

Sommaire

Evénements

Standards

Technologie

Formation

## Au sommaire de ce numéro :

- **Evénements**
  - Le 8 juin 2016 à 11h00 : Assemblée générale d'ISA-France
  - Les 18 et 19 octobre 2016 à Villeurbanne, forum « Sûreté de fonctionnement et cybersécurité »
  - Du 24 au 26 septembre 2016 à Newport (Californie) : l'ISA Fall Meeting
- **Standards** : Gestion des alarmes : une nouvelle version de l'ISA 18.2 par Patrice Noury
- **Technologie**
  - Internet Industriel des objets : MQTT – Jean-Pierre Hauet
- **Formation**
  - Le programme de formation 2016 – Trois nouveaux cours ISA-France

Sommaire

Evénements

Standards

Technologie

Formation

## Le 8 juin 2016 à 11h00 : Assemblée générale d'ISA-France

L'Assemblée générale ordinaire d'ISA-France s'est tenue le mercredi 8 juin à 11h00 à Paris. Une occasion de faire le point sur les thèmes d'actualité en rapport avec le monde de l'instrumentation et des automatismes. **Jean-Pierre Hauet** a été reconduit comme président avec **Bernard Dumortier**, **Jean Vieille** et **Patrice Noury** comme vice-présidents.

## Cybersécurité et sûreté de fonctionnement : comment concilier deux objectifs essentiels de la sécurité industrielle ? 18 et 19 octobre 2016 à Villeurbanne

La sûreté de fonctionnement et la cybersécurité sont aujourd'hui des préoccupations essentielles de l'industrie. L'une et l'autre des disciplines visent à se prémunir contre des risques dont la réalisation peut avoir des conséquences considérables sur le bon fonctionnement de l'entreprise et sur les biens et les personnes. Les deux concepts partagent un certain nombre de points communs fondamentaux, d'importantes différences existent. La sûreté de fonctionnement est une discipline plus ancienne qui bénéficie de nombreux retours d'expérience. Mais la cybersécurité s'affirme quotidiennement comme une préoccupation essentielle à prendre en compte.

### Un rapprochement entre les deux disciplines est nécessaire. Jusqu'où ira-t-il et comment s'y préparer ?

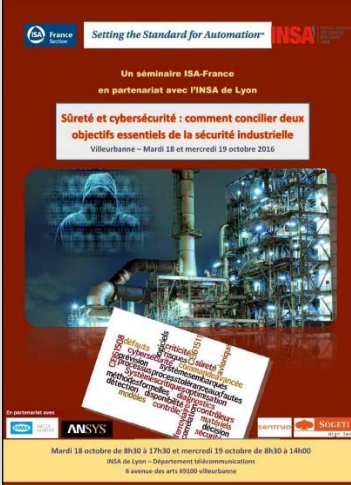
Le Forum des mardi 18 et mercredi 19 octobre organisé par ISA-France en coopération avec l'INSA de Lyon, vise à analyser la problématique des deux approches. Des travaux universitaires sur le sujet seront présentés ainsi que les travaux normatifs actuellement en cours, notamment au sein de l'ISA (ISA99, ISA 84) et de l'IEC. Des cas d'usage et des retours d'expérience de situations réelles où sûreté et cybersécurité sont amenées à coexister, seront discutés, le but étant in fine de mettre en évidence de bonnes pratiques pour une gestion optimisée des risques industriels.

Les inscriptions sont ouvertes sur le site de [l'ISA-France](http://www.isa-france.org).

