Microgrid user-side detection

This paper proposes a novel observer-based cyberattack-resilient control and operation method for direct current microgrids to enable cybersecurity against fals

This Review surveys the key developments and challenges in securing microgrids against cyber threats, with a focus on microgrid control.

Accordingly, the reliable protection of MGs considering uncertainty in RESs is crucial for planners and operators. This paper uses data analysis to extract knowledge from locally available...

We implement predictive analytics using machine learning to deal with cyber-uncertainties and threats within the microgrid environment. An autoencoder neural network is implemented to classify...

The results demonstrate that the proposed detection frame-work is not limited to the specific microgrid modeled in this study. Instead, it provides a scalable foundation that can extend to a broad class of ...

AI-based cyber-attack detection and mitigation in microgrids were summarized, along with a case study where utilizing such techniques is presented. In addition, learning-based ...

A comprehensive end-to-end microgrid protection solution that offers a range of functionalities--from data collection to fault detection, localization, and isolation.

This paper presents decision tree-based protection solutions that combine fault detection and fault type classification in a fully inverter-based microgrid, using local measurements with-out any communication.

We present a novel two-tiered strategy employing data-driven and artificial intelligence methodologies. This approach is designed to detect and mitigate False-Data Injection (FDI) attacks, ...

This study presents a new approach and an innovative LSTM-based method, provided for the first time, for the detection and removal of cyber-attacks in DC microgrids. It also aims to enhance real-time ...

Web: https://falconengineering.co.za