dell, *2015 Dell Security Annual Threat Report*, (Dell). https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf

[6] Brian Krebs, *Target Hackers Broke in Via HVAC Company* (Krebs On Security, February 2014) http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[7] BBC, *Hack attack causes massive damage at steel works* (BBC, 22 December 2014). http://www.bbc.com/news/technology-30575104

[8] ISA/IEC62443, ISA. https://www.isa.org/isa99/

[9] NIST Cybersecurity Framework, NIST. http://www.nist.gov/cyberframework/

[10] Terry Macalister, *Piper Alpha disaster: how 167 oil rig workers died* (The Guardian, 4 July 2013). http://www.theguardian.com/business/2013/jul/04/piper-alpha-disaster-167-oil-rig

[11] Daniel Schorn, *The Explosion at Texas City - 2005 Refinery Explosion In Texas Killed 15, Injured 170* (CBS News, October 26 2006). http://www.cbsnews.com/news/the-explosion-at-texas-city/

[12] NERC, *NERC CIP Cyber Security – Electronic Security Perimeter(s)* (NERC, NERC-CIP-005-3a)

[13] Functional Safety and IEC 61508, International Electrotechnical Commission. http://www.iec.ch/functionalsafety/

[14] ARC Advisory Group, *Reduce Risk with a State-of-the-Art Safety Instrumented System* (ARC Advisory Group, September 2004). http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Articles/ARCWhitePaper/Reduce-Risk-with-a-State-of-the-Art-Safety-Instrumented-System.pdf

[15] Samuel Gibbs, *US Aviation Authority: Boeing 787 bug could cause 'loss of control'* (The Guardian, 1 May 2015). http://www.theguardian.com/business/2015/may/01/us-aviation-authority-boeing-787-dreamliner-bug-could-cause-loss-of-control

[16] Pierluigi Paganini, *Nearly 7600 critical infrastructure vulnerable to bugs in Yokogawa App* (Security Affairs, March 16 2014). http://securityaffairs.co/wordpress/23085/security/7600-yokogawa-scada-application-vulnerable.html

[17] About NCMCO. http://ncmco.us/about/

[18] ISA, *ISA to Develop a New Certification Program as part of a $23 million grant to fund degree programs and prepare workers for careers in "Mission Critical Operations"* (ISA, 10 December 2013). https://www.isa.org//news-and-press-releases/2014/january-2014/isa-new-certification-program-23m-grant-fund-degree-programs-careers-in-mission-critical-operations

[19] Automation Federation, *Automation Competency Model is First Complete U.S. DOL Produced Competency Model* (Automation Federation, 30 April 2009). http://www.automationfederation.org/AFTemplate.cfm?Section=Press_Room5&template=/ContentManagement/ContentDisplay.cfm&ContentID=76163

Sommaire | Evénements | Standards | Technologie | Formation

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	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	16 octobre 2015 18 décembre 2015
JVI1	**ISA-88 : Conception fonctionnelle automatismes et contrôle des procédés industriels - Deux jours**	**Fontainebleau**	5 et 6 octobre 2015 7 et 8 décembre 2015

JVI2	ISA-95 : Conception fonctionnelle et interopérabilité MES/MOM - Deux jours	Fontainebleau	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	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	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	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	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 au format Word

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
Direction de la publication : Jean-Pierre Hauet – ISA-France – Siège social : 17 rue Hamelin – 75016 Paris
Adresse postale : Chez KB Intelligence - 10 rue Lionel Terray 92500 Rueil-Malmaison
Tel : 33 1 41 29 05 09 – contact@isa-france.org

Rejoignez-nous sur LinkedIn