Special Session 12: Safeguarding Artificial Intelligence-Enabled Advanced Power Systems Against Emerging Cyber-Physical Security Threats

Session Organizers：

Jiaqi Ruan, Sichuan University, jiaqiruan@scu.edu.cn
Gaoqi Liang, Harbin Institute of Technology, Shenzhen, lianggaoqi@hit.edu.cn
Qisheng Huang, Harbin Institute of Technology, Shenzhen, huangqisheng@hit.edu.cn
Peipei Yu, Shanghai University of Electric Power, peipeiyu@shiep.edu.cn

Brief Description of the Session Thematic:

The advent of advanced artificial intelligence (AI) technologies, such as large language models like ChatGPT with superior intelligent levels, reasoning ability, and extensive domain knowledge, has revolutionized many industries, including the power sector. These capabilities present unprecedented opportunities to support increasingly complex power systems. AI can greatly assist in the operation and planning of power systems by optimizing performance, predicting demand, and enhancing decision-making processes. However, the integration of AI into power systems introduces substantial security risks. These vulnerabilities stem from the inherent complexity of AI algorithms and their susceptibility to sophisticated cyber-physical threats. The potential for malicious attacks to exploit these weaknesses poses significant risks to the reliability and stability of power systems. Securing AI-enabled advanced power systems is thus both a technical challenge and a strategic necessity. This special issue aims to address the emerging security threats associated with the deployment of AI in power systems. We seek contributions from leading academic researchers and industry professionals who are developing innovative solutions to these critical security challenges. We welcome high-quality, original research papers, reviews, and case studies that offer insights and practical approaches to safeguarding AI-enabled power systems.

Topics and Keywords:

1 Utilization of AI applications to accelerate the advancement of more intelligent power systems
2 Investigation of security issues associated with AI applications and their impact on power systems
3 Development of threat models reflecting potential attack strategies and their impact on AI-enabled power system operations
4 Development of effective mitigation strategies to address AI-related security vulnerabilities in power systems
5 Strategies to enhance the resilience of AI-enabled power systems against cyber-physical security threats
6 Analysis of current policies and formulation of new regulations to ensure the safe application of AI in power systems
7 Documentation and discussion of real-world scenarios, successful implementations, and lessons learned from securing AI-enabled power systems