Supplemental Project Notice

SUBSTATION DETECTION DEVICES AND IEMI IMPACT

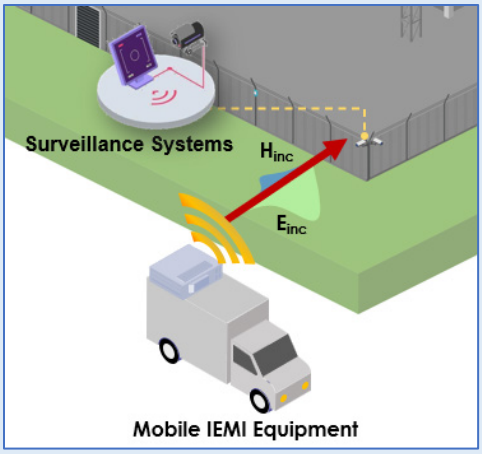

Figure 1: Illustration of IEMI attack on a substation security camera system using a portable weapon

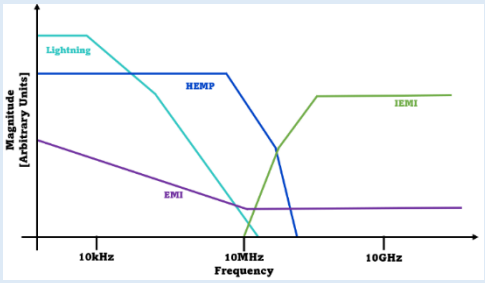

Figure 2: IEMI frequency spectrum compared to E1 HEMP and lightning

PROJECT HIGHLIGHTS

- Technical guidance and tools for assessing the potential impacts of IEMI on substation physical security and detection systems.
- Options for mitigating the potential impacts of IEMI on physical security systems.
- Improved understanding of the costs and potential unintended consequences associated with employing IEMI mitigation.

Background, Objectives, and New Learnings

Intentional electromagnetic interference (IEMI) refers to a manmade electromagnetic attack where the target, for example, cameras or door access controls inside a substation, are intentionally subjected to intense electromagnetic (EM) and/or electrical signals. Like the threat posed by early-time high-altitude electromagnetic pulse (E1 HEMP), IEMI threats can be categorized as either radiated or conducted. In the case of a ***radiated attack***, a high-voltage source is connected to an antenna and is used to generate an intense electromagnetic field that propagates through the air and unshielded infrastructure and interacts with electronic systems directly or through coupling to cables that are connected to the device(s). ***Conducted attacks*** use exposed physical wiring to inject high-frequency signals directly into the affected systems with the intent of disrupting or damaging connected equipment. Both attack vectors require some level of sophistication and physical access to the target location.

IEMI sources vary in technology, capabilities, and mobility. Radiated and conducted IEMI signals can be broadband or narrow band and delivery systems can be small portable devices that fit inside of a suitcase or larger devices that require a vehicle to transport. Radiated field amplitudes can be 150 kV/m or higher with frequency content up to 20+ GHz as shown in Figure 2.

EPRI has begun to consider the possibility that an IEMI weapon could be used to disable substation physical security and detection devices, such that a bad actor could gain unrestricted access to a substation.

Physical attacks on a substation have become an ever-increasing threat to the reliability of the electrical gird. Some of these incidents have resulted in thousands of customers with an outage. Through this, EPRI is looking to identify risks in this physical security space. Ongoing research in this area has indicated that substation electronics exhibit significant vulnerabilities to radiated IEMI attacks, making this a potentially feasible method of attack.

Additionally, IEMI may represent an attractive attack vector for the following reasons:

- Radiated electromagnetic fields generated by IEMI weapons can penetrate physical boundaries such as fences and walls.
- IEMI attacks can be undertaken covertly and anonymously by state actors or criminals with minimal obvious evidence left after a failed attempt.
- There is significant potential to disable or disrupt functionality of critical systems and infrastructure.
- IEMI sources and their components are available on the open market; many are small and highly mobile, for example the suitcase weapon shown in Figure 1.

While EPRI and the electric utility industry have made significant progress understanding the potential impact of E1 HEMP on electric power infrastructure and have identified methods for mitigating the impacts, little information is available regarding the potential impacts of IEMI to electronic systems that support substation physical security. The primary objective of this research is to improve the industry's understanding of IEMI threats applied to physical security and how to mitigate them in a cost-effective way by leveraging the vast body of knowledge and resources developed through EPRI's ongoing E1 HEMP and IEMI R&D programs.

Benefits

This project can potentially provide the following benefits:

- Technical guidance and tools for assessing the potential impacts of IEMI attacks on substation physical security and detection systems.
- Options for mitigating the potential impacts of IEMI on substation physical security and detection systems.
- Improved understanding of the costs and potential unintended consequences associated with IEMI hardening.

Project Approach and Summary

This project will leverage prior and ongoing R&D in the area of high-altitude electromagnetic pulse (HEMP) and IEMI. Specific tasks planned for this project include:

Task 1: Determination of physical security and detection devices commonly used in substations through surveys and site visits followed by procurement of identified systems.

Task 2: Laboratory testing of equipment and systems identified in task 1 using EPRI's mesoband IEMI source. This task may include procurement of additional IEMI sources as appropriate.

Task 3: Determination of mitigation options based on the vulnerability of equipment demonstrated during task 2.

Deliverables

This section lists the deliverables you may expect to get from this project.

- A technical guidebook summarizing the methodology and results for each project task, enabling the reader to assess the potential impacts of IEMI on substation physical security systems as well as providing guidance to develop engineering solutions to mitigate the potential impacts.
- Final workshop and periodic update WebEx meetings.

Price of Project

The price of the project is $40k per year for two years ($80k total).

Project Status and Schedule

This two-year project is expected to start in Q1 2025.

Who Should Join

Asset owners responsible for the resiliency, reliability, and security of transmission, distribution, or associated systems.

Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 (askepri@epri.com).

Technical Contacts

Erika Willis at 704.595.2670 (ewillis@epri.com)
Josh Butterfield at 865.217.5041 (jbutterfield@epri.com)

Additional Contacts

Northeast: Dan Tavani at 704.595.2714 (dtavani@epri.com)
Southeast: Brian Long at 704.595.2875 (blong@epri.com)
Central: Jeff Hlavac at 972.556.6553 (jhlavac@epri.com)
West: David Welch at 650.855.1072 (dwelch@epri.com)

Product ID: 3002031076 **Project ID:** 1-120172 **October 2024**

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA • 800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com