

# Proposal for Workshop/Tutorial at IEEE CASE 2021

## Goal:

This workshop is intended to gather research scientists, engineers and practitioners, related to the cybersecurity of Industrial Control Systems (ICSs) with an automation vision. Since the beginning of the century, Industrial Control Systems are integrating information and communication technology to improve the performance of industrial plants. Beyond the performance improvement, this integration has led control systems to be vulnerable as much as Information Technology (IT) systems. This new challenge has attracted the attention of the automation community. The goal of this workshop is to exchange the recent advances in academic and industry for securing the ICSs with an automation vision. Based on talks from industrials and academia, the following topics will be discussed:

*Begining of the workshop: 9h00*

*Welcome/Introduction (9h00 – 9h25)*

- **How do the threats to cybersecurity have changed over time in Industrial Control Systems?**

Speaker : - Pr. Eric Zamaï, INSA Lyon, Laboratoire Ampère

*Demonstration of cyberattacks (9h30 – 10h30)*

- **Demonstration of cyberattacks on a small-scale manufacturing system**

Speaker : - M. Bertrand Felix, La Ruche Industrielle

- M. Simon Navizet, Volvo Group

- Dr. Cédric Escudero, INSA Lyon, Laboratoire Ampère

*Coffee break (10h30 – 11h00)*

*Session 1 (20min of presentation+10min of questions/answers) (11h00 – 12h30)*

- **Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics.**

11h00 – 11h30: Dr. Frank Sicard, Naval Group : « Feedback of integrators and end users »

11h30 – 12h30: Actemium group

*Lunch (12h30 – 14h00)*

*Session 2 (20min of presentation+10min of questions/answers) (14h00 – 15h30)*

- **Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics.**

14h00 – 14h30: M. Riccardo Colelli, Universita Degli Studi Roma Tre : «Deep Packet Inspection approach – Securing ICS devices»

14h30 – 15h00: Dr. Michelle Chong, Control Systems Technology at Eindhoven University of Technology (TU/e): «Secure state estimation for control systems under sensor attacks»

*Coffee break (15h30 – 16h00)*

16h00 – 16h30: Dr. Cédric Escudero, INSA Lyon, Laboratoire Ampère: « Constraining control

signals to protect control systems against stealthy aging attacks»

16h30 – 17h00: Dr. David Espes, Université de Bretagne Occidentale, Laboratoire Lab-STICC:

« coming soon »

*Round table (17h00 – 18h00)*

- **Education for cybersecurity: what are the trends and needs of ICS cybersecurity for the industry? (table ronde)**

Participants: M. Bertrand Felix, La Ruche Industrielle

M. Simon Navizet, Volvo Group

Dr. Franck Sicard, Naval Group

Pr. Eric Zamaï, INSA Lyon, Laboratoire Ampère

Dr. Cédric Escudero, INSA Lyon, Laboratoire Ampère

M. Amaury Beaudet, INSA Lyon, Laboratoire Ampère

M. Riccardo Colelli, Università Degli Studi Roma Tre

Dr. Michelle Chong, Eindhoven University of Technology (TU/e)

Dr. David Espes, Université de Bretagne Occidentale, Laboratoire Lab-STICC

Keywords: Cybersecurity in automation systems, Intrusion Detection Systems, Model-based detection, Model-based prevention, Cyber physical production systems and industry 4.0, Networked control systems, Machine learning and artificial intelligence, Cybersecurity in transportation systems, Autonomous systems, Power and energy system automation, Smart factories, Smart automation in construction and manufacturing

Time	Instance of schedule
08:15	Welcome reception
09:00	<b>How do the threats to cybersecurity have changed over time in Industrial Control Systems?</b>
9:30	<b>Demonstration of cyberattacks</b>
10:30	Coffee Break
11:00	<b>Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics (Session 1)</b>
12:30	Lunch
14:00	<b>Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics (Session 2)</b>
15:30	Coffee break
17:00	<b>Education for cybersecurity: what are the trends and needs of ICS cybersecurity for the industry?</b>
18:00	End of the workshop