# PhD thesis proposal

# Detection of Cyber-Malicious Actions in Distributed Power Grid Systems

**Host institution:** INSA Lyon, Laboratoire Ampère (UMR CNRS 5005), Lyon, France
**Supervisors:** Cédric Escudero (INSA Lyon), Corinne Alonso (LAAS), Paolo Massioni (INSA Lyon)

**Preferred starting date:** October 2026

**Keywords:** Cyber-resilience; Networked control systems; Future energy networks; Stealthy cyberattacks; Attack detection and diagnosis.

**Candidate profile and required skills:**

We are looking for excellent candidates from engineering schools or top universities with strong background in:

- Control theory and state-space methods (estimation and control)
- Machine learning methods
- Signal processing methods
- Linear algebra and dynamical systems
- Scientific programming in Matlab/Simulink, Python
- Very good written and spoken English.

**Project context and objectives:**

Future energy networks will increasingly rely on interconnected and interoperable cyber-physical infrastructures to coordinate electricity, heat/cold, storage, mobility, renewable generation, and other sources of flexibility. This evolution is essential to support the energy transition, but it also introduces new challenges in terms of supervision, control, interoperability, and cybersecurity. In particular, the growing interconnection between experimental platforms, software tools, communication networks, and control systems increases the exposure of multi-energy

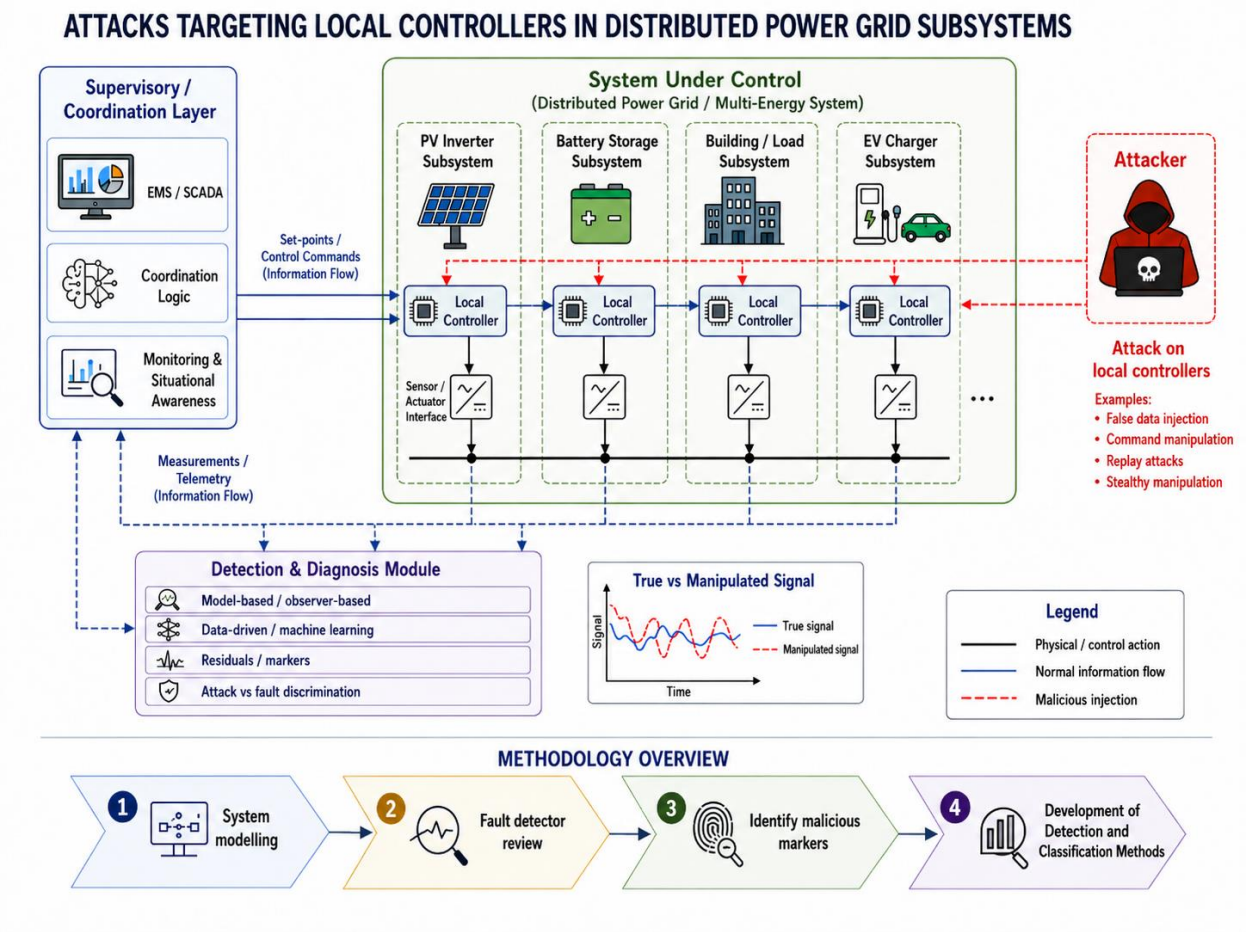
infrastructures to cyber-malicious actions targeting measurement signals, control commands, data exchanges, or monitoring systems.

