POLITECNICO MILANO 1863 | DIPARTIMENTO DI ENERGIA

EDI Lab Energy Data and Information Lab

RESEARCH THESIS ON:

DIAGNOSIS OF COMMUNICATION CYBERATTACKS IN MULTI-ENERGY SYSTEMS UNDER PARTIAL OBSERVABILITY

CONTEXT OF THE RESEARCH

Multi-Energy Systems (MESs) are emerging as strategic solutions for decarbonization by integrating multiple energy carriers, such as electricity, heat, hydrogen and gas, through interconnected conversion and storage assets. Their coordinated operation relies on Telecommunication Networks (TLCNs) to exchange measurements and control actions between distributed Internet of Things (IoT) devices and control centers. Cyber-attacks, such as latency attacks or Distributed Denial-of-Service (DDoS) attacks, can block End-to-End (E2E) communication between IoT devices, impairing control decisions and causing increased operational costs and safety constraint violations. E2E communication disruptions can also limit the information available to identify their causes and assess their physical consequences, making diagnosis and risk assessment dependent on the location in which diagnostic artifacts are deployed.

This thesis offers the opportunity to combine TLCN simulation with Bayesian Network (BN)-based diagnosis of E2E communication cyber-attacks in MESs. The student will integrate open-source TLCN and MES modeling to simulate normal and disrupted (attacked) scenarios, which will serve to investigate how deploying diagnostic tools at different locations affects their design and performance. The outcome will inform MES operators about potential defense strategies.

OBJECTIVE OF THE RESEARCH

This thesis aims to develop and evaluate a BN-based diagnostic tool for E2E communication disruptions in an MES, examining how the design and performance of diagnostic artifacts vary with deployment location (e.g., control centers, IoT modules). The research comprises the following expected activities:

- *Literature review.* Open-source TLCN simulation, cyber-physical risk assessment, BN-based diagnosis and construction under partial observability, and cyber-security in emerging MESs.
- *Problem formulation.* Define the MES architecture, control interactions and TLCN topology, together with attacker capabilities and mechanisms to induce E2E communication loss or delay. Specify consequences in terms of operating costs, service losses and constraint violations for comparing normal and attacked operation.
- *Scenario generation.* Embed the obtained TLCN into an available MES simulator to generate normal and attacked scenarios, specifying tracked quantities across different locations; the system response (cyber and physical) to a lack of E2E communication will need to be defined.
- *BN design under partial observability.* Propose a systematic method to construct BNs for E2E cyber-attack diagnostics and consequence quantification according to location and available information.
- *Validation and results analysis*. Study how missing or outdated E2E communication information affects BN diagnostic performance, identify the most suitable approaches across different disruptions, and ultimately suggest defense mechanisms for the MES operator.

The student will have the opportunity to contribute to scientific publications based on the project's outcomes. The expected duration of the research activities is 7 to 9 months (depending on progress) plus thesis writing.

CANDIDATE PROFILE

- Scientific programming skills (e.g., Python, MATLAB, Julia); knowledge of Git and OOP.
- Good technical communication skills in English.
- No more than two exams remaining.
- Familiarity with cybersecurity and knowledge of graph theory and energy systems is welcome.

RESEARCH TEAM

For further information, please contact:

- Dr. Juan-Pablo Futalef (juanpablo.futalef@polimi.it)
- Prof. Enrico Zio (enrico.zio@polimi.it), 02 2399 6340