**Cyber Security Roadmap for System Lockout (Physical Attack)**

**Introduction**

To improve the efficiency and reliability, a significant investment has been made by industry and government to build a smarter and more automated/connected power grid system.

<https://www.sciencedirect.com/science/article/pii/S0142061517328946>

Since power grids span a wide geographic area, public and private networks (e.g., fiber optics, RF/microwave, cellular) can provide a communication path between remote sites and a control center. These capabilities also open doors for attackers to access a power grid and cause disruptions to the normal operation of the grid.

The roadmap focuses on the intersection of industry and government and recommends activities in four related areas: stakeholder engagement, cyber security research and development, standards development, and industry best practices.

Jay Johnson, 2017, Roadmap for Photovoltaic Cyber Security, Sandia Report, SAND2017-13262, 66 Pages

**Background**

Cybersecurity is a serious and ongoing challenge for the energy sector. Cyber threats to energy delivery systems can impact national security, public safety, and the national economy.

<https://www.energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf>

A Cyber security attack in Ukraine left 225,000 people without power.1 A similar attack was carried out a year later that caused an outage of 200 MW2.

Jay Johnson, 2017, Roadmap for Photovoltaic Cyber Security, Sandia Report, SAND2017-13262, 66 Pages

Cyber security

Many industry and government reports have identified that cyber intruders have become a serious threat to the secure operation of a smart grid. Forty-six [cyber attack](https://www.sciencedirect.com/topics/engineering/cyber-attack) incidents have been reported in the energy sector in 2015, most of which targeted the IT system of utilities and vendors. The U.S. Department of Energy (DOE) indicates that the actual number of cyber attacks is higher than reported . To identify and eliminate cyber vulnerabilities in a smart grid, methods to detect cyber intrusions and mitigate their impact need to be developed.

**Technology Gaps /drivers**

* Without physical security of the building and network, hackers or even an employee can exploit it.
* One of the most important problems of Cyber security is the lack of a fast and easy authentication method.

Physical Attack

Computer controls depend upon some kind of digital connection to a control mechanism. A physical attack on a sub-station can disable that control connection, as was done at the Metcalf sub-station in San Jose, California [15], where the telephone cables providing the control signals were physically cut prior to a kinetic attack. So, the assumption of continuous cyber connection is not necessarily valid. A nefarious actor with access to a switch box would need do no more than disconnect ethernet cables to cause havoc in the command-and-control network. In the generation of a technology roadmap, it may be necessary to consider redundant communication techniques, especially where critical control mechanisms are concerned. If the system relies on a single point of failure, it is easier to disable the system.

<https://drive.google.com/drive/folders/1JZ-iMoaqjT48FXtyM5cw6xIVHcNrFNe->

**Market Drivers**

* Electricity transmission losses
* Frequent power outages
* Electromobility
* Grid modernization
* Threat of cyber attacks
* Threat of terrorist attacks

<https://fuergy.com/blog/7-problems-and-challenges-of-a-power-grid>

**Objectives**

* Identifying Strategic Risks
* Security Tools and Practices
* Control Systems Architecture
* Guiding and Aligning Existing Efforts
* Addressing Critical Needs and Gaps
* Proposed Mechanism for Oversight and Project Management
* Facilitating Energy Sector Operation
* Evolution of Control Systems
* Escalating Threats and New Vulnerabilities
* Strategies for Securing Control Systems
* Key Stakeholders

<https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf>

**Methodology**

1. Auditing and mapping the network to increase the security
2. Always keep the network updated to increase network security
3. Physical network security
4. Consider MAC Address filtering: (Although it is possible to bypass the MAC address filter by changing the physical address, it can at least act as a first layer of security. This feature won't stop hackers, but it can help you prevent unauthorized employees and equipment from connecting.)
5. Use a virtual private network for secure data transfer
6. Encrypt the entire network

**References**

1. <https://www.osha.gov/etools/electric-power/hazardous-energy-control/lockout-tagout-generation>
2. <https://www.osha.gov/etools/lockout-tagout>
3. <https://safetyculture.com/topics/lockout-tagout/>
4. <https://www.ijaar.org/articles/v8n5/sms/ijaar-v8n5-May22-p8505.pdf>
5. Jay Johnson, 2017, Roadmap for Photovoltaic Cyber Security, Sandia Report, SAND2017-13262, 66 Pages