EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Proceedings of the EPRI/NATF Summit on Electromagnetic Pulse (EMP)

Utility Needs, Gaps, and Next Steps

3002004027

Proceedings of the EPRI/NATF Summit on Electromagnetic Pulse (EMP)

Utility Needs, Gaps and Next Steps

3002004027

Technical Update, June 2014

EPRI Project Manager

R. Lordan

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THE FOLLOWING ORGANIZATION PREPARED THIS REPORT:

Electric Power Research Institute (EPRI)

This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization prepared this report:

Electric Power Research Institute (EPRI)
3420 Hillview Avenue
Palo Alto, California 94304

Principal Investigator
R. Lordan

This report describes research sponsored by EPRI.

EPRI gratefully acknowledges the participants of the EMP Summit, conducted April 2-3, 2014 at the EPRI Conference Center in Charlotte, North Carolina.

This publication is a corporate document that should be cited in the literature in the following manner:

Proceedings of the EPRI/NATF Summit on Electromagnetic Pulse (EMP): Utility Needs, Gaps, and Next Steps. EPRI, Palo Alto, CA: 2014. 3002004027.

ABSTRACT

Power system operations in increasingly complex electromagnetic components lead to increased vulnerability to attack by electromagnetic pulse (EMP), high altitude EMP (HEMP), and intentional electromagnetic interference (IEMI). The increasing adoption of digital microprocessor-based systems, including smart grid technologies, may be increasing this vulnerability due to the typical lower operation voltage required compared to legacy analog technology.

To begin a process of addressing EMP threats, EPRI and the North American Transmission Forum (NATF) jointly sponsored an EMP Summit at EPRI's Charlotte offices April 2-3, 2014. EPRI and NATF have similar and complementary missions with common stakeholders and interests as well as a memorandum of understanding to collaborate on issues affecting grid reliability, security, and resiliency.

The purpose of the EMP summit was to review the state of the science of EMP, understand the potential threats that electricity providers are facing, and identify knowledge gaps and next steps. More than 50 representatives from utilities, regulatory, and government agencies, NATF, and EPRI participated in two days of information sharing and insights. Participants presented a wealth of superior practices, approaches, insights, and recommendations for technology research. Participants also expressed significant interest in ongoing collaboration and coordination.

Keywords
Electromagnetic Pulse (EMP)
EMP hardening
Grid resiliency
High-altitude EMP (HEMP)
High impact, low-frequency events (HILF)
Intentional Electromagnetic Interference (IEMI)
Spares strategy
System restoration

CONTENTS

LIST OF FIGURES

1
INTRODUCTION

Background

Power system operations in an increasingly complex electromagnetic components lead to increased vulnerability to attack by electromagnetic pulse (EMP), high altitude EMP (HEMP), and intentional electromagnetic interference (IEMI). The increasing adoption of digital microprocessor-based systems, including smart grid technologies may be increasing this vulnerability due to their typical lower operation voltage required, compared to legacy analog technology.

To begin a process of addressing EMP threats, the Electric Power Research Institute (EPRI) and the North American Transmission Forum (NATF) jointly sponsored an EMP Summit at EPRI's Charlotte offices April 2-3, 2014. EPRI and NATF have similar yet complementary missions with common stakeholders and interests, and have a memorandum of understanding to collaborate on issues affecting grid reliability, security, and resiliency.

The purpose of the EMP summit was to review the state of the science of EMP, to understand the potential threats that electricity providers are facing, and to identify knowledge gaps and next steps. This was the fourth industry summit in a series cosponsored by EPRI and NATF. Previous summits addressed Grid Resiliency, Physical Security, and Geomagnetic Disturbances (GMD).

More than fifty representatives from utilities, regulatory and government agencies, NATF, and EPRI participated in two days of information sharing and insights. Participants presented a wealth of superior practices, approaches, insights, and recommendations for technology research. Participants also expressed significant interest in collaboration and coordination. Although government agencies may assume principal responsibility for protecting the grid from an EMP attack, the participants believe there is an appropriate role for the electricity utility industry in areas including vulnerability assessment, hardening of critical components, and recovery.

Figure 1-1
EMP Summit, April 2-3, 2014

The summit included presentations from NATF, EPRI, and several utilities. Presentations were followed by facilitated discussions. In addition, EPRI staff conducted tours of laboratories on the Charlotte campus where EMP-related research and development are conducted.

Report Purpose and Organization

This report summarizes the EMP Summit presentations and participant discussions, and summarizes key conclusions, knowledge gaps, and next steps.

Chapter 1 provides an introduction and overview of the Charlotte EMP Summit.

Chapter 2 summarizes the fundamentals of EMP and potential effects on power systems, threat assessment and mitigation.