This PhD is part of a national project, whose ambition is to develop a national reference infrastructure for the modelling, simulation, control, and experimental validation of future multi-energy systems.

Within this framework, a major challenge is to ensure the resilience of the interconnected energy infrastructure against cyber-malevolence. Abnormal system behavior may originate either from accidental faults, physical disturbances, communication issues, or intentional malicious manipulations. Conventional anomaly detection methods, such as Chi-square or sum-of-squares residual tests, can detect deviations from nominal behavior, but they generally do not distinguish between failures and cyberattacks. This limitation is particularly critical for stealthy attacks, whose objective is to remain hidden from operators and monitoring systems while progressively degrading the system, compromising control decisions, or affecting vital functions.

The main objective of this PhD is to develop signal-processing for the detection and diagnosis of cyber-malicious actions in multi-energy networked control systems. The work will focus on identifying abnormal trajectories and signal manipulations that are specifically designed to avoid classical anomaly detectors. By analyzing the interaction between attack strategies, system dynamics, communication architectures, and detection mechanisms, the PhD will contribute to the design of resilient monitoring methods capable of detecting, diagnosing, evaluating, and ultimately supporting the reconfiguration of multi-energy systems under attack.

This research will contribute to the work package “Resilience against cyber-malevolence”, led by INSA Lyon, by proposing methods to understand vulnerabilities, detect and diagnose malicious actions, evaluate attack scenarios, and support reconfiguration strategies aimed at preserving the critical functions of future energy networks. The methods developed during the PhD will be validated through simulation and experimental scenarios, in connection with the Grid4Mobility platform at INSA Lyon. Grid4Mobility is an experimental platform dedicated to the study and management of energy networks integrating buildings, energy storage systems, and electric vehicles. It aims to develop a systemic approach to analyze and optimize the management of energy and information flows in such networks, and includes two demonstrators: the La Doua campus demonstrator and the Transpolis site, which provides realistic and protected environments for electric vehicle experiments. This platform will provide a relevant experimental framework to assess cyberattack detection, diagnosis, and resilience strategies in realistic multi-energy and electromobility scenarios.




**Main research steps:**

The PhD will be structured around five key components:

- Modelling of distributed power grid systems: develop mathematical and simulation models of distributed energy networks, including interconnected subsystems such as distributed energy resources, power electronic converters, storage systems, electric vehicles, and local control architectures. These models will provide the basis for studying normal operating conditions, faults, disturbances, and cyber-malicious scenarios.
- Literature review of fault and anomaly detection methods: conduct a detailed review of existing detection and diagnosis methods for power grid and cyber-physical energy systems. This review will cover both model-based approaches, such as observers, residual generators, unknown-input observers, and robust fault detection filters, and model-free approaches**,** including machine-learning-based anomaly detection methods. The objective will be to identify their strengths, limitations, and vulnerability to intelligent attacks.

