# WS4 at IEEE CASE 2021
# “Cybersecurity in Industrial Control Systems with an automation perspective: advances in academia and industry”

**Abstract:**

Since the beginning of the century, Industrial Control Systems (ICSs) have received a lot of attention in academics and industry. The integration of information and communication technology in the control of physical systems is commonly admitted as a requirement to improve the performance of industrial plants. Therefore, controllers, sensors and actuators are nowadays embedded in computer-based systems, and legacy communication systems have been progressively replaced by network-based systems (e.g. ASI, Profibus, Modbus TCP/IP). Nevertheless, this integration increases the vulnerability of control systems. Therefore, ICSs are now exposed to cyberattacks leveraging the use of information and communication technology to alter the behavior of the physical system. Well-known cyberattacks examples are the Stuxnet malware on a uranium enrichment plant in 2010, the Crash Override malware on the Ukrainian power grid in 2015, the Triton malware on a petrochemical facility in 2018, or recently on water treatment systems in Israel and in USA.

The goal of this workshop is to exchange the recent advances in academic and industry for securing the ICSs with an automation vision. Invited speakers from both industry and academics will talk on four main topics ranging from the main cyberattacks of ICS since the beginning of this century, the main trends for securing ICSs, implementation and design of solutions, and the education for securing ICSs. This workshop includes an introduction of cyberattacks in Industrial Control Systems, a demonstration of cyberattacks on small-scale manufacturing system, 3 sessions of presentations given by automation system integrators, vendor solution and academics on cybersecurity solutions for ICS with an automation vision, and lastly a roundtable on the education for cybersecurity.

**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.

**Format:**

- Introduction/sessions: 20 minutes of presentation + 10 min of Answers/Questions

- Roundtable: discussion with all the speakers of the workshop

| **Time** | **Workshop program** |
|---|---|
| **Welcome reception** | |
| 8 :15 – 8 :45 am | Registration |
| | |
| **How do the threats to cybersecurity have changed over time in Industrial Control Systems?** | |
| 9 :00 - 9 :25 am | « Cyberthreats to industrial environments and companies », M. Mathieu Delaplace, ANSSI Representative for Auvergne-Rhônes-Alpes (in-person) |
| | |
| **Demonstration of cyberattacks on a small-scale manufacturing system** | |
| 9 :30 – 10 :30am | M. Bertrand Felix, La Ruche Industrielle (in-person) ; M. Simon Navizet, Volvo Group (in-person) ; Dr. Cédric Escudero, INSA Lyon, Laboratoire Ampère (in-person) |
| | |
| **Coffee break** | |
| | |
| **Session 1: Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics** | |
| 11:00 – 11:30am | « Feedback of integrator and end users », Dr. Franck Sicard, Naval Group (in-person) |
| 11 :30am – 12:00pm | Industrial - Waiting for confirmation |
| 12 :00 – 12 :30pm | Industrial - Waiting for confirmation |
| | |
| **Lunch (12:30 – 2:00pm)** | |
| | |
| **Session 2: Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics** | |
| 2:00 – 2:30pm | «Deep Packet Inspection approach – Securing ICS devices», M. Riccardo Colelli, Universita Degli Studi Roma Tre (online) |
| 2:30 – 3:00pm | «Secure state estimation for control systems under sensor attacks», Dr. Michelle Chong, Control Systems Technology at Eindhoven University of Technology (TU/e) (in-person) |
| | |
| **Coffee break** | |
| | |
| **Session 3: Automation based-solutions/methods for securing Industrial Control Systems: Feedback of integrators and advances in industry and academics** | |
| 3:30 – 4:00pm | « Constraining control signals to protect control systems against stealthy aging attacks», Dr. Cédric Escudero, INSA Lyon, Laboratoire Ampère (in-person) |
| 4:00 – 4:30pm | «Intrusion Detection Systems for Industrial Control Systems : Techniques to detect advanced persistebt threats and future challenges», Dr. David Espes, Université de Bretagne Occidentale, Laboratoire Lab-STICC (in-person) |
| | |
| **Coffee break** | |
| | |
| **Roundtable: Education for cybersecurity: what are the trends and needs of ICS cybersecurity for the industry?** | |

| | |
|---|---|
| 5:00 – 6:00pm | M. Mathieu Delaplace (ANSSI), M. Bertrand Felix (La Ruche Industrielle), M. Simon Navizet (Volvo Group), Dr. Franck Sicard (Naval Group), Industrials – Waiting for confirmation, Pr. Eric Zamaï (INSA Lyon, Laboratoire Ampère), Dr. Cédric Escudero (INSA Lyon, Laboratoire Ampère), M. Amaury Beaudet (INSA Lyon, Laboratoire Ampère), M. Riccardo Colelli (Universita Degli Studi Roma Tre), Dr. Michelle Chong (Control Systems Technology, Eindhoven University of Technology (TU/e)), Dr. David Espes (Université de Bretagne Occidentale, Laboratoire Lab-STICC) |

**Speaker biography:**

M. Mathieu Delaplace, ANSSI Representative for Auvergne-Rhône-Alpes :
ANSSI is the French National Cybersecurity Agency. The role of ANSSI is to foster a coordinated, ambitious, pro-active response to cybersecurity issues in France, to drive raising-awareness actions, as well as to spread French vision and expertise, and European values, abroad.

Dr. Cédric Escudero, Postdoctoral researcher at INSA Lyon, Laboratoire Ampère:
He received the Master degree in automation and control systems engineering from the University of Grenoble, France, in 2017. He obtained a PhD in cybersecurity of control systems at the Laboratoire G-SCOP, University of Grenoble. During his PhD, he was a visiting researcher at Laboratoire Ampère, INSA Lyon, where he is currently a postdoctoral researcher in cybersecurity of control systems.