Chapter 3 presents utility perspectives and current activities in EMP planning, protection, and suggestions for best practices, as well as participant comments.

Chapter 4 summarizes conclusions and key messages from the summit, identifies opportunities for research, knowledge gaps, and next steps.

2
EMP 101: UNDERSTANDING THE THREAT

Introduction

The EPRI/NATF summit included overview presentations on the principal types of possible electromagnetic attacks with the potential to inflict damage to the power grid.

The information in this chapter is adapted from the summit presentation and from two recently published EPRI documents, which provide more detailed information:

- *Electromagnetic Pulse and Intentional Electromagnetic Interference (EMI) Threats to the Power Grid* (Report 3002000796),
- *Electromagnetic Pulses (EMPs) and the Power Grid* (white paper 1026426).

Additional information is contained in the references listed at the end of this chapter.

Definitions: EMP, HEMP, IEMI

The summit addressed three principal types of electromagnetic attack with the potential to damage electronics and disrupt power grids and other infrastructure including communications, computer networks, and transportation systems dependent on microprocessors or susceptible embedded electrical systems.

- Electromagnetic Pulse (EMP): An EMP is a short burst of electromagnetic energy unleashed by the detonation of a nuclear or other high-energy explosive device.
- High-altitude EMP (HEMP) – EMP from weapons detonated at high altitude to produce more widespread effects.
- Intentional Electromagnetic Interference (IEMI) – non-nuclear EMP attacks whose effects are similar in nature to nuclear EMP events but affect a more limited target area.

Altitude and Impact Area

A U.S. nuclear test conducted in 1962, called Starfish Prime, was the first to confirm in the field the potential widespread disruption of electrical devices by high-altitude nuclear explosions. The nuclear device was detonated at an altitude of 400 km (250 miles) over the Pacific Ocean 1445 km (900 miles) from Hawaii. The blast knocked out streetlights, damaged a telephone company's microwave link, set off numerous burglar alarms, and reportedly disabled automobiles on the islands. Despite the long distance from the test site, the damage in Hawaii was directly attributable to the EMP that was generated during the nuclear explosion [17, 18].

The impact area of the EMP is limited to the physical horizon of the Earth in relation to the location of the nuclear detonation [20]. For example, in the case of a ground detonation, the EMP damage radius spreads to the horizon, which is approximately 62 miles (100 km) depending on the topology of the surrounding terrain, as seen from the surface level. However, high altitude detonations, such as the 1962 experiment, provide a far wider horizon for EMP propagation (albeit with a commensurate reduction in energy per exposed area), so that its effects can spread over hundreds of miles [21]. Aside from their range and scope, these HEMP events are similar to the surface level ones in terms of basic physical characteristics.

Figure 2-1
Bust Altitude and Impact Area

Three Component Pulses of HEMPs

HEMPs generated by the detonation of nuclear devices create a three-component pulse, each with distinct characteristics as defined by the International Electrotechnical Commission (IEC). The commission labeled the sequential components E1, E2, and E3 [5]. Understanding the types of pulses is important to understanding potential power system impacts and countermeasures.

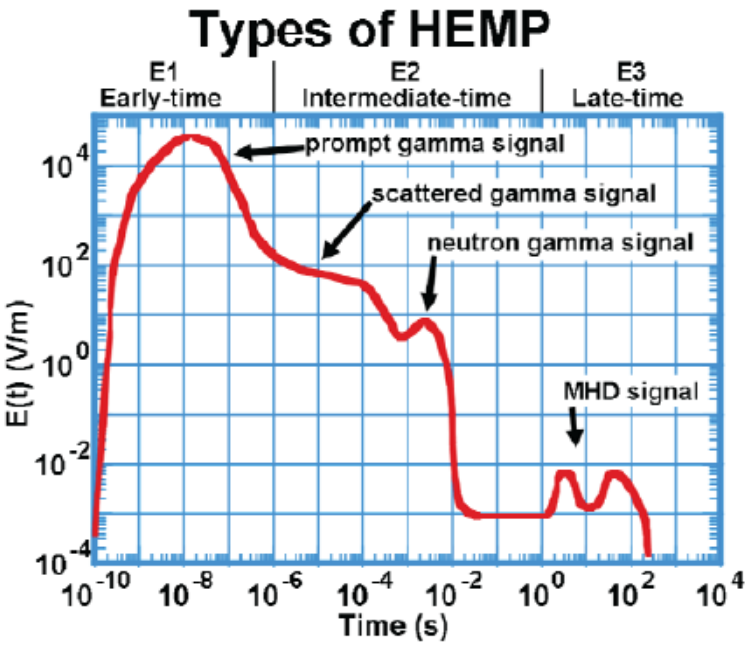

Figure 2-2
HEMP Characteristics

E1 Pulse

The first pulse, E1, generates a brief yet highly energetic electromagnetic field that induces extremely high voltages in any electrically conductive material. This E1 voltage is responsible for the most damage in any HEMP event or attack, as the high voltages induced may cause conductive materials such as processors, transmission and distribution lines, and other components to break down. The rapid, energetic impact may in some cases overwhelm traditional surge protection used to prevent damage from lightning strikes or sudden line voltage fluctuations [1].

