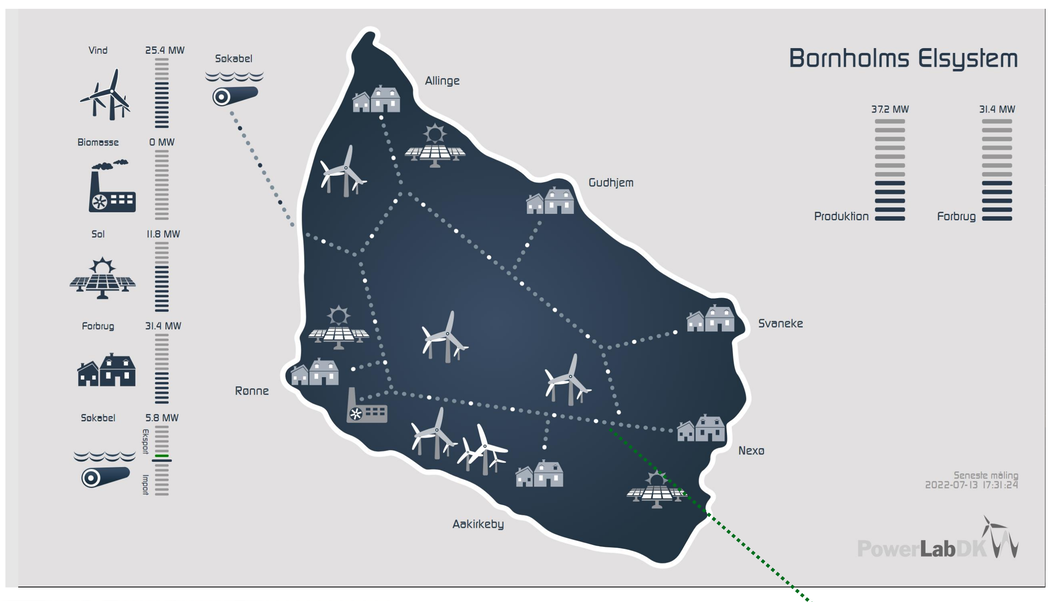
Cyber-Secure Operation of Battery Energy Storage Systems Providing Grid Services

Nina Kharlamova , Seyedmostafa Hashemi, Chresten Træholt
DTU Wind and Energy Systems, Technical University of Denmark (DTU)

PhD student
Nina Kharlamova
ninkhar@dtu.dk
+45 91411971

What is the practical purpose?



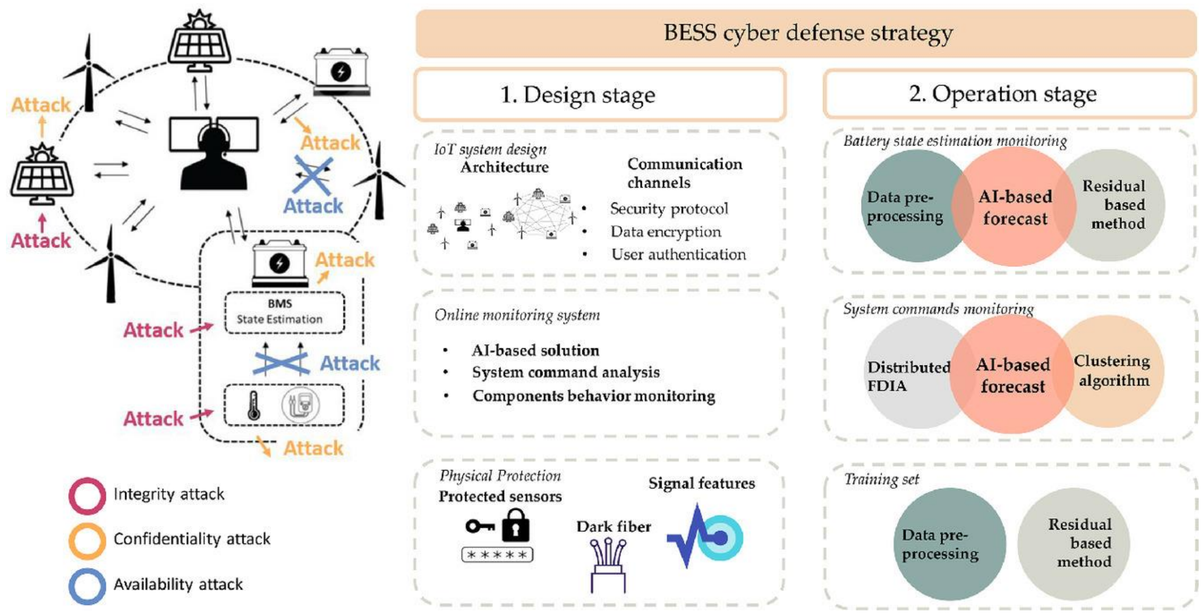

DTU PowerLab 79kWh/ 2x55kW

Bornholm 1MWh/ 1MW

Highlights –why cybersecurity is relevant?

- Utility-scale battery energy storage systems are vulnerable to cyberattacks.
- There is a lack of extensive review on the battery cybersecure design and operation.
- We review the state-of-the-art battery attack detection and mitigation methods.
- We overview methods to forecast system components behavior to detect an attack.
- We discuss how ML and AI-based methods can support cyber defense of battery systems.

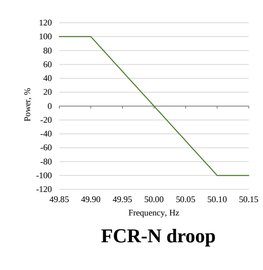
How to protect your battery?



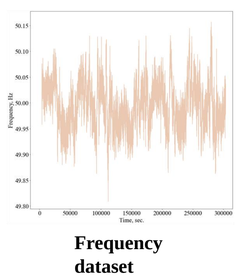
Abstract

This study reviews state-of-the-art methods for securing Battery Energy Storage Systems (BESS) from cyber threats. It focuses on detecting and mitigating potential cyberattacks on BESS using machine learning and artificial intelligence techniques. The study also investigates the design and operation of a secure BESS and suggests potential methods to detect new cyberattacks. In addition, various machine learning techniques are compared for accurate state of charge estimation of BESS using real data from PowerLabDK, providing a helpful guide for time series forecasting in BESS.

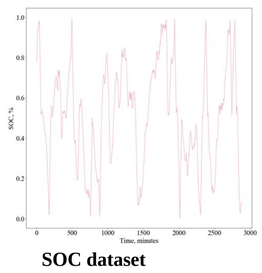
What should we know before modeling?



FCR-N droop



Frequency dataset



SOC dataset

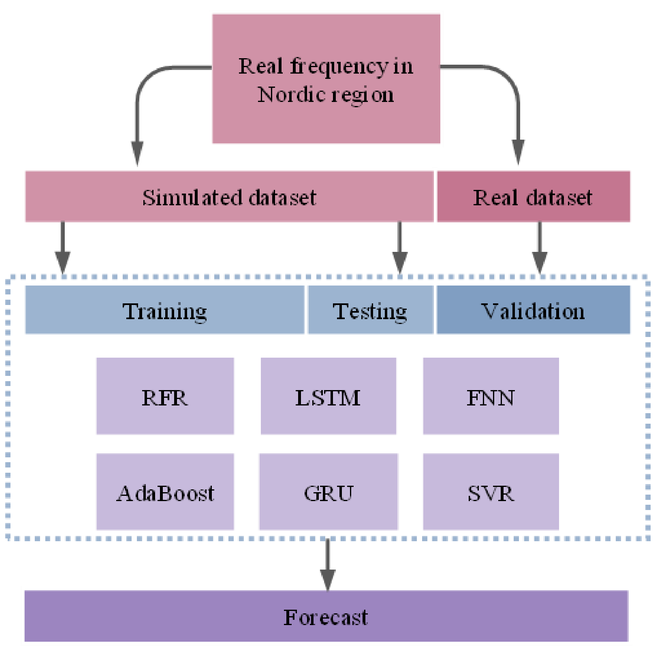
Ongoing work:

BOSS Project: Bornholm Smartgrid Secured – by grid-connected battery systems

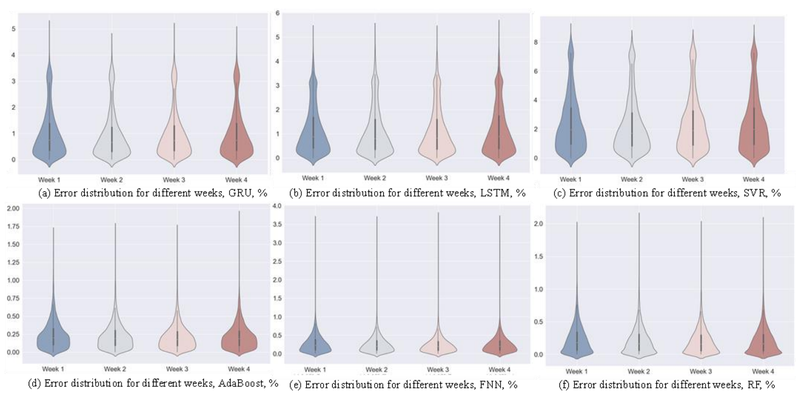
- Increasing the size of a real dataset and attack models;
- Creating a cyberattack detector and validating its performance;
- Testing a detector on the group of batteries working as virtual power plant;
- Applying mitigation algorithm to ensure flawless performance.

What is the future?

Machine learning

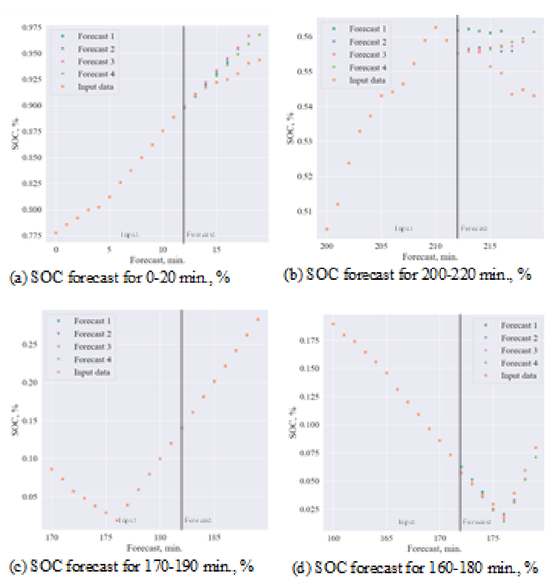


Accuracy of methods



The accuracy of prediction has to **be higher** that the **cyberattack vector size**.
We compare best methods on dataset, comparing both **accuracy** and **computational heaviness**.

Examples of forecast for different patterns



Evaluating Machine-Learning-Based Methods for Modeling a Digital Twin of Battery Systems Providing Frequency Regulation, N Kharlamova, S Hashemi, IEEE Systems Journal