- Identification of markers of malicious manipulation: investigate how intelligent, intentional, or malicious signal manipulations affect the behavior of classical detectors.

The goal will be to identify specific markers that distinguish cyber-malicious actions from accidental faults or physical disturbances, especially when attacks are designed to remain stealthy with respect to standard anomaly detectors.

- Development of detection and classification methods: based on the identified markers of malicious manipulations, develop methods for the detection and classification of abnormal behaviors affecting local controllers. The objective will be to design approaches capable of distinguishing normal operation, faults or disturbances, and intentional cyber-malicious actions. Both model-based and data-driven strategies may be considered, with the aim of improving the reliability, interpretability, and robustness of detection and in distributed power grid systems.

- Testing and validation of the proposed approach: evaluate the developed detection and diagnosis methods through simulation and experimental scenarios. The approach will be tested on representative distributed power grid models and, when possible, in connection with the Grid4Mobility platform at INSA Lyon, in order to assess its relevance for realistic energy-management and cyber-resilience scenarios.

Experimental validation will be carried out in connection with the Grid4Mobility platform at INSA Lyon, which integrates buildings, storage systems, electric vehicles, and energy networks. This will allow the proposed detection and diagnosis methods to be assessed on realistic scenarios involving energy management, information exchange, and cyber-malicious actions in multi-energy infrastructures.

**Impact:**

This PhD addresses a key challenge in the cybersecurity of critical infrastructures: detecting malicious actions that are specifically designed to remain hidden from classical monitoring systems. The expected results will contribute to improving the resilience of networked control systems by enabling earlier detection, more accurate diagnosis, and better evaluation of cyber-malicious scenarios.

Beyond its academic contributions in control theory, signal processing, and cyber-physical systems security, the project has strong practical relevance for industrial infrastructures, energy networks, transportation systems, and other domains where the integrity of monitoring and control signals is essential for safety, availability, and operational continuity.

**Salary, healthcare, and accommodation:**

The PhD position is funded for 36 months through a French doctoral contract. The gross monthly salary will follow the French national regulations for doctoral contracts, i.e. €2,300 gross per month from January 2026 for a full-time research contract. Additional teaching or valorization activities may be possible depending on institutional rules and may lead to additional compensation.

The doctoral contract includes access to the French social security system, which covers a significant part of medical and hospital expenses in France. Complementary health insurance may also be available or recommended according to the host institution's rules.

The PhD student will be based at INSA Lyon, Ampère Laboratory, in Lyon, France. Accommodation is not included in the contract, but student housing on or near the INSA Lyon campus may be available, usually at a lower cost than private accommodation in Lyon. The host institution can provide guidance on available options, including campus residences, university housing services, and administrative procedures for international students.

**Submission deadline:** August, 20th, 2026

**To apply:** send your CV and academic transcripts to cedric.escudero@insa-lyon.fr and paolo.massioni@insa-lyon.fr

**References:**


Ahn, B., Kim, T., Ahmad, S., Mazumder, S. K., Johnson, J., Mantooth, H. A., & Farnell, C. (2023). An overview of cyber-resilient smart inverters based on practical attack models. *IEEE Transactions on Power Electronics*.

Anand, S. C., Nguyen, A. T., Teixeira, A. M. H., Sandberg, H., & Johansson, K. H. (2025). Quantifying security for networked control systems: A review. *arXiv preprint arXiv:2510.18645*.

Blanchini, F. (1999). Set invariance in control. *Automatica, 35*(11), 1747–1767.

Boyd, S., El Ghaoui, L., Feron, E., & Balakrishnan, V. (1994). *Linear Matrix Inequalities in System and Control Theory*. SIAM, Philadelphia.