Gamma radiation is generated by the high altitude nuclear explosion and produces the E1 pulse by dislodging electrons from upper atmospheric particles (via Compton effect). The Earth's magnetic field, forces the electrons, on a spiral trajectory around the geomagnetic field lines. Because of the geomagnetic field symmetrical pattern (essentially a dipole) for a blast near the equator, the severity of damage occurs in a roughly symmetrical (circular) pattern. North or south of the equator, these deflections would cause damage in a U-shaped curve (see Figure 2-3). An E1 pulse lasts approximately 1 microsecond [1].

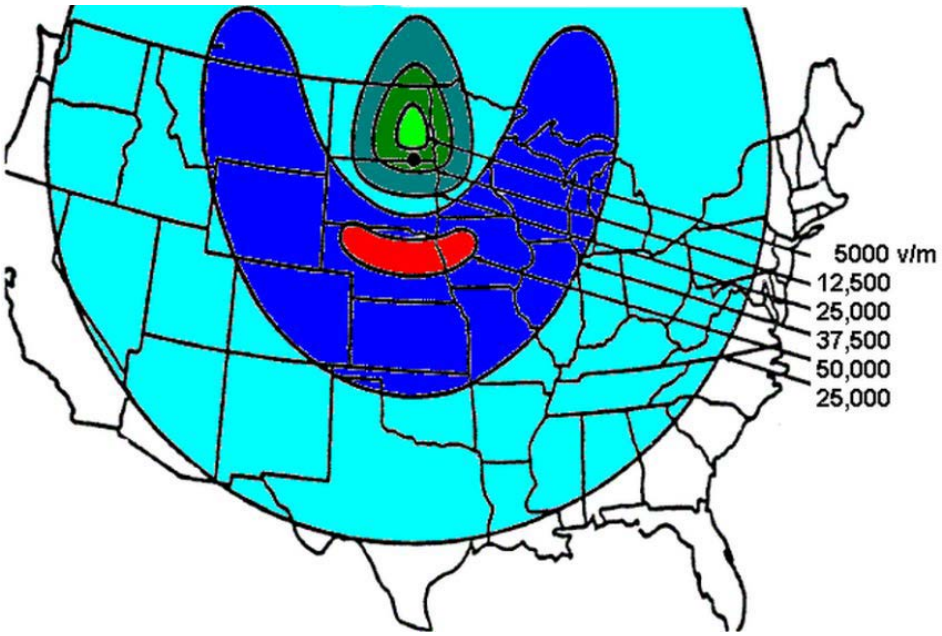

Figure 2-3
Pattern of HEMP E1 Pulse determined by of Earth's magnetic Field

E2 Pulse

The E2 pulse produced by HEMP explosions has characteristics similar to a conventional lightning strike, beginning approximately between a few microseconds to one full second after the onset of the E1 pulse. Because the energy associated with the E2 pulse is not nearly as intense as for the E1, it is easier to protect against its damage with conventional technology. However, due to the initial onslaught of power influx from the E1 pulse, some surge mitigation and protection measures might be already compromised. Consequently, the E2 pulse may pass relatively unhindered deep into the power grid, with potential damages to critical electronics [1].

E3 Pulse

The E3 pulse associated with an HEMP event is most similar in nature and potential impact to a geo-magnetic disturbance (GMD) experienced during an extremely strong solar flare strike on Earth. During the initial HEMP blast, a perturbation of the Earth's magnetic field is produced. This fluctuation may produce geomagnetic-induced currents in long electrical conductors. Lasting from tens of seconds to minutes in duration, the E3 pulse, similarly to the GMD from a solar storm, has the potential for creating damages to large transmission line transformers[1].

Non-Nuclear EMP Weapons

Military agencies have developed non-nuclear EMP weapons that induce pulse voltages over limited, targeted strike zones. These weapons, if properly deployed, could cause damage to the electrical grid, command and control communications, transformers (potentially at any voltage level, due to the induced transients on the grid above nominal values) and electronic circuitry. While some of the effects of non-nuclear EMP attacks are similar in nature to nuclear HEMP events, they cover a much more limited target area. These threats are often referred to as intentional electromagnetic interference (IEMI) or high-power electromagnetic (HPEM) weapons.