Dr. Franck Sicard, Research engineer at Naval Group:
Graduated from Grenoble INP - ENSE3 (2014), I worked 1 year as a development engineer in an industrial automation integrator. I then did a thesis on attack detection in ICS based on behavioral models (2015-2018). Following a post-doc on the application of my research work at an industrial company, I joined Naval Group as a research engineer in cybersecurity, particularly on the OT perimeter. Naval Group, the European leader in Naval Defense, has made cybersecurity a major issue.

M. Riccardo Colelli, PhD student at Universita Degli Studi Roma Tre:
He received the master's degree in computer science and automation engineering from the University of Roma Tre, Rome, Italy, in 2018. He is currently a Ph.D. student in computer science and automation with the University of Roma Tre, Rome, Italy. His current research interests include cyber physical systems, cybersecurity and critical infrastructure protection.

Dr. Michelle Chong, Assistant Professor in the Control Systems Technology at Eindhoven University of Technology (TU/e):
She is an Assistant Professor in the Control Systems Technology section at the Eindhoven University of Technology (TU/e), the Netherlands. She hails from Melbourne, Australia, where she also obtained a PhD in systems and control theory at the University of Melbourne. Dr. Chong has held postdoctoral positions at KTH Royal Institute of Technology and Lund University in Sweden, as well as University of California Santa Barbara, at the Centre of Control, Dynamical-Systems and Computation (CCDC). She is a recipient of the American Australian Association's ConocoPhillips postdoctoral fellowship in 2013. Her research interests are in the development of control and estimation algorithms for nonlinear and hybrid systems with a special interest in cyber security and its applications to power systems and neuroscience.

Dr. David Espes, Associate Professor at Université de Brest, LabSTICC:
He received the MS degree in Computer Sciences (2004) and the PhD degree in Computer Sciences (2008) all from the University of Toulouse, France. In September of 2009, he joined the "Network, Security and Multimedia" department at Telecom Bretagne (Rennes) as a post-doctoral researcher. Since 2010, he has been with the University of Brest, France, as an associate professor. He is the leader of the CNRS LabSTICC IRIS team on Security and Resilience of Information Systems. He works on cybersecurity in the field of the Industry of the Future, topics including management and deployment of security policies, intrusion detection and response to cyber-attacks.

Pr. Eric Zamaï, Full Professor at INSA Lyon, Laboratoire Ampère:
He received his Ph.D degree from the University of Toulouse III, Toulouse, France, in 1997, and the Habilitation à Diriger des Recherches degree from the University of Grenoble Alpes (INP Grenoble), France, in 2006.
After 21 year of teaching and research activity at the Ecole Nationale Supérieure de l'Energie, l'Eau et l'Environnement and G-SCOP Laboratory,
He joined the Institut National des Sciences Appliquées of Lyon (INSA-Lyon) and the AMPERE Laboratory in 2019. He is currently full professor within INSA-Lyon in charge of Control and Reliability Engineering, SCADA Systems and CyberSecurity of industrial processes lectures for various undergraduate courses. His main research interests are Cyber-Security, Supervision, Diagnostic,Reconfiguration and Pronostic Health Management for industry.
He had supervised in this field more than 14 PhD defended thesis, and is author/coauthor of over 80 publications including over 20 journal articles and seven parts of books in his area of expertise.
He has been Director of Education of École nationale supérieure d'ingénieurs électriciens de Grenoble (ENSIEG) from 2006 to 2008, in charge of National French-Vietnam partnership (PFIEV) from 2007 to 2012, and director of S.MART Grenoble Alpes Technical Center from 2014 to 2019.

M. Amaury Beaudet, PhD student at Laboratoire Ampère:
He received the Master's degree in automation and control systems from the University of Grenoble, France, in 2018. He is currently a Ph.D. student in automation and control sytems with the University of Lyon at Laboratoire Ampère, Lyon, France. His current research interests include cyber physical systems, discrete-event systems, cybersecurity and critical infrastructure protection.

**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

**Organizers:** [Cédric ESCUDERO], [Postdoctoral researcher]

[Laboratoire Ampère CNRS, INSA Lyon, Université de Lyon, 69621 Villeurbanne CEDEX, France]
E-mail: [cedric.escudero@insa-lyon.fr]
Phone: +[33] – [767925934]

[Amaury BEAUDET], [PhD candidate]
[Laboratoire Ampère CNRS, INSA Lyon, Université de Lyon, 69621 Villeurbanne CEDEX, France]
E-mail: [amaury.beaudet@insa-lyon.fr]
Phone: +[33] – [787659983]

[Emil DUMITRESCU], [Associate Professor]
[Laboratoire Ampère CNRS, INSA Lyon, Université de Lyon, 69621 Villeurbanne CEDEX, France]
E-mail: [emil.dumitrescu@insa-lyon.fr]
Phone: +[33] – []

[Eric ZAMAI], [Full Professor]
[Laboratoire Ampère CNRS, INSA Lyon, Université de Lyon, 69621 Villeurbanne CEDEX, France]
E-mail: [eric.zamai@insa-lyon.fr]
Phone: +[33] – [687023316]

[Franck SICARD], [PhD-Engineer]
[Naval Cyber Laboratory, Naval Group, Ollioules, France]
E-mail: [franck.sicard@naval-group.com]
Phone: +[33] – [685426161]

**Time:** August 23, 2021