Implementing Cyberattacks on an Electrical Substation Testbed
Student / Research Assistant (m/f/d)
35 hours/month

Join the Secure Energy Systems (SES) Research Group at the KASTEL Security Lab Energy, located within the Institute of Automation and Applied Informatics (IAI). Our team of researchers is at the forefront of addressing cyber-physical security challenges in energy systems.

We are currently engaged in a dynamic project that investigates security vulnerabilities within Smart Grids, focusing particularly on the communication protocols used in electrical substation automation systems. Our research facilities include a small-scale power generation setup equipped with various Siemens devices such as Programmable Logic Controllers (PLCs), Process Control Systems (PCS), and Intelligent Electronic Devices (IEDs), complemented by Simulink-based models for renewable energy.

This project involves the development of attack simulations, including Denial of Service (DoS), Man-In-The-Middle (MITM), data modification, time-delay, and replay attacks, to identify and explore protocol-specific vulnerabilities. We aim to capture network traffic and logs to create valuable datasets that will aid future research in Intrusion Detection Systems (IDS). Furthermore, we are interested in assessing the robustness of learning-based models in the context of Smart Grids via adversarial attacks.

We invite you to join our mission to protect critical infrastructure and build secure energy systems.

We offer

- Interesting tasks with the possibility of contributing to scientific publications
- Flexible working hours
- Long term employment opportunity and close supervision

Requirements

- Bachelor's or Master's in Electrical/Power Engineering/Computer Science
- Hands on experience with Python programming language and cybersecurity topics
- Prior experience with Siemens Energy devices or Machine Learning is a plus
- Motivated to work independently and as part of a team

Tasks

- Familiarization and planning
- Coding and testing
- Implementation, data collection and documenting

If you are interested, contact us via email to sanchez@kit.edu.
Please include your transcript of records and CV.

Contact Data

Karlsruher Institut für Technologie (KIT)
Automation and Applied Informatics (IAI)
Location: Campus North

Gustavo Sánchez
Secure Energy Systems (SES)
Phone: +49 721 608-22602
E-mail: sanchez@kit.edu