At least one successful demonstration of a non-nuclear EMP weapon has been reported in the United States. On October 12, 2012, Boeing announced that it successfully tested its Counter-electronics High-powered Microwave Advanced Missile Project (CHAMP) over the Utah Test and Training Range. Boeing Phantom Works and the U.S. Air Force Research Laboratory reported that CHAMP emitted a high-powered microwave pulse at specific targets during its test flight. The pulse reportedly disabled data and electronic systems, including a room of computers, but caused no physical damage. Boeing reports that CHAMP followed a pre-programmed flight path during the test and claims that it can strike numerous targets during a single mission [7].

For the purpose of utilization in the battlefield, these devices attempt to disable enemy communications and transportation. As means for a widespread attack on a nation's infrastructure, non-nuclear EMP devices are impractical, but they could nonetheless easily target a city, specific generation facilities, or major communication hubs to cause significant, potentially long-lasting, material and economic damage. Because of the relatively simple design of such devices compared to nuclear weapons, it is conceivable that rogue nations or terrorist groups could develop a credible threat based on coordinated non-nuclear EMP attacks on a variety of targets.

Hence, the potential for two different types of threats exists. One type of threat is a limited-impact attack (e.g., an HPEM or IEMI), requiring less sophisticated—and more accessible—technology that can be carried out by a smaller organization or isolated individuals. Another type of threat is a catastrophic-scale HEMP attack that requires a nuclear weapon and ballistic missile launch and control capability that can only be carried out by a government with a technologically-developed military.

Potential Damage to Power Grids

Various agencies, including the EMP Commission, U.S. Department of Homeland Security, North American Electric Reliability Corporation (NERC), Energy Infrastructure Security Council, and members of the U.S. Congress, are expressing concerns about power system vulnerabilities to these various EM attacks or are recommending mitigation measures.

Today's power systems may be more vulnerable to electromagnetic attacks than in the past. This is partly due to the evolution toward digital electronics control systems. The widespread proliferation of smart grid systems, including advanced metering infrastructures and distribution and substation automation systems, illustrates this increasing complexity. The dependence of other critical infrastructures (for example, telecommunications, water supply, transportation, healthcare, food supply, and others) on the electric power grid increases the need to address vulnerability and related mitigation issues for the grid itself.

In a joint report issued in June 2010, the U.S. Department of Energy (DoE) and NERC outlined a number of HEMP vulnerabilities in power grid and power distribution systems [10]. The report, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System", details vulnerabilities, some of which are summarized below.

High voltage substation controls and communications

The coupling of sensors in the transformer to cables inside of control rooms is most vulnerable to HEMP pulses. While a 3.2-kV surge is sufficient to trigger relays, initial maximum HEMP levels of 10 kV could propagate to relays and other electronic controls. A surge as little as 0.6 kV could cause significant damage to PROMs and other microprocessors in computer and embedded system controls, crippling substation operations.

Generation Facilities

Testing at generation facilities has shown that voltages as low as 0.6 kV are sufficient to destroy programmable logic controllers used in the flow of fuel and other power generation processes. In addition, cabling within these facilities is subject to the same inadequate protection as those in substation control and communications.

Control Centers and SCADA

Supervisory Control and Data Acquisition (SCADA) systems in nearly all power grid operations rely heavily on digital control systems (DCS) and programmable logic controllers (PLC) networked together over the grid. SCADA systems resemble the physical architecture of common personal computers, with microprocessors, system bus controllers, and interfaces for communicating with external devices and with other SCADA components. These systems monitor and control the operation of most power systems. In the event of a critical loss of a power generation facility or failure of other major components, the SCADA systems automatically issue alerts and then issue commands to other facilities under their control to remedy the situation, including rerouting power from other systems. Testing reveals that levels as low as 0.6 kV cause significant damage to PC-type components, and a large-scale EMP could then disrupt entire centers and inter-center communications through these components. In addition, a cascading failure effect could occur as the current(s) passes from one networked SCADA device to another [11].

Distribution Lines

According to NERC, approximately 78% of all electric power delivery to end-users passes through 14-kV distribution lines. The variation of orientation of the single feeder lines increases the potential for exposure along some feeder segments that would allow maximum E1 HEMP voltage, creating a possible insulator flashover and system failure. This conclusion was reached by the *EMP Commission on the Threat and Critical National Infrastructure* analysis of induced

over-voltages ranging from 200 kV to 400 kV over geographically widespread areas, especially if flashovers occur within one mile of a substation with high fault current [11].

