KAPSARC
مركز الملك عبدالله للدراسات والبحوث البترولية
King Abdullah Petroleum Studies and Research Center

Cybersecurity perspectives in the energy and power systems: An Overview

Ahmed Albalawi
Khalid Alhadhrami
Faris Aljamed

July 2023

Context

Important to realize that while cyber threats are low frequency, high consequence events. They are also very probable to happen.

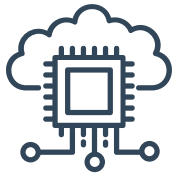
Cybersecurity in the power system is growing in importance with the transition to smart grid and electrification of other sectors

Millions of daily cyber attacks on energy infrastructure occurs with increased sophistication. Complacency is not allowed

Cybersecurity is a critical issue across various fields, including the power sector, electric vehicle infrastructure, and critical infrastructure.

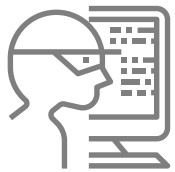
Drivers for cybersecurity in the power system

Distributed energy resources and increased connected devices



Digital transformation; enhanced use of data, automation, and interoperability

Industrial Control Systems protection amid use of hybrid IT environments



Cyber attacks sophistication on IT and OT systems

Increased recovery cost from a cyber attack

Methodology

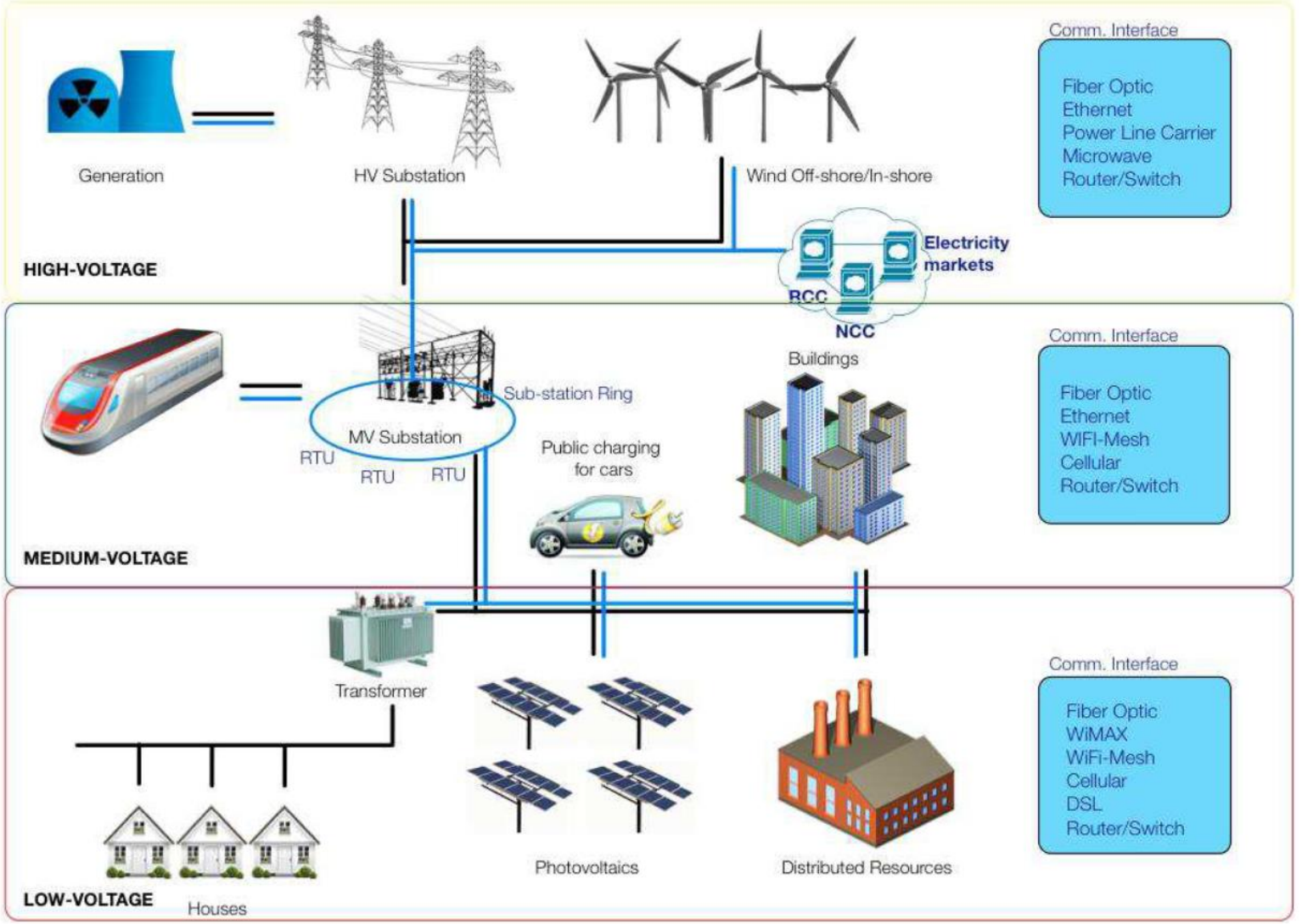
A comprehensive literature review was conducted to look at looks at the cybersecurity across three specific fields, namely:

