**Open Invited Track Proposal for the IFAC World Congress 2023, Yokohama, Japan**

# Modeling and Design of Secure and Resilient Control Systems

**Track Code: 4bi4c**

## Chairs:

Michelle Chong, Eindhoven University of Technology, Email: *m.s.t.chong@tue.nl*
Qing-Long Han, Swinburne University of Technology, Email: *qhan@swin.edu.au*
Craig Rieger, Idaho National Laboratory, Email: *craig.rieger@inl.gov*
Henrik Sandberg, KTH Royal Institute of Technology, Email: *hsan@kth.se*
Quanyan Zhu, New York University, Email: *qz494@nyu.edu*
Yuhan Zhao, New York University, Email: *yhzhao@nyu.edu*

## Abstract:

This track aims to create a platform between practitioners and control theorists to share knowledge and insights on the modeling and design of next-generation high-confidence control systems that are secure and resilient to a growing number of cyber threats.

## Choice of IFAC Technical Committee for Evaluation:

This Open Invited Track is proposed by the IFAC Technical Committee TC 1.5 (Networked Systems) under the Systems and Signals Coordinating Committee (CC).

## Keywords:

IFAC TC 1.5, Network Systems, Complex Systems, Network Security, Resilient Control Systems, Cyber-Physical Systems, Critical Infrastructure Protection

## Description of the topic:

Modern control systems are increasingly interconnected and consist of heterogeneous subsystems of diverse functions, integrating Informational Technology (IT) and Operational Technology (OT) units to achieve task-specific objectives and support critical services. The connectivity also enlarges the attack surface of the control systems and makes them vulnerable to cyber attacks. The past few years have witnessed many calamitous attacks on ICSs ranging from the Stuxnet attack on nuclear power plants in 2010 [1] to the ransomware attack on Automotive technology manufacturer, Denso, in 2022 [2]. There is an urgent need to strengthen the security of control systems. Mere IT solutions alone are, however, insufficient to address the security challenges since they overlook the security of the OT systems. The OT systems contain physical units such as sensors and actuators for real-time task execution and communicate with IT systems via fieldbus. Their performance is affected by the well-being of cyber systems as well as the disturbances and internal faults on physical units. Therefore, OT security aims to not only mitigate malicious attacks from the cyber domain but also to stabilize the physical systems.

The security of control systems is challenging, not only due to the cross-layer and system-wide needs but also because of the role of the attacks. Growingly sophisticated attacks make it harder or infeasible to achieve "perfect" security, which aims to protect control systems from any attacks and ensure system performance. Resilience becomes an effective way to further mitigate security risk. Resilience refers to the system's ability to "maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature" [3]. A resilient control system can effectively respond to an unknown attack to mitigate its impact and maintain acceptable system performance [4].

This track invites scientists, engineers, and stakeholders from government, industry, and academia to contribute with theoretical and applied research papers. The topics of interest in this track include (but not limited to):

- Resilient network control
- Design of secure and resilient networks
- Model-based design for integration of security and control
- Game-theoretic approaches for the security of networked systems
- Testbeds for the security of critical infrastructures
- Emerging system theory and design methods
- Homomorphic encryption for control
- Management of interdependent risks
- Economics of security and privacy
- Mechanism design and incentives for resilience
- Security and privacy of networks
- Adaptive and autonomous defense
- Supply chain risks for control systems
- Machine learning and artificial intelligence for security and resilience
- Security of AI-enabled control systems
- Visualization of cybersecurity operations
- Privacy in control systems
- Applications to critical infrastructures, including power and energy systems, transportation networks, unmanned aerial vehicles (UAVs), unmanned surface vehicles (USVs), water and food systems

**Submission:**
For author guidelines, please refer to https://www.ifac-control.org. All papers must be submitted electronically at https://ifac.papercept.net/. All papers must be prepared in a two-column format in accordance with the IFAC manuscript style. Please use the official IFAC instructions and template to prepare your contribution as a full-length draft paper and submit it online. Submission details are available on the conference website. All submissions must be written in English. All papers that conform to submission guidelines will be peer-reviewed by IPC members.

The corresponding authors need to submit their paper online (pdf format) as ***Open Invited Track Paper***.

**Important deadlines:**

- Oct. 31, 2022: Open invited track paper submission
- Feb. 21, 2023: Notification of acceptance
- Mar. 31, 2023: Final paper submission

**References:**

[1] Kim, Do-Yeon. "Cyber security issues imposed on nuclear power plants." *Annals of Nuclear Energy*, 65 (2014): 141-143.

[2] A. Hope, "Japanese automotive suppliers targeted as denso suffers pandora ransomware attack and bridgestone compromised by lockbit," Accessed May 31, 2022 [Online]. Available: https://www.cpomagazine.com/cyber-security/japanese-automotive-suppliers-targeted-as-denso-suffers-pandora-ransomware-attack-and-bridgestone-compromised-by-lockbit/

[3] Rieger, Craig G., David I. Gertman, and Miles A. McQueen. "Resilient control systems: Next generation design research." In *2009 2nd Conference on Human System Interactions*, pp. 632-636. IEEE, 2009.

[4] Zhu, Quanyan, Craig Rieger, and Tamer Başar. "A hierarchical security architecture for cyber-physical systems." In *2011 4th international symposium on resilient control systems*, pp. 15-20. IEEE, 2011.