

Un séminaire ISA-France

en partenariat avec le laboratoire G-SCOP de l'Université Grenoble-Alpes

**Cybersécurité de l'industrie, des infrastructures, des bâtiments...  
Nouvelles vulnérabilités, nouvelles attaques, nouvelles solutions**

Grenoble – Mardi 30 et mercredi 31 janvier 2018



En partenariat avec



Mardi 30 janvier de 9 h à 17 h 30 et mercredi 31 janvier de 9 h à 14 h 30

INP Grenoble – Amphithéâtre Gosse  
46 avenue Félix Viallet - 38000 Grenoble

## Energie, industrie, infrastructures, bâtiments...

### Rançongiciels, DDoS, sabotage...

## Nouvelles vulnérabilités, nouvelles attaques, nouvelles solutions

Les deux dernières années ont vu une recrudescence des cyberattaques de grande ampleur. Après les attaques contre les réseaux électriques ukrainiens de décembre 2015 et 2016, ce sont les attaques en déni de service distribué, via la prise de contrôle de milliers d'objets connectés, qui ont fait l'actualité. Dans le même temps, la preuve était apportée de la vulnérabilité d'objets aussi élémentaires que les ampoules connectées et de nouvelles menaces sont apparues : DoS (Denial of Sleep), DoWF (Denial of Wi-Fi)...

L'année 2017 est marquée par l'arrivée massive des rançongiciels, notamment ceux basés sur EternalBlue qui exploite une faille de Windows (Wannacry, Petya, NotPetya...), occasionnant des arrêts de production significatifs dans de grandes sociétés, avec des objectifs variés : crapuleux, politiques...

Le développement de l'Internet des objets et de ses versions industrielles ouvre la voie à de nouvelles menaces. Pour y faire face, les méthodes de prévention et de protection mises au point dans le cadre traditionnel et répondant notamment aux standards ISO 2700x ou ISA/IEC 62443 permettent de réduire certains risques mais devront être complétées par des contre-mesures adaptées.

**Le séminaire des 30 et 31 janvier 2018 de l'ISA-France, organisé avec le Laboratoire G-SCOP de l'Université Grenoble-Alpes, répond à trois objectifs :**

- I. Expliciter l'origine et le déroulement des attaques survenues ces deux dernières années et analyser les vulnérabilités nouvelles liées au développement de l'Internet des objets, dans les domaines de l'industrie, des infrastructures, des transports et de la gestion des bâtiments ;
- II. Analyser dans quelle mesure le respect des standards actuels tels que l'ISA/IEC 62443 permet de réduire les risques
- III. Montrer comment des approches nouvelles, objets « Secure by Design », systèmes de détection d'intrusion comportementaux, sécurisation des logiciels... permettent de réduire encore davantage la probabilité de voir la menace se matérialiser.

Le séminaire ISA-France est destiné à éclairer les utilisateurs potentiels mais aussi, comme les précédents, à promouvoir les liens entre Université et Industrie.

**Des conventions de formation peuvent être établies sur demande. ISA-France est un organisme de formation enregistré sous le numéro 11754084175.#**

L'ISA, *International Society of Automation* ([www.isa.org](http://www.isa.org)) compte plus de 30 000 membres dans le monde. Sa mission est de promouvoir les techniques et de faire progresser les compétences de ses membres dans les secteurs de l'Instrumentation, des Systèmes et de l'Automation.

ISA-France ([www.isa-france.org](http://www.isa-france.org)) est une association loi de 1901 correspondante de l'ISA en France. Elle offre à ses adhérents l'accès à un réseau relationnel international, des moyens de formation et d'échanges au travers de ses publications et de ses manifestations. Elle est enregistrée comme organisme de formation.