- cybersecurity in the power sector.
- cybersecurity in the electric vehicle infrastructure.
- cybersecurity in critical infrastructure.

Over fifty papers were reviewed and synthesised to reach an overview of the emerging cybersecurity threats and policy responses in the electric power sector.

Focus on the papers scope, challenges identified, and solutions presented.

Physical consequences of a cyber attack are growing with the increased connectivity in the communication infrastructure including industrial control systems



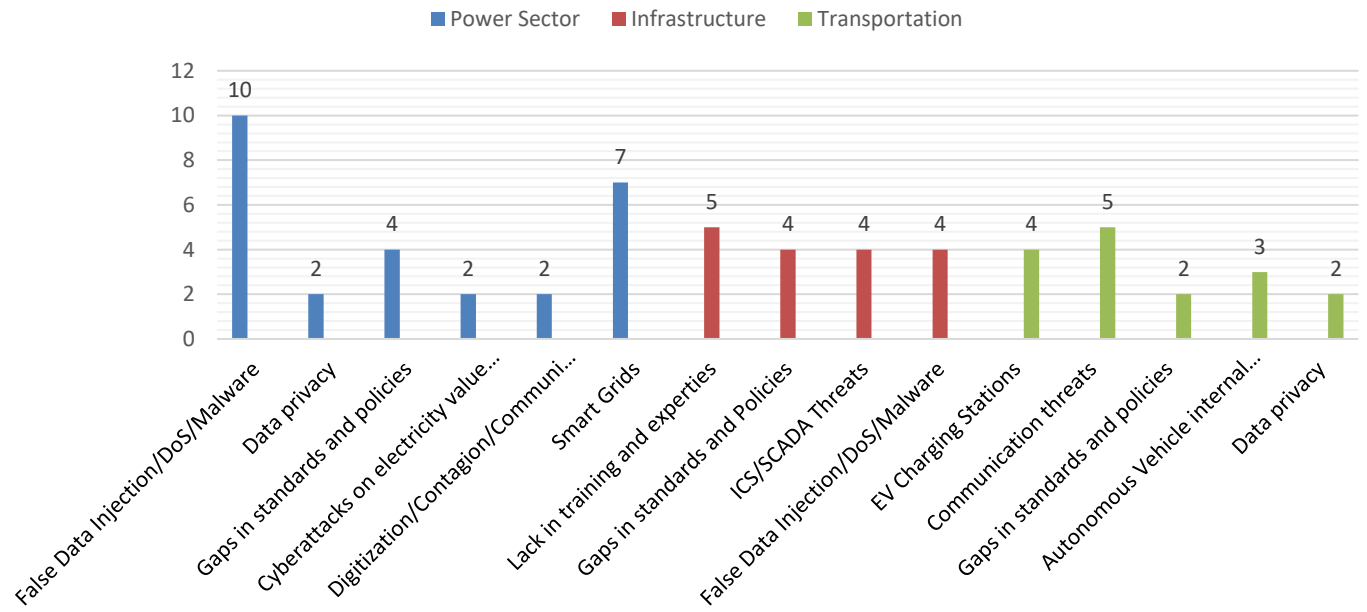
Graph source: Sanchez Torres, José Libardo. 2013. "Vulnerability and Interdependencies of coupled infrastructures: Power Distribution Network and ICT." Engineering Sciences. Université de Grenoble. DOI:10.13140/2.1.1234.5129.