Distribution Transformers

Testing at Oak Ridge National Laboratories in the 1980s examined possible E1 pulse damage to step-down transformers. The 19 tests performed found that the systems experienced operational damage during fast-peak pulse simulations in 7.2-kV/25-kVA power distribution systems. The pulses caused pinhole damage and dielectric breakdown within the windings. This means that HEMP attacks could affect step-down transformers and could cause multiple system failures [10].

Smart Grid Semiconductor Devices

Due to the nature of E1 and E3 pulses, there is a high probability that computing devices, unshielded control devices, and smart grid components not specifically hardened for HEMP events could fail. An initial literature review revealed no knowledge of systematic smart grid component research or testing regarding HEMP effects.

Power Grid Support Transportation Systems

Another uncertainty is the extent of damage to transportation systems, such as repair vehicles and diesel/electric locomotives used to service and transport spare transformers or parts and repair crews to damaged plants affected by E1 and E3 HEMP. While adequate replacement components may be on hand through advance preparation planning, transportation is essential to quickly and reliably repair equipment and systems in the event of a catastrophic GMD, EMP, or HEMP event.

Modern cars and trucks in particular contain a significant number of microelectronic components and could experience damage that incapacitates the vehicles if not sufficiently shielded. Independent testing by vehicle manufacturers concerning EMP shielding and protection is not publicly available, although major manufacturers have conducted such tests [12]. The manufacturers will not allow White Sands to disclose the results of these tests, nor the model vehicles and/or trucks they have tested. In addition to these vehicles, testing of locomotives may be needed, as the delivery of recovery transformers and repair crews and equipment would rely heavily on this mode of transportation support.

Damage to Other Critical Infrastructure and End-Use Load

With a disabled power grid, a cascade of collateral damage such as non-functional healthcare facilities and hospitals, waste treatment, and food distribution systems could put the public at high risk.

In addition, electromagnetic attack could disrupt other critical infrastructure, including much of the customer load the grid serves. For example:

- Cellular communications failure could occur as the E1 and subsequent E3 pulses disrupt and destroy unprotected cell tower components and cell phone microprocessors.
- Computer systems could fail as bridges, routers, and CPUs absorb and overload from initial E1 and E2 pulses, much as they might do during severe, unprotected lightning strikes.
- Business and financial computing and power systems could collapse.

- Non-military grade (unhardened) video, radio, and Internet communication could incur major, debilitating damage.
- Unhardened or unprotected aircraft could become disabled in flight as electrical engine and instrumentation components fail.
- Petroleum and natural gas delivery systems could shut down.

The likelihood or capabilities of hostile entities to launch such an attack is subject to considerable debate, but various high-level military operations and studies have documented the effects of HEMP attacks as observed in the field and simulated and tested in laboratories and experimental operations. All confirm the potential for the above HEMP effects on unprotected systems.

Risk Assessment

A HEMP attack requires both a nuclear device and a ground-to-space vehicle capable of reaching orbital levels. Although nuclear missile strike capabilities are no longer limited to superpower nations, the high level of technology required for a HEMP attack reduces the risk of occurrence.

However, a ballistic missile is not required to achieve a near-surface (non-HEMP) nuclear blast that would cause significant damage. Moreover, as noted above, non-nuclear electromagnetic weapons exist that are capable of disrupting grid operations including potentially triggering cascading failures leading to widespread regional blackouts.

Understanding the risk posed by electromagnetic attack is an essential first step in developing countermeasures and strategies for prevention, mitigation, and recovery. A HEMP attack is a less likely but higher impact event than an IEMI attack. However, quantifying the risk is difficult.

