



## Industrial Control

# Preface: Security and safety for next generation industrial systems

Xinping Guan<sup>1,\*</sup>, Yan Zhang<sup>2</sup>, Niyato Dusit<sup>3</sup>, Yongfeng Huang<sup>4</sup>, and Jiawen Kang<sup>5</sup>

<sup>1</sup> School of Electronic, Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

<sup>2</sup> University of Electronic Science and Technology of China, Chengdu 611731, China

<sup>3</sup> Computer Science and Engineering, Nanyang Technological University, Singapore 639798, Singapore

<sup>4</sup> Department of Electronic Engineering, Tsinghua University, Beijing 100084, China

<sup>5</sup> School of Automation, Guangdong University of Technology, Guangzhou 510006, China

Received: 29 October 2025 / Revised: 29 October 2025 / Accepted: 30 October 2025 / Published online: 31 October 2025

**Citation** Guan X, Zhang Y, Dusit N, Huang Y and Kang J. Preface: Security and safety for next generation industrial systems. Security and Safety 2025; 4: E2025016. <https://doi.org/10.1051/sands/2025016>

Industrial Control Systems (ICS) are the backbone of modern industrial automation, integrating cyber intelligence with physical processes to manage critical infrastructure in energy, manufacturing, and transportation. The rapid proliferation of digital technologies, such as artificial intelligence (AI), the Internet of Things (IoT), and renewable energy systems, has enhanced operational efficiency but also escalated vulnerabilities to sophisticated cyberattacks. The 2015 Ukrainian power grid attack serves as a stark reminder of the potential for cascading failures, economic losses, and safety hazards from threats like denial-of-service (DoS), false data injection (FDI), and collusive stealthy attacks. This topical issue tackles these challenges through a structured approach across three phases: risk and vulnerability assessment, analytical and detection methodologies, and control optimization. The six selected papers collectively provide a comprehensive strategy to fortify the security and safety of ICS.

In the paper by Huihui Huang, Yunkai Song, Qiang Wei, Yangyang Geng, and Hongmin Wang [1], a comprehensive review systematically examines the multifaceted cyber-physical security risks in new power systems amid the global energy transition toward low-carbon models. The authors dissect threats across the Sensing-Transmitting-DecisionMaking-Controlling (STDC) loop and the Generation-Grid-Load-Storage (GGLS) integration model, drawing on real-world instances like the 2015 Ukrainian “Black Energy” attack to highlight Cyber-Physical Coupling Threats (CPCT). They identify vulnerabilities in renewable energy integration and propose six future risk categories, advocating for adaptive cybersecurity measures to ensure the stable operation of power grids, thus providing a theoretical foundation for enhancing resilience in evolving energy infrastructures.

A study of vulnerability assessment in high-voltage direct current transmission systems to cyberattacks is presented by Rong Guo, Mengxiang Liu, and Ruilong Deng [2], focusing on the critical role of voltage-source converter-based HVDC (VSC-HVDC) in long-distance power transmission. The researchers conduct real-time simulations on the OPAL-RT OP5707 XG platform to evaluate the impacts of denial-of-service (DoS), time-delay, false data injection (FDI), and hybrid attacks on converter stations. Their findings reveal severe consequences, including DC over-voltage, power transmission failure, and system oscillations, underscoring the urgent need for robust cybersecurity enhancements to protect HVDC control systems and maintain grid stability.

\* Corresponding author (email: [xpguan@sjtu.edu.cn](mailto:xpguan@sjtu.edu.cn))

Yuheng Wu, Zhenyong Zhang, Zheqiu Hetu, Xinyu Cheng, and Peng Cheng [3] organized a survey on reverse engineering of industrial control protocols (ICP), addressing the prevalence of proprietary protocols in Industrial Control Systems (ICS) with limited documentation. The authors construct a comprehensive technical framework encompassing seven aspects: data acquisition, message clustering, field division, key field identification, field semantic derivation, state machine modeling, and application. They discuss common limitations, such as scalability in heterogeneous environments, and suggest future research directions, providing a vital tool for understanding and managing protocol behavior to bolster ICS security.

A study of countermeasures against collusive stealthy attacks in cyber-physical microgrids is presented by Zhihua Wu, Chen Peng, Engang Tian, and Yajian Zhang [4], targeting the integration of computation, communication, and physical devices in industrial systems. The team deploys an  $L_\infty$  unknown input observer (UIO) at the control center to monitor distributed generation units (DGUs), analyzing attack vulnerabilities and devising a dynamic encoding mechanism for communication links. This approach, involving encoding control signals and decoding at the center, is validated through simulation experiments, offering an effective framework to detect and mitigate stealthy attacks without triggering false alarms.

In the paper by Zhixu Du, Hao Zhang, Zhuping Wang, and Sheng Gao [5], an optimized adaptive asymptotic control is developed for leaderless multi-agent systems (MAS) under deception attacks, addressing a critical challenge in cooperative control. The authors employ a backstepping technique to formulate transformed tracking errors and integrate a critic-actor structured reinforcement learning algorithm with Nussbaum techniques to eliminate destabilizing effects of time-varying gains. Using Lyapunov stability analysis, they demonstrate that all closed-loop signals remain bounded, achieving asymptotic output consensus, with simulation results confirming the efficacy of this approach.

A survey of random number generators is conducted by Haozhe Chai, Qianqian Pan, and Jun Wu [6], emphasizing the role of true random number generators (TRNGs) in security-critical industrial applications. The authors trace the historical development from early hardware to modern implementations, covering physical phenomena like electronic noise and quantum effects, and evaluate randomness through statistical and visual analysis methods. They explore TRNG applications in blockchain for tamper-resistant operations and integration with machine learning for improved generation, highlighting challenges like hardware costs and entropy source stability.

This topical issue collectively advances the field by providing a structured response to ICS security challenges, from risk identification to resilient control. We hope these contributions inspire further research and practical implementations. We extend our gratitude to the authors for their scholarly efforts and to the reviewers and editors for their invaluable support.

## References

- [1] Huang H, Song Y and Wei Q et al. A comprehensive review of cyber-physical security risks in new power system. *Secur Saf* 2025; 4: 2025005. <https://doi.org/10.1051/sands/2025005>
- [2] Guo R, Liu M and Deng R. Vulnerability assessment of high-voltage direct current transmission systems to cyberattacks. *Secur Saf* 2025; 4: 2025008. <https://doi.org/10.1051/sands/2025008>
- [3] Wu Y, Zhang Z and Hetu Z et al. Reverse engineering of industrial control protocol: A survey. *Secur Saf* 2025; 4: 2025012. <https://doi.org/10.1051/sands/2025012>
- [4] Wu Z, Peng C and Tian E et al. Countermeasures against collusive stealthy attacks in cyber-physical microgrids: A dynamic encoding approach. *Secur Saf* 2025; 4: 2025007. <https://doi.org/10.1051/sands/2025007>
- [5] Du Z, Zhang H and Wang Z et al. Optimized adaptive asymptotic control for leaderless multi-agent systems under deception attacks. *Secur Saf* 2025; 4: 2025013. <https://doi.org/10.1051/sands/2025013>
- [6] Chai H, Pan Q and Wu J. A survey of random number generator: Approaches, tests, novel applications in block-chain and AI driven industrial networks. *Secur Saf* 2025; 4: 20250010. <https://doi.org/10.1051/sands/20250010>