Common cyber threats – power sector

Transition to smart grids represents a big challenge to the power sector

Several papers referred to the inadequate standards and policies to keep up with the increased digitalization.

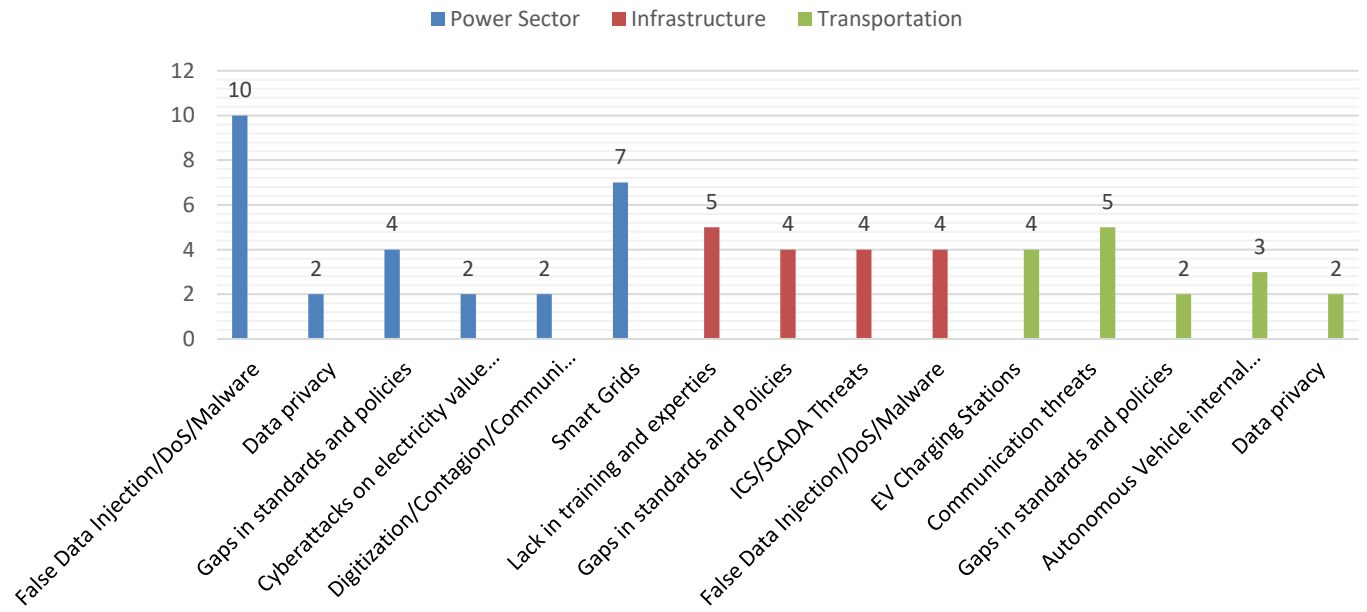
The importance of data governance and protection is highlighted.



Common cyber threats – critical infrastructure

Threats are broad since it covers multiple sectors.