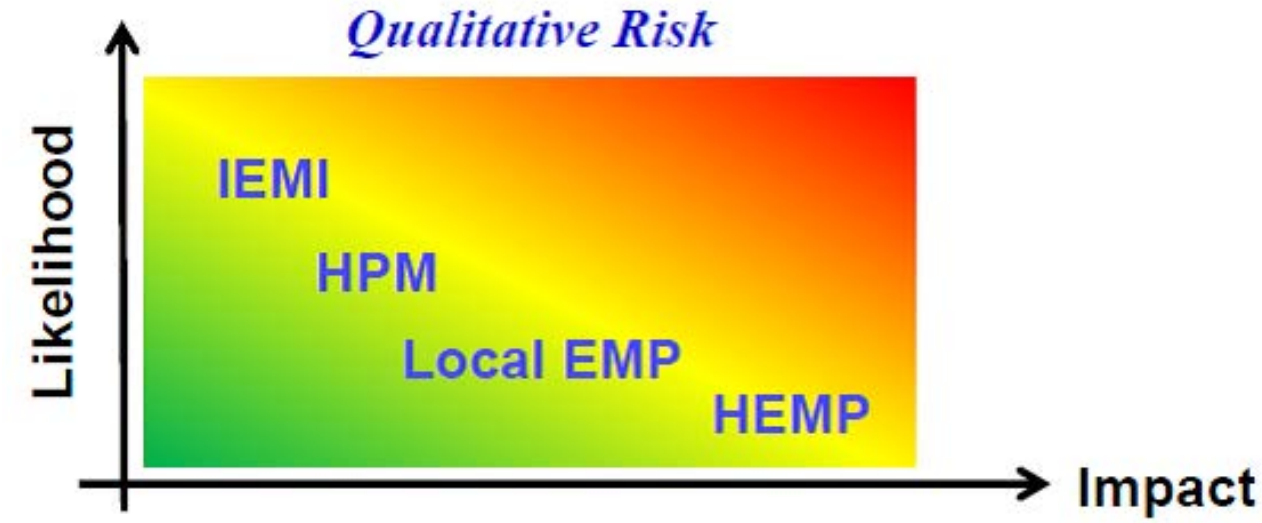

Figure 2-4
Likelihood and Potential Impact of Different Electromagnetic Attacks

Risk assessment and development of a prioritization framework are key steps in managing the risk of EMP as well as other high impact low frequency events.

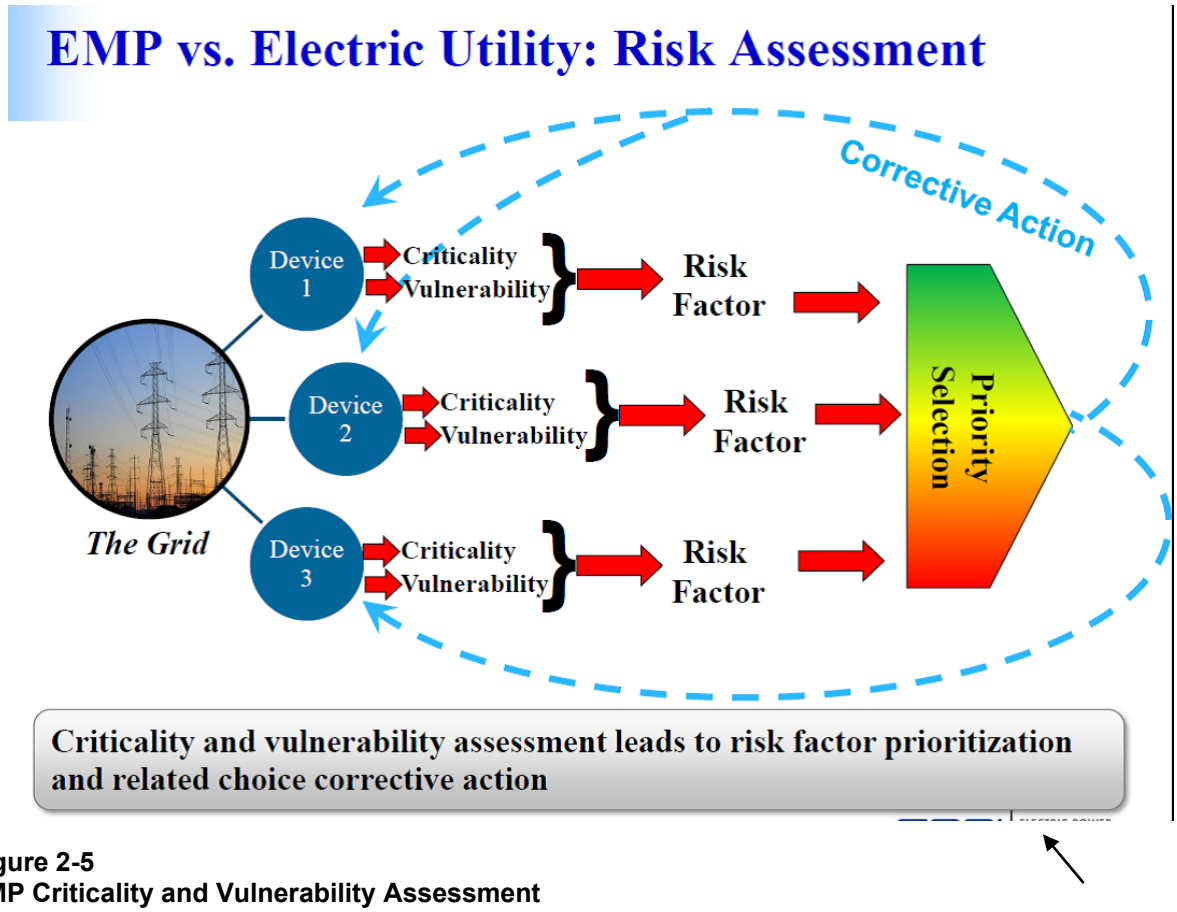

Figure 2-5
EMP Criticality and Vulnerability Assessment

A prioritization framework has five components:

1. **Characterize Threats**. Threat characterization ultimately drives countermeasures and mitigation. In addition, developing a common language and methodology for characterizing threats, helps identify commonalities across different threats to support development of a robust mitigation strategy. Key aggregators of threats include warning, firepower, knowledge of actors, duration, frequency or probability, and the breadth of the event.
2. **Determine Vulnerability**. Determining vulnerability is performed at the component level, i.e., assessing which types of equipment are vulnerable to electromagnetic attack.
3. **Understand Impact and Probability**. This component involves a risk-based system impact assessment that determines, for a given event scenario, the extent of component failure, then calculates the probable system impact measured terms of customers out of power and duration. The assessment is repeated for different event scenarios to yield probability weighted risk. This is crucial for business case development.
4. **Effect of Mitigation Measures**. Mitigation includes hardening and recovery, and also encompasses mitigation identification, development, evaluation, the relative cost of application and reduction in risk.
5. **Balance with Day-to-Day Priorities**. This component involves decision support to help organizations determine a cost effect response to the specific threat, as the impact in relation to other threats in relation to overall business.

Mitigation and Recovery

In the event of a HEMP attack, various countermeasures must be in place to reduce the number of affected systems, limit the scope of damage, and bring systems and infrastructure back online as soon as possible. EPRI and NATF will respond to share good practices and close research gaps. Countermeasures include, but are not limited to the following:

1. Early detection and solid response plans are essential to preparedness. While detection or prevention of an attack is beyond the purview of private stakeholders, coordination between the military and the power industry and other affected agencies and first responders is needed to limit initial damage and initiate procedures for a swift recovery of damaged systems.
2. Broader understanding within the private sector of the potential for HEMP threats can lead to greater hardening and defensive preparation of systems. In parallel to hardening of existing systems, stakeholders can stockpile adequate supplies of spare components and emergency operations procedures.
3. Post-HEMP plans should focus on swift repair, re-supply, and infrastructure recovery. Because HEMP attacks can cause wide spread damage, coordination is desired at an Interconnect level as well as at local levels. Planning Ahead

Some specific mitigation and recovery actions were emphasized at the Summit, and are listed below. Participants recommended the development of an EMP Working group and production of an EMP white paper describing industry actions and providing a no-regrets strategy for addressing EMP.

Emergency plans to be in place at the electric utility level should include:

- Early damage assessment tools and strategy
- First-response plans for different scenarios
- Links for coordination with utilities and government at national and local level

Prevention strategies should include:

- Cost analysis and procurement for HEMP-resilient components
- National plans for critical spare components
  - Derive from EPRI-DHS Recovery Transformers pilot project
  - Account for geographic distribution and transportation requirements
  - Coordinate with EEI STEP program, NERC Spare Equipment Database, etc.
- Integrated modeling and simulation tools
  - Simulated grid HEMP impact exercises

Simulated response / impact on critical components

EMP Hardening

In testimony before the U.S. Congress, military officials have assured the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack that the military and military facilities are largely prepared and hardened against HEMP disruptions and regularly test equipment and facilities for HEMP vulnerabilities. All critical U.S. military equipment must now conform to the MILSTD-188-125 standard for mitigating HEMP [9]. Some commercial systems

have also adopted these standards for hardening against GMD/EMP/HEMP attacks, including aerospace, automotive, financial institutions, and government agencies.

Apart from these efforts, however, widespread and coordinated R&D on civilian, electric power industry, and commercial protection and mitigation is lacking.

The following chapter summarizes EMP Summit participants' perspectives, practices, and concerns.