Télécharger : [programme](#) et [bulletin d'inscription](#)

Inscription et paiement en ligne possibles sur [www.isa-france.org](http://www.isa-france.org)

Renseignements : [contact@isa-france.org](mailto:contact@isa-france.org) Tel : 01 41 29 05 09



Un séminaire ISA-France en partenariat avec l'INSA de Lyon

**Sûreté et cybersécurité : comment concilier deux objectifs essentiels de la sécurité industrielle**

Villeurbanne - Mardi 18 et mercredi 19 octobre 2016

Mardi 18 octobre de 9h30 à 17h30 et mercredi 19 octobre de 9h30 à 14h00  
INSA de Lyon - Département Télécommunications  
8 avenue des arts 69100 Villeurbanne

En partenariat avec

**INSA** INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

**ANSYS**

**HIMA** SAFETY NONSTOP

**SOGETI** High Tech

**sentryo**

## ISA Fall meeting 2016: du 24 au 26 septembre 2016 à Newport (Californie)

L'ISA revient sur la côte Ouest des Etats-Unis pour son grand meeting d'automne qui se tiendra des 24 au 26 septembre à Newport (Californie), au Newport Beach Marriott Resort. De nombreuses réunions sont programmées, en particulier l'Annual Members Assembly and Council of society Delegates qui se tiendra le 25 septembre et la 54th Annual ISA Honors & Awards Reception au cours de laquelle seront remises les prestigieuses distinctions décernées par l'ISA. Chaque membre de l'ISA est invité à participer. Voir [ICI](#) le programme.

[Sommaire](#)[Evénements](#)[Standards](#)[Technologie](#)[Formation](#)

## Gestion des alarmes : une nouvelle version de l'ISA 18.2 – Patrice Noury



Une nouvelle version de la norme ISA 18.2 (gestion des alarmes pour les procédés industriels) – l'ANSI/ISA-18.2-2016, **Management of Alarm Systems for the Process Industries** – vient d'être publiée par l'ISA. Cette nouvelle version, qui se substitue à la version de 2009, répond à deux objectifs : prendre en compte le retour d'expérience depuis la première publication de 2009 et harmoniser le vocabulaire et les concepts avec la norme IEC 62682.

Suite aux 302 commentaires des membres du comité reçus lors de la dernière relecture, 111 étaient éditoriaux, 139 techniques mineurs et 52 techniques majeurs. La plupart des commentaires éditoriaux visaient à améliorer le texte et ont été généralement pris en compte, pour ce qui est des commentaires techniques, seuls cinq commentaires techniques majeurs ont été pris en compte :

- ajout d'un chapitre sur l'interface homme/machine ;
- modifications du caractère obligatoire ou recommandé de certaines dispositions. Certains souhaitant une moindre obligation pour ne pas avoir à modifier des produits existants ;
- autorisation de stocker la documentation des alarmes dans un système séparé du système de gestion des alarmes ;
- suppression de la possibilité pour l'opérateur de modifier les attributs d'une alarme ;
- assouplissement de la distribution des alarmes par priorité et en particulier autoriser plus de 5 % d'alarmes prioritaires (la philosophie des alarmes le précisera).

Cette version apporte une meilleure définition des termes et une exigence plus forte des fonctionnalités pour être conforme à la norme. Par exemple la définition de l'alarme inclut maintenant un terme temporel qui dit que la réponse attendue à un défaut ou défaillance doit être effectuée dans un temps donné (« timely response »).

Pour ce qui est des dispositions exigées de tout système de gestion des alarmes pour être conforme à la norme, le tableau ci-dessous résume les contraintes :