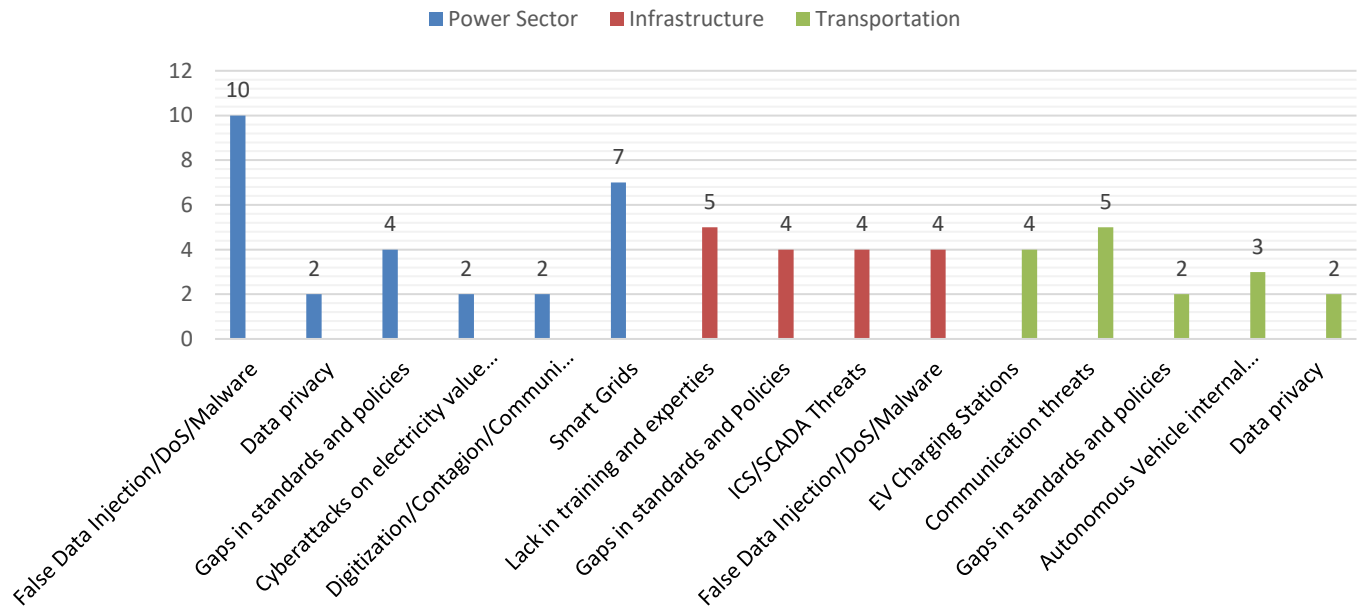
One threat to note is the lack in training and expertise. The challenge in training is not only in developing the training materials but also in engaging the end users in these training.



Common cyber threats – transportation

EV charging stations is a major concern as it is the interface between two sectors.

communications safety against all attacks that could affect the operation of the EV fleet is strongly highlighted



Considerations for response

A grid scale cyber attack would pose tremendous challenge technically and logistically

Lack of financial and human resources limit ability to address legacy technology issues

Grid resiliency phases: robustness – resourcefulness – recovery – adaptability

Governance framework for cyber response clarifies the chain-of-command and the roles of different stakeholders

Cybersecurity should be part of the system design and engineering

Solutions to address cyber threats

Invest in new cybersecurity technologies. This includes intrusion detection systems, software-defined networking, and blockchain.

Train employees on cybersecurity best practices.

Develop incident response plans. This will help to minimize the impact of a cyberattack.

Share information and coordinate with other organizations.

Adopt a cross-sectoral approach to cybersecurity. This recognizes that cybersecurity is an issue that affects all sectors of the economy, not just the energy sector.

Develop cybersecurity standards that are specific to the sector.

Monitor the cybersecurity landscape and adapt as needed. The threat landscape is constantly evolving, so it is important to be able to adapt to new threats.

Role of regulator in driving cybersecurity measures

Framework with clear responsibilities of stakeholders

Increase information flow without compromising data privacy

Continuous communication between the utility and regulator

Data policy and third-party access

Frequent audits of utilities practice

Adoption of standard framework

Awareness and training

Incentivizing cybersecurity investments

Thank you