UNIVERSITÄT DUISBURG ESSEN

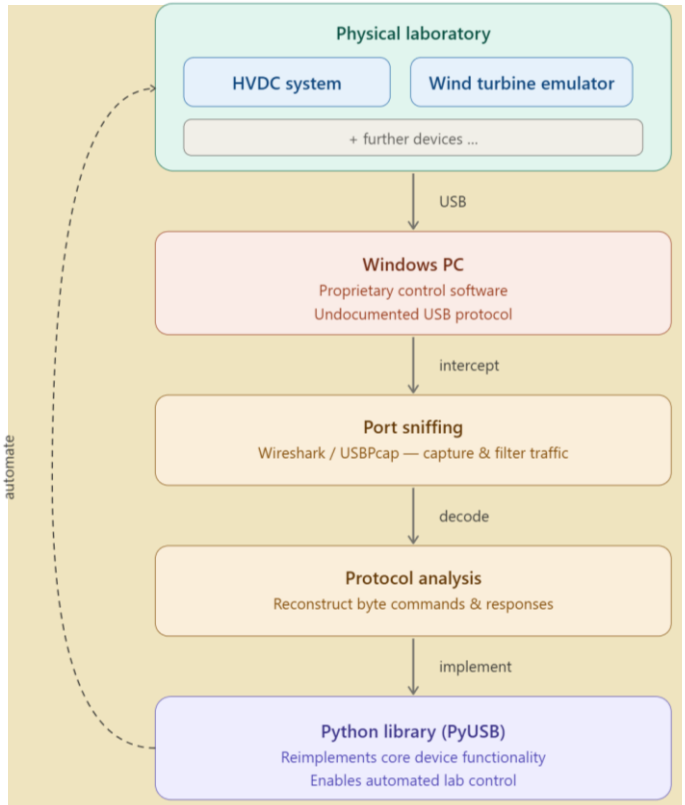
Offen im Denken

Fachgebiet für Elektrische Energiesysteme (EES)

Reverse Engineering and Python Implementation of a USB Device Communication Interface

Power-Hardware-In-The-Loop (PHIL) laboratories offer valuable opportunities for hands-on experimentation with control and automation concepts. A key long-term goal is the comprehensive automation of all devices within such a lab — enabling use cases like remote experiments, automated test sequences, and integration into higher-level control systems. A first step towards this goal is the **individual automation of each device** in the lab, including an HVDC system and a wind turbine emulator. These devices are currently controlled via **proprietary Windows software** that communicates over **USB** using an **undocumented binary protocol**. Since no protocol documentation is available, the communication must be **reconstructed independently through port-sniffing** — i.e. capturing and analyzing the USB traffic using tools such as Wireshark and USBPcap.
The work encompasses the following tasks:

- **Systematic capture and analysis of USB traffic generated by the existing Windows application**
- **Decoding of binary command-response sequences to reconstruct the protocol structure (in accordance to successful example)**
- **Development of a Python library (e.g. using PyUSB) reimplementing a defined subset of core device functionality**
- **Validation of the implementation against the physical device and documentation**



Supervisor and contact person

- **Marc Wöstefeld**
  marc.woestefeld@uni-due.de, +49 (0)203 379 1015, BA060

Candidate

- Nurin Binti-Shaheran