
DTU

Nina Kharlamova, ninkhar@elektro.dtu.dk

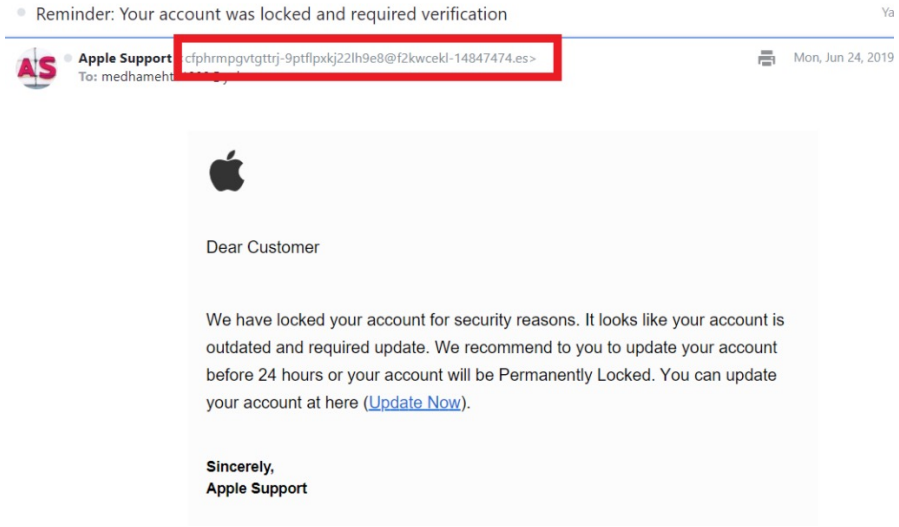
How can AI (and ML) make Utility-Scale Batteries more Cybersecure?

What is cybersecurity?

- *Cybersecurity* - The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
- *Cyberattack* - an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks

Expectation

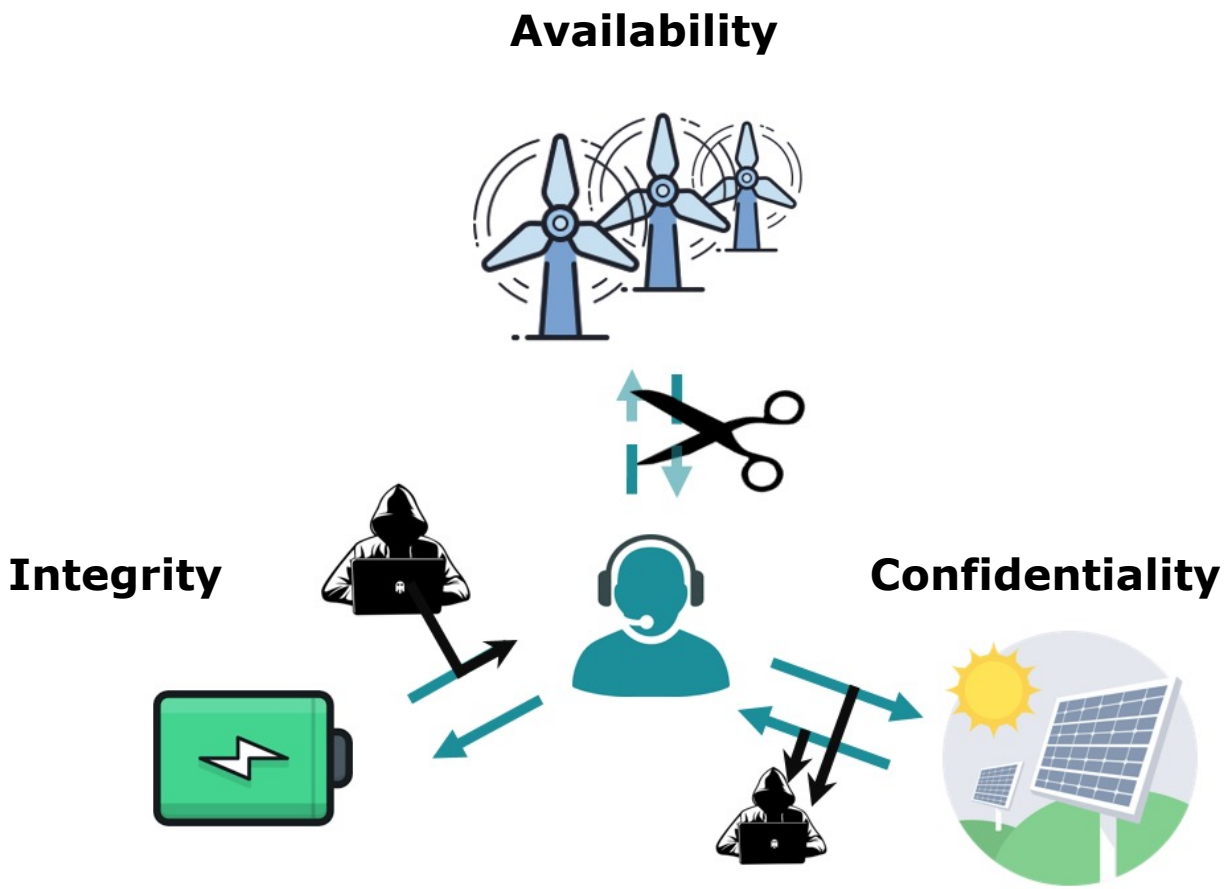
Reality



Background: why cybersecurity is important?

