HiWi Position

Model wind turbine for cyber attack demonstration development and improvement

We developed a model wind turbine with an active pitch control system to demonstrate cyber attacks. The turbine can be directed from an ESP32 based wireless console and is controlled by a Siemens S7 PLC. It can operate in different modes as generator or as a motor for scripted or wind-still scenarios. The purpose of our model is to demonstrate attacks on wireless communication and unsafe applications in a visible manner.

Your job will be to implement the existing plans into code for all the components, more specifically ESP32 microprocessors and a Siemens S7 PLC. The desired goal is to get all components to work together in a integrated way with clean, custom PCBs and 3D printed parts. You will not have to design the circuits and PCBs.

When all parts are set-up and working, we want you to develop simple attacks on the ESPnow wireless communication and the S7 control unit to demonstrate cyber attacks.

Main Tasks:
- Programming the remote console, an ESP32 controller and a PLC controller
- Implementing further refinements like limit switches
- Documenting the project for replication in the future
- Develop simple attacks and exploits

Education, experience and skills:
- Studies in Computer Science or Electrical Engineering
- Know your way around 5V circuits or no fear to learn it
- Coding with Microprocessors like ESP32 or Arduino or no fear to learn it
- C / C++ programming
- (Optional) 3D modelling

What we offer:
- A fun project with electronics and 3D printing
- An opportunity to learn various skills
- Possible thesis within our research group
- Variable working hours for optimal studies

Richard Rudolph
Robust Secure Automation (RSA)
richard.rudolph@kit.edu

Institute for Automation und Applied Informatics (IAI)
Karlsruhe Institute of Technology, Campus North
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen