Call for Papers

IEEE Transactions on Power Electronics (TPEL) Letters

Special Section on Cyber-Security in Power Electronics Systems: Modeling, Detection, and Resilience

Scheduled Publication Time: October 2026

Brief description

Power electronics systems underpin modern energy applications such as transportation electrification, data centers, and renewable integration. These systems are increasingly integrated with digital controllers and communication networks. While such integration enhances operational efficiency, it also introduces cyber-security threats across multiple levels. At the system-level, converter-based networks are vulnerable to communication-based and coordinated attacks, while at the component-level, threats such as hardware Trojans and side-channel tampering can compromise converter functionality.

The cyber-threats faced by power electronics are exacerbated by their unique characteristics. Particularly, power converters operate on sub-millisecond timescales, are highly controllable, and exhibit low inertia. This makes them highly responsive but also sensitive to disturbances from both component- and system-level intrusions. Even minor perturbations can propagate rapidly, leading to instability. Therefore, the existing cyber-security frameworks, designed for conventional power grids and have a system-level focus, cannot be directly applied to power electronics systems due to their fast dynamics and the multi-layered attack surface spanning from converter to grid.

This highlights a pressing need for cyber-security research tailored to power electronics. It is imperative to identify cyber-vulnerabilities, develop attack models, design detection strategies, and establish practical validation platforms. Addressing these challenges is critical to ensuring the secure and reliable operation of power electronics systems.

Objective

The objective of this Special Section is to engage researchers from both academia and industry worldwide to explore and address cyber-security challenges that are unique to power electronics across diverse applications. The focus is on raising awareness, consolidating recent advances, and encouraging systematic approaches that enhance the security and resilience of power electronics within modern energy, industrial, transportation, and information systems.

Subtopics

Prospective authors are invited to submit original contributions and industry-oriented papers on related topics of interest including, but are not limited to, the following:

- Cyber-physical modeling and co-simulation frameworks for power electronics systems
- Multi-layered vulnerability assessment and attack impact analysis on power electronics systems
- Intrusion detection and mitigation schemes tailored to fast power electronics dynamics
- Cyber-resilient control and protection methods of power electronics systems
- Application-specific cyber-security frameworks and considerations (e.g., solid-state transformers, electric vehicles, data centers, renewable integration)

- Digital twin and real-time hardware-in-the-loop platforms for multi-layered cyber-attack emulation and testing
- Challenges and opportunities of artificial-intelligence (AI) enabled cyber-security methods in power electronics systems

Timeline

- **March 31, 2026: Manuscript submission deadline**
- May 15, 2026: Revised manuscript submission deadline
- June 30, 2026: Final acceptance notification
- July 31, 2026: Manuscript forwarded to IEEE editorial production team for publication
- October 2026: Special Section appear in IEEE TPEL

Guest editors

- Zhi Jin (Justin) Zhang, The University of British Columbia
- Reynaldo Nuqui, Hitachi Energy

Guest editorial

Power electronics systems (PES) are now central to the modernization of energy, industrial, information, and transportation infrastructures worldwide. They enable technologies such as renewable energy integration, electrified transportation, and modern data centers. These advances are made possible by increasingly digital control platforms, extensive communication links, as well as the integration of readily available third-party equipment and software. While such a transformation brings significant benefits, it also introduces potential vulnerabilities and backdoors that can be exploited by malicious players. As a result, cyber-security threats are becoming directly relevant to the operation of power electronics.

The reality of these cyber-vulnerabilities is underscored by real-world cyber incidents targeting industrial systems and critical infrastructure. From 2006 to 2019, the total number of attacks on cyber-physical systems increased by 2000%, with an annual cost of $445 billion to the global economy. Although the notable cyber-security breaches have targeted the conventional power grid (e.g., Ukrainian power grid cyber-attacks of 2015 and 2016), an increasing number of events involving the PES, such as solar plants and wind turbine generators, have been reported in both the United States and Europe. These developments highlight that the cyber-security of PES is now an urgent and practical issue.

However, cyber-security challenges in power electronics are different from those in conventional power systems. Cyber-threats faced by PES can originate from both component- and system-levels. For example, hardware Trojans, side-channel leakage, and firmware tampering can compromise the converter and control integrity. Meanwhile, the falsification of system-level communication links will potentially trigger wide-area instability or shutdowns. Moreover, PES operate on sub-millisecond timescales, are highly controllable, and exhibit low inertia. Such fast dynamics, combined with the multi-level threat, test the limits of the existing detection and mitigation frameworks.

Another important aspect is the manifestation and impact of cyber-vulnerabilities vary widely across applications. In electric vehicles, manipulated chargers endanger battery safety and present power quality problems. In solid-state transformers, side-channel noise poses a threat to the control performance of the stacked modules and can lead to cascading failures. In microgrids and renewable plants, attacks on grid-forming and grid-following converters undermine grid stability. These examples illustrate that cyber-security frameworks in PES may not have a one-size-fits-all solution, but instead require application-specific considerations informed by the domain knowledge.

Additionally, artificial intelligence (AI) is emerging as both an opportunity and a challenge. AI-enabled methods offer promising tools for intrusion detection and resilient control. At the same time, their reliance on large datasets and black-box models can introduce new vulnerabilities, such as adversarial manipulation and data integrity risks. In addition, the reliability and performance of AI-based algorithms beyond their training data must be addressed. Balancing the strengths and risks of AI in cyber-security for power electronics will therefore be another key research direction.

This Special Section on *Cyber-Security in Power Electronics Systems* provides a timely platform for consolidating knowledge and advancing solutions in this field. Contributions spanning vulnerability analysis, attack modeling, detection methods, resilient control, and digital twin, on both system- and component-levels, will help to shape the scope of this emerging area. By engaging researchers from both academia and industry, the Section aims to establish a technical foundation for cyber-secure power electronics in diverse applications. As these systems continue to expand in scale and importance, ensuring their security and resilience will be essential for the reliable operation of modern energy, industrial, transportation, and information infrastructures.