- According to Security Magazine, there are over 2,200 **attacks** each day which breaks down to nearly 1 **cyberattack** every 39 seconds;
- Energy sector is highly vulnerable towards cyberattacks since the failure can cause **economical** and **physical damage**;
- In Ukraine 2015, a total of **30 electrical substations** were switched off and around **230,000 people** were left without electricity for up to six hours;
- Cyberattacks are constantly evolving using **up-to-date technologies**, e.g. machine learning.

Types of cyberattacks based on data features violation



Types of cyberattacks based on data features violation

Data feature	Type of attack	Potential consequences	Real examples
Integrity	False data injection (FDIA), replay attack	Losing system's observability, wrong control commands resulting in economic losses	Energy theft (commercial losses), Stuxnet worm compromised work of nuclear power station in Iran
Confidentiality	Phishing, Man-in-the-Middle	Using stolen data to make better cyberattacks, hiding fault in the system, economic and physical damage	Blackout in 225 000 households in Ukraine due to phishing
Availability	Denial of service (DOS)	Losing system observability and control over the part of the system	More than 5 DOS attacks against the USA electrical grid over the last 2 years

Bornholm example:

1MW/1MWh BESS – the largest battery in Denmark to date

How to protect a system from cyberattacks?

System design

- System architecture
- Data protection
- Additional protection

Online attack detection

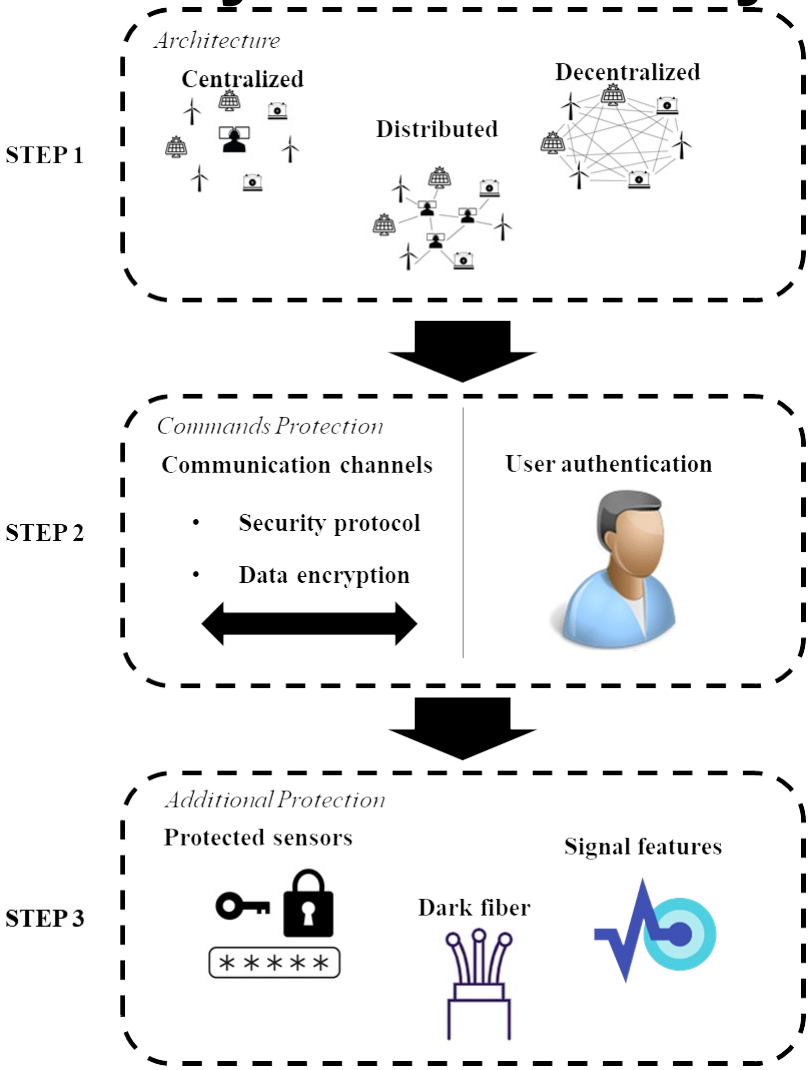
- System behavior forecast
- Residual based method

What kind of data can be injected into the system?

- False consumption data (**commercial losses**);
- **Random data** with zero mean (to maintain consumption-production balance).

  First cyberattack suggested for electric grid in 2009 by Lui;
- **Replay** attack;
- Targeted false data (used to achieve a **particular goal**, e.g. degradation of the battery);
- Targeted false data to cover **physical damage** (combining shortcut in line with cyberattack of normal line operation);
- Unknown attack.

Cyber secure Utility-scale battery design

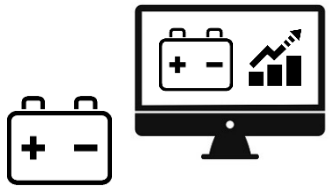


How to detect cyberattack?

Define and model an attack

Forecast battery state of charge

Compare forecast with measurements



Test an algorithm

SOC forecasting methods

Model-based Methods	Data-driven Methods	Pseudo measurement generation
• Equivalent circuit model • Extended Kalman filter	• Support Vector Regression • Artificial Neural Network • Random Forest • Gaussian Process Regression • Fuzzy logic • Hybrid approach	• Probabilistic neural network • Parallel distributed processing network • Artificial Neural Network • Clustering

Battery state estimation	Dealing with missing data

Summary

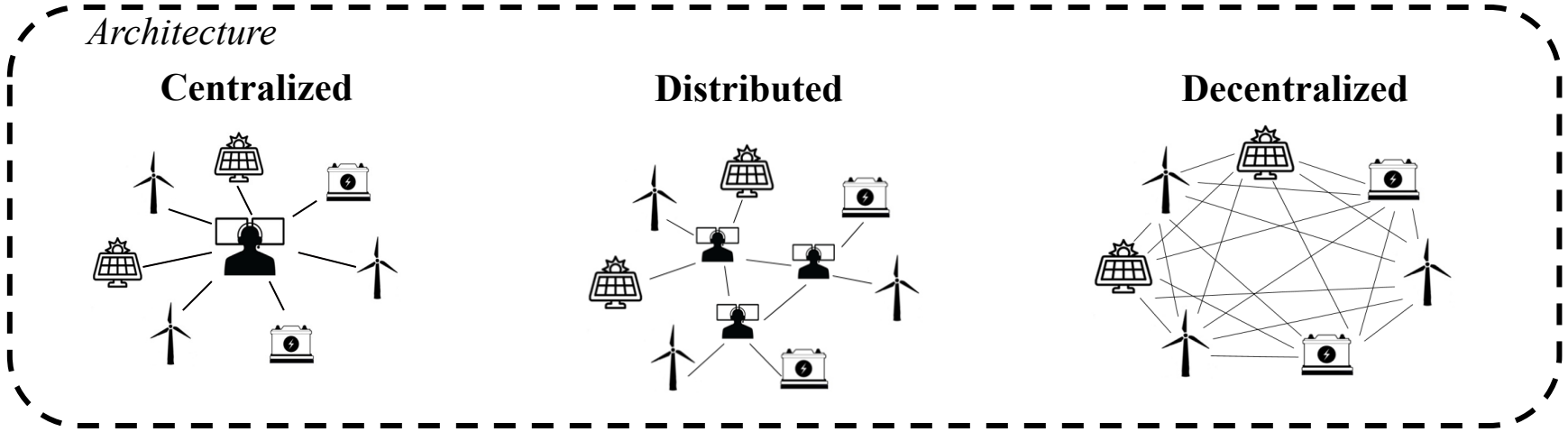
- Cyber security is an important concern for a **battery design and operation**;
- Cyberattack on a component of energy system can cause **economical** and **physical damage**;
- **Cyber security** is to be ensured both on the design and operational stages;
- Reliable **forecast** tools are needed to detect and mitigate a cyberattack;
- Cyberattacks are changing and evolving so we have to be **creative**.

Cyber secure BESS design – Step 1

A **system architecture** is the conceptual model that defines the structure of a **system**

- *Centralized architecture* – all nodes are connected to the control unit.
- *Decentralized architecture* – all nodes carry out decision making process on their own.
- *Distributed architecture* – the processing is shared across multiple nodes, but the decisions may still be centralized and use complete system knowledge.

STEP 1



Cyber secure BESS design – Step 2

Method	Tool	Description	Safety level
Cryptography	Communication protocols	Such as HTTP (*HyperText Transfer Protocol*), SOAP (*Simple Object Access Protocol)* are used to exchange data that does not have to be secured	Low
	Symmetric key	The same key is used to encrypt sent data and decrypt received one	Medium
	Asymmetric key	There are different keys for encryption and decryption	High
User authentication	Password	User authentication decreases the chance of Denial of Service attacks when the system is overloaded with requests. It prevents attackers from manipulating, copying and falsifying system data.	Medium
	Biometric data		High
	Two-factor authentication		High

Cyber secure BESS design – Step 3

- Restricting physical access;
- Regular patches;
- Disabling unused ports and services;
- Adopting the principle of least privilege – using software, sharing data that is minimum needed to fulfill the task;
- Using antivirus programs;
- Minimizing data-in-transit manipulation, falsification, or spoofing;
- Employing intrusion detection and prevention systems;
- Maintaining functionality under duress—redundant critical components, restorations plans, fault tolerant systems.