<b>Alarm Philosophy contents</b>	<b>ISA-18.2 (2009)</b>	<b>IEC 62682 (2014)</b>	<b>ISA-18.2(2016)</b>
Objet du système d'alarme	exigé	exigé	exigé
Définitions	exigé	exigé	exigé
Références	recommandé	exigé	recommandé
Rôles et responsabilités	exigé	exigé	exigé
Principes de conception des alarmes	exigé	exigé	exigé
Rationalisation	exigé	exigé	exigé
Définition des classes d'alarmes	exigé	exigé	exigé
Alarmes a haut niveau de gestion	recommandé	recommandé	recommandé
Guide conception de l'IHM	exigé	exigé	exigé
Détermination des seuils d'alarme	recommandé	recommandé	recommandé
Méthode de priorisation	exigé	exigé	exigé
Suivi de la performance du système	exigé	exigé	exigé
Maintenance système d'alarme	exigé	exigé	exigé
Tests des alarmes	exigé	exigé	exigé
Techniques d'alarmes avancées autorisées	recommandé	recommandé	recommandé
Documentation des alarmes	recommandé	recommandé	recommandé
Guide de mise en œuvre	exigé	exigé	exigé
Gestion des modifications	exigé	exigé	exigé
Formation	exigé	exigé	exigé
Conservation de l'historique des alarmes	exigé	exigé	recommandé
Procédure relatives au site	recommandé	recommandé	recommandé
Considérations spécifiques de conception	recommandé	recommandé	recommandé
Audit du système de gestion des alarmes	n/a	exigé	exigé
Guide de conception des alarmes	n/a	n/a	exigé
Procédures de réponses aux alarmes	n/a	n/a	exigé
Consignation des alarmes	n/a	n/a	recommandé

On peut constater l'apparition de nouveaux items :

- l'audit de gestion des alarmes qui constate l'application des procédures de mise en œuvre de la gestion des alarmes ;
- l'existence d'un document guide pour la conception des alarmes ;
- les procédures à suivre pour la réponse aux alarmes, ces procédures étaient auparavant intégrées dans la documentation individuelle des alarmes ;
- la consignation des alarmes pour pouvoir suspendre temporairement une alarme.

La consignation d'une alarme est une fonction nécessaire, issue de l'expérience, pour éliminer une alarme devenue temporairement gênante ou source d'information non pertinente. Elle comporte les éléments fonctionnels suivants :

- possibilité de consigner toute alarme individuellement ;
- visualiser les alarmes consignées ;
- définition d'une durée limite de consignation ;
- contrôle d'accès à la consignation individuelle d'alarme ;
- possibilité de déconsignation ;
- Enregistrement de la consignation / déconsignation.

Lorsque la durée limite est atteinte, l'alarme est automatiquement déconsignée.

#### La normalisation ISA de la gestion des alarmes est constituée de la norme

- ANSI/ISA 18.2-2016 "Management of alarms for the process industry", publiée le 26 avril 2016,

#### et des rapports techniques suivants :

- ISA TR18.2.2-2016 Alarm identification and rationalisation (approbation en mai 2016) ;
- ISA TR18.2.3-2015 Basic alarm design ;
- ISA TR18.2.4-2012 Enhanced and advanced alarms methods ;
- ISA TR18.2.5-2012 Alarm system monitoring assessment and auditing ;
- ISA TR18.2.6-2012 Alarm system for batch and discrete processes

Le rapport ISA TR18 2.1 a été soumis aux commentaires et vote du comité pour le 1<sup>er</sup> août 2016. Ce rapport est important car la définition de la philosophie des alarmes est primordiale pour la mise en œuvre d'une bonne gestion des alarmes.

Il restera un dernier rapport relatif aux sous-systèmes packagés intégrés dans les procédés industriels.

#### Quelques rappels concernant les rapports techniques :

<b>ISA TR18 2.2-2016 « Alarm identification and rationalization</b>	<p>Ce rapport fournit un guide, des bases et des exemples pour mettre en œuvre cette phase du cycle de vie :</p> <ul style="list-style-type: none"> <li>○ <b>Identification</b> : c'est un concept générique pour les différentes méthodes qui peuvent être utilisées pour définir de nouvelles alarmes ou modifier celles existantes. L'étape d'identification est le point d'entrée recommandé du cycle de vie de la gestion des alarmes et permet de fournir une liste de données d'entrée à l'étape rationalisation ;</li> <li>○ <b>Rationalisation</b> : recouvre plusieurs activités, justification de chaque alarme, documentation, priorité et classification. Au niveau de la justification, les alarmes candidates sont confrontées aux critères définis dans la philosophie. Si l'alarme répond à tous ces critères, alors le type d'alarme, le seuil, la cause, la conséquence et l'action opérateur seront documentés. L'alarme est priorisée et classifiée, c'est-à-dire assignée à un groupe ou à une classe imposant des exigences spécifiques. Ces activités sont souvent conduites de façon combinée. Il n'est pas nécessaire de faire des sessions séparées.</li> </ul>
<b>ISA TR18 2.3-2015 « Basic alarm design »</b>	<p>Ce rapport fournit une aide pour mettre en œuvre les concepts définis dans la norme de base. Selon le cycle de vie défini par la norme, il considère que les alarmes ont été identifiées et rationalisées et donc que les attributs tels que seuils et priorité ont été définis.</p>
<b>ISA TR18 2.4-2012 « Enhanced and advanced alarm methods »</b>	<p>Ce rapport aide l'utilisateur à évaluer l'opportunité de les utiliser, les bénéfices possibles et les enjeux et coûts en attendre. Il s'agit de méthodes qui vont au-delà des méthodes initialement prises en compte dans la phase de conception de base. Même si ces méthodes peuvent apporter des améliorations significatives, dans certains cas elles peuvent s'avérer insuffisantes pour répondre aux objectifs définis dans la philosophie des alarmes.</p>

**ISA TR18 2.5-2012 « Alarm system monitoring, assessment and auditing » :**

Ce rapport est un guide pour l'analyse du système d'alarmes pour à la fois le suivi opérationnel, l'évaluation périodique des performances. Suivi, évaluation et audit sont essentiels pour obtenir et maintenir les objectifs de performance du système d'alarmes. Ces activités peuvent permettre des améliorations dans les autres phases du cycle de vie telles que philosophie, rationalisation, conception détaillée, mise en œuvre, exploitation, maintenance et gestion des modifications.

**ISA TR18 2.6-2012, « Alarm systems for batch and discrete Processes » ,**

Ce rapport couvre l'application des principes de gestion du cycle de vie des alarmes à ces procédés. Les principes et techniques décrites sont conçues pour être utilisées dans les systèmes d'alarmes basés sur des automates programmables et des interfaces homme machine numériques. Ce guide aide à identifier et pointer les opportunités de spécification, conception, mise en œuvre et de gestion des alarmes. Il permet aussi de limiter les alarmes gênantes qui peuvent compliquer et même frustrer l'attention de l'opérateur, la compréhension et la réponse à la situation anormale à laquelle il est confronté.

Pour tout renseignement complémentaire : **Patrice Noury** - [patrice.noury@club-internet.fr](mailto:patrice.noury@club-internet.fr)

Sommaire

Evénements

Standards

Technologie

Formation

**Internet Industriel des objets : MQTT – Jean-Pierre Hauet**

L'Internet des objets est aujourd'hui très présent dans les médias. Il ne se passe pas un jour sans qu'un nouvel article ne paraisse sur les vertus supposées de ce concept dont on attend dans le domaine industriel, interopérabilité, flexibilité, productivité, extensibilité, etc. Bien entendu, passées au crible des réalités toutes les annonces de nouveaux produits et de nouvelles technologies ne connaîtront pas l'essor qu'on nous promet. Cependant, il existe des solutions qui s'affirment de jour en jour et parmi celles-ci, nous appelons l'attention de nos lecteurs sur le protocole **MQTT (Message Queuing Telemetry Transport)**.