En partenariat avec



## Cybersécurité de l'industrie, des infrastructures, des bâtiments... Nouvelles vulnérabilités, nouvelles attaques, nouvelles solutions



### Programme du mardi 30 janvier 2018

08h45– 09h15



Accueil et enregistrement

09h15 – 09h30

#### Allocutions d'ouverture

Jean-Pierre Hauet – Président – ISA-France

Jean-Marie Flaus – Professeur – Laboratoire G-Scop – Université Grenoble-Alpes

### Panorama général

09h30 – 10h30

**Panorama des attaques cyberattaques récentes et enseignements à en tirer – Hervé Schauer –**  
Co-animateur du groupe de travail cybersécurité des systèmes industriels du CLUSIF

**La norme ISA/IEC 62443 : avancement et extensions nouvelles – Jean-Pierre Hauet – ISA-France**

10h30 – 11h00



Pause

### Nouvelles méthodes d'analyse et de protection

11h00-12h30

**Comment assurer la transformation numérique des entreprises en intégrant des dispositifs renforcés de cybersécurité ? – Eric Dubois - ABB**

**Une nouvelle approche pour les analyses de risques associant sûreté et sécurité des systèmes de contrôle – Houssein Abdo – G-SCOP**

**Safe & Secure OPC-UA pour l'IIoT – Christophe Métayer - Systemel**

12h30-14h00



Déjeuner

14h00 – 15h30

**A Gold Standard for Industrial Control System Security – Waterfall**

**Pains and Gains of cyber security certification – Stefan Ditting, Hervé Bodinier – HIMA**

**Comment mettre en place une cartographie des risques cybers consolidée ? – Orion Ragozin – SI-nerGIE**

15h30 – 16h00



Pause

16h00 – 17h45

**Jean-Christophe Mathieu – Siemens**

**Intégration de secure elements dans les objets – Dr Thierry Fensch – ST Microelectronics**

**Génération de scénarios d'attaque contre les systèmes industriels – Maxime Puys – VERIMAG**

**Discussion générale et fin de la première journée**



## Programme du mercredi 31 janvier 2018

08h30 – 09h00



Accueil du deuxième jour

### La détection d'intrusions

09h00 – 10h30

Revue des différentes approches pour les systèmes de détection d'intrusion (IDS) pour les systèmes de contrôle industriels : des approches classiques aux approches par machine learning – Jean-Marie Flaus – G-SCOP

Détection d'intrusion dans les réseaux industriels par modélisation de la normalité et détection d'anomalie – Jean-Christophe Testud – Sentyro

Approche par filtre basée sur la distance aux états critiques pour la sécurisation des systèmes cyber-physiques face aux cyberattaques – Franck Sicard – G-SCOP

10h30 – 11h00



Pause

### Internet industriel des objets et transports

11h00 – 12h30

Quel avenir pour la voiture connectée ? – Medhi Boucherak - Sogeti

Comment modéliser des attaques sophistiquées ? – Jean Caire - RATP

La sécurité de l'internet des objets dans les infrastructures critiques – CoESSI – Hocine Ameur

12h30 – 14h00



Déjeuner – Fin de la conférence

Bulletin d'inscription téléchargeable sur [www.isa-france.org](http://www.isa-france.org)

Convention de formation sur demande (ISA-France est un organisme déclaré sous le N°11 75 408 41 75)



## Plan d'accès

### Localisation des journées

#### INP Grenoble

Mardi 30 janvier et  
mercredi 31 janvier

Amphithéâtre Gosse  
46 avenue Félix Viallet  
38000 Grenoble

[Google Map](#)

### Informations et contacts

**ISA-France**  
Anne Jean-Jarry  
10 rue Lionel Terray  
92500 – Rueil-Malmaison  
Tél : + 33 1 41 29 05 05  
[contact@isa-france.org](mailto:contact@isa-france.org)

**Laboratoire G-Scop**  
**Université Grenoble-Alpes**  
Professeur Jean-Marie Flaus  
46 avenue Félix Viallet, F-38031  
Grenoble cedex 1  
Tel.: (33) 4 76 82 62 29