Davari, M., Aghababa, M. P., Blaabjerg, F., & Saif, M. (2021). An innovative, adaptive faulty signal rectifier along with a switching controller for reliable primary control of GC-VSIs in CPS-based modernized microgrids. *IEEE Transactions on Power Electronics, 36*(7).

Escudero, C., Massioni, P., Scorletti, G., & Zamaï, E. (2020). Security of control systems: Prevention of aging attacks by means of convex robust simulation forecasts. *IFAC-PapersOnLine, 53*(2).

Escudero, C., Massioni, P., Zamaï, E., & Raison, B. (2022). Analysis, prevention, and feasibility assessment of stealthy ageing attacks on dynamical systems. *IET Control Theory & Applications, 16*(4).

Escudero, C., Murguia, C., Quevedo, D., Massioni, P., & Zamaï, E. (2025). Safety filters against actuator attacks. *International Journal of Robust and Nonlinear Control, 35*(9), 3640–3657.

Fu, R., Lichtenwalner, M. E., & Johnson, T. J. (2023). A review of cybersecurity in grid-connected power electronics converters: Vulnerabilities, countermeasures, and testbeds. *IEEE Access, 11*, 113543–113559.

Gonzalez, R. S., Aryasomyajula, V. A., Ayyagari, K. S., Gatsis, N., Alamaniotis, M., & Ahmed, S. (2023). Modeling and studying the impact of dynamic reactive current limiting in grid-following inverters for distribution network protection. *Electric Power Systems Research, 224*, 109609.

Ibrahim, H. A. J., Kim, J., Ramos-Ruiz, J. A., Ko, W. H., Huang, T., Enjeti, P. N., Kumar, P., & Xie, L. (2023). Detection of cyber attacks in grid-tied PV systems using dynamic watermarking. *IEEE Transactions on Industry Applications, 60*(1), 819–827.

IEEE. (2023). *IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*. IEEE Std 1547.3-2023.

Jamali, M., Sadabadi, M. S., & Davari, M. (2025a). A set-theoretic adaptive current control design for grid-following inverter-based resources to tackle practically non-ideal control inputs. *IEEE Transactions on Automation Science and Engineering, 22*, 9528–9543.

Jamali, M., Sadabadi, M. S., Davari, M., Sahoo, S., & Blaabjerg, F. (2025b). Resilient-by-design control for in situ primary controller of grid-following inverter-based resources by a novel state augmentation to tolerate false data injection cyberattacks. *IEEE Transactions on Power Electronics, 40*(2), 2746–2760.

Khan, A., Hosseinzadehtaher, M., Shadmand, M. B., Saleem, D., & Abu-Rub, H. (2020). Intrusion detection for cybersecurity of power electronics dominated grids: Inverters PQ set-points manipulation. In *2020 IEEE CyberPELS* (pp. 1–8). IEEE.

Li, Y., & Yan, J. (2022). Cybersecurity of smart inverters in the smart grid: A survey. *IEEE Transactions on Power Electronics, 38*(2), 2364–2383.

Lin, Y., Chong, M. S., & Murguia, C. (2026). Secondary safety control for systems with sector bounded nonlinearities. *Automatica, 183*, 112610.

Ramos-Ruiz, J., Kim, J., Ko, W. H., Huang, T., Enjeti, P., Kumar, P., & Xie, L. (2020). An active detection scheme for cyber attacks on grid-tied PV systems. In *2020 IEEE CyberPELS*. IEEE.

Rezaeizadeh, A., Smith, R. S., & Mastellone, S. (2024). Stealthy cyber attack filter and its impact on control of grid-forming inverter. In *2024 IEEE 63rd Conference on Decision and Control (CDC)* (pp. 2367–2372). IEEE.

Schneeberger, M., Dörfler, F., & Mastellone, S. (2024). Advanced safety filter for smooth transient operation of a battery energy storage system. In *2024 IEEE 63rd Conference on Decision and Control (CDC)* (pp. 2385–2390). IEEE.