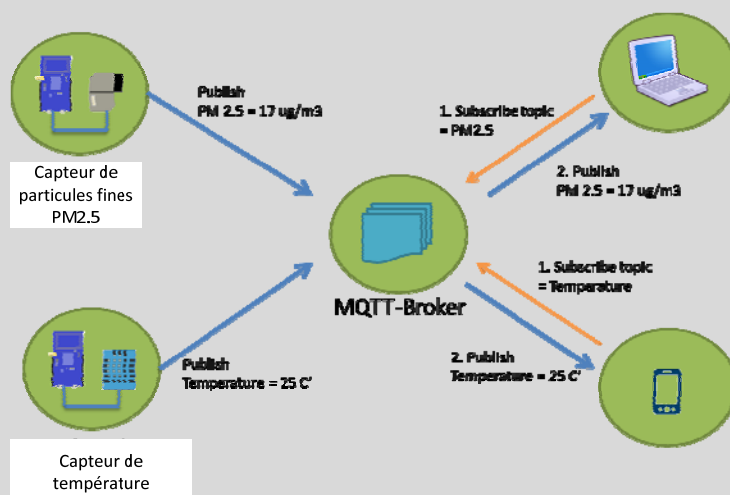
**MQTT** est un protocole de couche application, fonctionnant au-dessus de TCP/IP et destiné à assurer les échanges de données avec des équipements distants, dotés de faibles ressources, ne requérant qu'une bande passante limitée. C'est donc un protocole léger adapté à l'Internet industriel des objets pour des applications de type Scada, lorsqu'il s'agit de communiquer avec des capteurs et des actionneurs sur la base de messages simples.

MQTT fut initialement proposé en 1999 par ses auteurs Andy Stanford-Clark et Arien Nipper mais c'est seulement en 2013 qu'IBM l'a proposé dans sa version 3.1.1 au consortium international OASIS (Advancing open standards for the information society) qui l'a standardisé (<http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html>). Le 15 juin, le standard a été publié par l'ISO/IEC JTC1 sous la référence **ISO/IEC 20922:2016**.

MQTT est un protocole du type Publish/Subscribe (Pub/Sub) dans lequel les données émises par les équipements de terrain sont transférées vers un serveur MQTT (un « broker »), qui les trie, les stocke et les publie en les mettant à la disposition de clients intéressés. Ces clients peuvent être des systèmes Scada ou n'importe quelle autre entité intéressée par certaines données publiées par le broker. Les clients s'abonnent auprès du broker à un service en sélectionnant les types de données qui les intéressent.

Ce découplage entre producteurs des données et consommateurs permet une gestion beaucoup plus efficace du trafic de données et offre davantage de simplicité pour les extensions éventuelles du système.

Plusieurs détails du protocole le rendent particulièrement





attractif pour les applications de contrôle distant de type Scada. Les informations sont transmises au broker par exception et, à la différence des protocoles de polling systématique, seules les données ayant évolué sont transmises. L'entête des trames MQTT est très courte (2 octets) et n'induit pas de frais généraux excessifs. Basé sur TCP, il fonctionne en mode connecté et lorsqu'un équipement perd la connexion, les clients concernés reçoivent automatiquement de la part du broker le « testament » de l'équipement perdu.

MQTT est bidirectionnel ce qui signifie qu'un client peut émettre à destination d'un équipement de bordure une nouvelle donnée. Cette donnée sera lue par cet équipement et l'information du changement de paramétrage sera ensuite mise à la disposition de l'ensemble des clients concernés.

La légèreté du protocole permet d'accroître le nombre de capteurs et de paramètres surveillés, ce qui est typiquement l'un des enjeux de l'IIoT. Les agents, chargés par exemple du service de maintenance, peuvent s'abonner, via leur smartphone, aux services de données qui les concernent. Le broker s'assure de leur accréditation avant de leur donner accès aux données. L'authentification et le chiffrement sont assurés au niveau de la couche transport.

MQTT n'impose pas de modèle de données. Seuls peuvent par conséquent interopérer les clients qui utilisent la même sémantique mais il existe dans la pratique un petit nombre de standards de fait et il est probable que la généralisation de l'utilisation de MQTT va entraîner une convergence vers un modèle unique de données.

MQTT est accessible en logiciel libre avec des brokers tels que Mosquito et RabbitMQ.

