DPS1: Threat modelling for digitalized power systems

PhD student: Engla Rencelj Ling, englal@kth.se
Supervisors: Mathias Ekstedt (KTH) and Lars Nordström (KTH)

Project funded by:
“Which are the potential cyber attacks against our power systems and which cyber attacks are the most important to defend against?”
Threat Modelling

- Attack Graph / TTC
  - Generate Attack Graphs for Security assessments
- ModelLang
  - Create a language for the system model (what should be included)
- System Model
  - Develop a model of the system
- System
  - The system itself
Plan of Action

Systematic Literature Review of Information Sources for creating Threat Models
First iteration: SCL-Lang
Second iteration: sasLang

Gather statistics for attack simulations
Estimating Time-To-Compromise for ICS Vulnerabilities
Information Gathering from Professional Pentesters

Method of Validating threat modeling languages
Validation of sasLang

Testing and validation of predictions

Build the threat modelling language
Thank you!

Engla Rencelj Ling
englal@kth.se