

## **We are looking for Support! Student / research assistant (m/f/d)**

Welcome to the Secure Energy Systems (SES) Research Group! We are working at the KASTEL Security Lab Energy, located at the Institute of Automation and Applied Informatics (IAI). In this lab we investigate the security challenges for Smart Grids and analyze the underlying communication protocols.

We are developing Intrusion Detection Systems (IDS) and use the open-source IDS Malcolm (<https://cisa.gov.github.io/Malcolm/>) as a baseline. The goal for this position is to develop and to configure Malcolm with a ruleset that is specific to each testbed through automation. Rather than manually writing the rules for each device in the lab, we aim to derive them i.e. from the Substation Configuration Description (SCD). This XML file contains the network devices and their connections within a substation. For this purpose, this position aims to develop an algorithm that automatically extracts information from the testbed and generates Zeek or Suricata detection rules.

### **We offer**

- Interesting & responsible tasks
- Flexible working hours
- Long term employment opportunity

### **Requirements**

- Programming in Python, Linux administration
- Prior experience with Suricata (<https://suricata.io/>) or Zeek (<https://zeek.org/>) is a plus

### **Tasks**

- Implement algorithm to generate Zeek and Suricata rules automatically
- Administration of Linux server with Malcolm IDS
- Support with dataset collection

If you are interested, contact us via email to [nicolai.kellerer@kit.edu](mailto:nicolai.kellerer@kit.edu), including current transcript of records and a resume/CV.

---

### **Contact Data**

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

Nicolai Kellerer  
Secure Energy Systems (SES)  
Phone: +49 721 608-2 4913  
E-mail: [nicolai.kellerer@kit.edu](mailto:nicolai.kellerer@kit.edu)