MQTT restera en concurrence avec les systèmes de polling classiques. Par ailleurs, d'autres solutions de couche application « cholesterol free » voient le jour pour l'IIoT, notamment CoAP (Constrained application Protocol). Le champ préférentiel d'application de MQTT semble être celui des systèmes à longue distance et faibles ressources. En termes de communication, c'est le domaine des LPWAN (Low Power Wide Area Network) et notamment des solutions d'origine française SIGFOX et LoRA. Cependant ces systèmes de communication ne supportent pas TCP/IP. Ce pourrait donc être, pour les applications industrielles, un atout pour les solutions LPWAN associées aux réseaux cellulaires LTE de 4<sup>e</sup> génération qui ont été standardisées en mars 2016 par le 3GPP : eMTC pour les communications requérant un débit de quelques centaines de kbit/s et NB-IoT pour les systèmes pouvant se contenter de quelques dizaines de kbit/s mais offrant alors une durée très longue d'autonomie.

Pour approfondir le sujet, suivez la nouvelle session de formation ISA-France : **L'Internet industriel des objets - Les futures architectures de systèmes d'automatisme et de contrôle** (voir ci-dessous)

Pour plus d'informations : Jean-Pierre Hauet – [contact@isa-france.org](mailto:contact@isa-france.org)

[Sommaire](#)[Evénements](#)[Standards](#)[Technologie](#)[Formation](#)

## Trois nouveaux cours ISA-France en 2016

### **Théorie et pratique de la maîtrise des risques des systèmes techniques – IEC 61508**

Ce cours permet d'acquérir les bases pratiques et théoriques nécessaires à la compréhension du contexte technique de la maîtrise des risques des systèmes industriels.

À l'issue du cours, les stagiaires sont en mesure de discuter les modalités de l'application d'un référentiel de sécurité aux cas concrets qu'ils peuvent rencontrer.

- **Premier jour** : sensibilisation au domaine, éléments de réglementation par domaine, terminologie et définition, management et cycle de vie de la sécurité, composantes du risque, performances des systèmes, intégrité du cycle de développement
- **Deuxième jour** : structuration de projet, documentation, analyse du risque, spécifications régissant la sécurité, spécification et réalisation du matériel, spécification et réalisation du logiciel
- **Troisième jour** : calcul et évaluation des systèmes, validation du matériel et des logiciels, phase installation, phase exploitation, phase maintenance

**Cours sur deux jours (Ref BRI3) - Instructeur : Bertrand Ricque**

## L'Internet industriel des objets - Les futures architectures de systèmes d'automatisme et de contrôle

L'Internet Industriel des objets fait partie du buzz technico-commercial actuel. Mais que signifie-t-il exactement ? Quels changements, voire quels bouleversements, entraînera-t-il dans les architectures d'automatisme et de contrôle ?

Le cours ISAF JPH4 (2 jours) permet de :

- Comprendre l'enjeu de l'Internet industriel des objets (IIoT) dans l'usine du futur (Industrie 4.0) pour une meilleure efficacité et une meilleure productivité
- Comprendre les évolutions dans l'architecture des systèmes qu'implique la généralisation de l'approche IP, tant au niveau local qu'au niveau des grandes distances
- Se familiariser avec les principales briques technologiques qui sous-tendent l'IIoT et avec leur impact opérationnel
  - Les architectures IP de l'IIoT (cloud, LLN) et les principaux protocoles d'adaptation de l'Internet (CoAP, 6LowPAN, 6Tisch, etc.)
  - L'enjeu des radiocommunications et les principales solutions (IEEE802.15.4, ZigBee, ISA100, WirelessHart, Thread, Wi-Fi ah, LoRA, SIGFOX...)
  - Les réseaux de capteurs – Le problème de l'alimentation en énergie
  - La cybersécurité aux différents niveaux

**Cours sur deux jours (Ref JPH4) - Instructeur : Jean-Pierre Hauet**

## La transformation digitale des systèmes industriels

Industrie 4.0, Smart Manufacturing, Industrie du Futur... ces initiatives marketing ou politiques sont révélatrices du besoin d'évolution des entreprises industrielles et tout particulièrement de la mise à profit des technologies de l'information. Au-delà des modes, l'entreprise doit sans cesse s'adapter, se transformer pour répondre aux exigences de son environnement, rester en vie, améliorer ses performances. L'informatique industrielle (MES) est particulièrement concernée alors que sa complexité et la criticité de son rôle opérationnel rendent les projets de transformation difficiles et risqués.

Le processus de transformation permanente étudié dans ce cours vise à prévenir ces difficultés tout en améliorant l'alignement métier dans une perspective de performance globale incluant la responsabilité des allocations budgétaires.

**Cours sur un jour (Ref JV17) - Instructeur Jean Vieille**

Code	Désignation	Calendrier 2016	
		Lieu	Date
<a href="#"><u>JPH1</u></a>	<b>L'IEC 62734 (ISA-100) et les applications nouvelles des radiocommunications dans l'industrie - Deux jours</b>	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	3 et 4 octobre 2016 28 et 29 novembre 2016
<a href="#"><u>JPH3</u></a>	<b>La norme ISA/IEC 62443 (ISA-99) et la cybersécurité des systèmes de contrôle - Un jour</b>	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	5 octobre 2016 30 novembre 2016
<a href="#"><u>JPH4</u></a>	<b>L'Internet industriel des objets - Les futures architectures de systèmes d'automatisme et de contrôle</b>	Rueil-Malmaison KB Intelligence 10, rue Lionel TERRAY	10 et 11 octobre 2016 5 et 6 décembre 2016
<a href="#"><u>JVI1</u></a>	<b>ISA-88 : Conception fonctionnelle du contrôle des procédés industriels - Deux jours</b>	Fontainebleau	3 et 4 octobre 2016 5 et 6 décembre 2016
<a href="#"><u>JVI2</u></a>	<b>ISA-95 : Conception fonctionnelle et interopérabilité MES/MOM - Deux jours</b>	Fontainebleau	5 et 6 octobre 2016 7 et 8 décembre 2016
<a href="#"><u>JVI7</u></a>	<b>Transformation digitale des systèmes industriels – Un jour</b>	Fontainebleau	7 octobre 2016 9 décembre 2016

<b><u><a href="#">PNO1</a></u></b>	<b>ISA-18.2 - Gestion d'alarmes : un outil efficace au service de l'opérateur - Un jour</b>	<b>Rueil-Malmaison</b> KB Intelligence 10, rue Lionel TERRAY	20 septembre 2016 13 décembre 2016
<b><u><a href="#">BRI1</a></u></b>	<b>ISA-84 - Sûreté de fonctionnement avec les normes IEC 61508 et IEC 61511- Deux jours</b>	<b>Rueil-Malmaison</b> KB Intelligence 10, rue Lionel TERRAY	22 et 23 septembre 2016 24 et 25 novembre 2016
<b><u><a href="#">BRI2</a></u></b>	<b>Modélisations et calculs de fiabilité pour IEC 61508/IEC 61511/S84 – Un jour</b>	<b>Rueil-Malmaison</b> KB Intelligence 10, rue Lionel TERRAY	21 septembre 2016 23 novembre 2016
<b><u><a href="#">BRI3</a></u></b>	<b>Développement d'applications de sécurité IEC 61508 / IEC 61511 / ISA-84 – Trois jours</b>	<b>Rueil-Malmaison</b> KB Intelligence 10, rue Lionel TERRAY	12 - 14 septembre 2016 14 - 16 novembre 2016

**ISA-France** est reconnue comme un organisme indépendant et qualifié de formation des ingénieurs et techniciens du monde de l'automatisation 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'automatisation : 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](http://www.isa.org) ou d'organiser des sessions de formation intra-entreprises (Prendre contact avec ISA-France sur [contact@isa-france.org](mailto: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](mailto: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](http://www.isa-france.org) et [www.isa.org](http://www.isa.org)

Pour toute demande de renseignements : Tel +33 1 41 29 05 09 ou [contact@isa-france.org](mailto: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](mailto:contact@isa-france.org)

Rejoignez-nous sur 