References

1. Metatech Corporation. *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid*. January 2010. Prepared for Oak Ridge National Laboratory. http://web.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Meta-R-320.pdf .
2. Vittitoe, Charles N. *Did High-Altitude EMP Cause the Hawaiian Streetlight Incident*? Sandia National Laboratories. June 1989. http://www.ece.unm.edu/summa/notes/SDAN/0031. pdf.
3. Department of Energy. *United States Nuclear Tests, July 1945 through September 1992*. December 1994. http://www.fas.org/nuke/guide/usa/nuclear/usnuctests.htm.
4. Oak Ridge National Laboratories. *Electric Utility Experience with Geomagnetic Disturbances*. September 1991. http://www.ornl.gov/~webworks/cpr/v823/rpt/51089.pdf.
5. Longmire, Conrad L. *Justification and Verification of High-Altitude EMP Theory, Part 1*. Lawrence Livermore National Laboratory. June 1986. (pp 14-16). http://www.ece.unm.edu/summa/notes/TheoreticalPDFs/TN368.pdf.
6. U.S. Army. *Nuclear Environment Survivability.* April 15, 1994. http://www.dtic.mil/dtic/tr/fulltext/u2/a278230.pdf.
7. Cho, Johee. *North Korea Nears Completion of Electromagnetic Pulse Bomb.* ABC News. March 9, 2011. http://abcnews.go.com/International/electronic-warfare-north-korea-nearscompletion-electromagnetic-pulse/story?id=13081667#.Tzkrg8Xy98E.
8. Schneider, Dr. Mark, United States Nuclear Strategy Forum. *The Emerging EMP Threat to the United States.* The National Institute Press. November 2007. http://www.nipp.org/National%20Institute%20Press/Current%20Publications/PDF/EMP%20Paper%20Final%20November07.pdf.
9. Department of Defense Interface Standard. *High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C41Facilities Performing Critical, Time-Urgent Missions, MIL STD 188-125-1.* July 17, 1998. http://www.wbdg.org/ccb/FEDMIL/std188_125_1.pdf.
10. North American Electric Reliability Corporation (NERC) and the U.S. Department of Energy. *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System.* June 2010. http://www.nerc.com/files/HILF.pdf.
11. EMP Commission. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures,* April 2008. http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.
12. White Sands Missile Testing Public Affairs. *Electromagnetic pulse testing.* Accessed February 15, 2011. http://www.wsmr.army.mil/PAO/wuaws/Pages/Electromagneticpulsetesting.aspx.

13. *Testimony of Gerry Cauley, President and Chief Executive Officer, North American Electric Reliability Corporation Before The Energy and Power Subcommittee of the House Energy and Commerce Committee Hearing on Discussion Draft Legislation to Improve Cybersecurity of the Electric Grid.* May 31, 2011. http://www.nerc.com/fileUploads/File/News/HECC%20May%2031%20Cauley%20Testimony%20Final.pdf.

3
INDUSTRY PERSPECTIVES AND PRACTICES

Introduction

EMP Summit participants shared concerns, perspectives, plans and practices regarding the EMP threat, mitigation, and system restoration. Participants offered comments and questions during and after presentations. Facilitated discussion sessions were held following the presentations.

This chapter summarizes industry presentations and participant comments made during and after presentations and during the facilitated discussions.

General Comments

The following comments reflect common industry perspectives and concerns regarding the EMP issue.

"Quantifying risk is difficult, but we cannot wait for perfect information about the threat and the risk. Where should we put our efforts? On IEMI, which is more likely, but has less impact per event, or HEMP, which is less likely but has more impact?"

"The priority is reliability, and dollars will naturally flow to reliability projects. How do we value resiliency? How do we measure it? How do we calculate the probability of EMP? How do we value the associated impact? There needs to be a path forward that supports decision making with imperfect data."

"The EMP issue is not simply about technology. There needs to be coordination among utilities, and with the Department of Defense and other government agencies."

"It is apparent that there is a lot going on, and sharing is valuable, but there remain gaps in the research that can be filled."

"What does the utility industry feel its responsibility is? The industry asserts that it is the government's role to protest against EMP. However, there is growing sentiment that the industry must work to harden against and recover from an EMP. The industry has a responsibility to explore and deploy countermeasures that provide an incremental level of protection that costs little. This is part of a growing demand to bolster system resilience."

"How will the system respond [to EMP]? Some believe that distribution systems cannot be protected and the system will go down. Therefore, the emphasis must be on protecting against catastrophic component damage and recovery."

"We need to address not only the grid components, but also the end-use components.

"A reasonable recovery target needs to be established. It will likely be sufficient to serve only half of the load."

Several participants observed that many of the IEMI mitigation strategies also support physical security. There is value in addressing all of the threats (GMD, Physical Security, Cyber Security EMP, IEMI) together as well as separately so that those strategies that support multiple threats can be valued appropriately.

Additional participant comments regarding good practices and utility needs are presented later in this chapter following the summaries of utility presentations.

Industry Presentations

Representatives from electric utilities and engineering laboratories delivered presentations on the following topics.

- Effects of EMP on Protection and Control Systems
- Utility Responses to EMP and Industry Needs
- Legislative Observations
- EMP Shielding Efforts
- EMP Concerns, Issues, Actions and Future Plans

Each presentation is summarized below, including comments from participants made during and following the presentation. The material is intended to provide the emphasis of the discussions without attribution to any specific individual or organization.

Presentation 1: Effects of EMP on Protection and Control Systems

Substation protection and control devices, communications equipment, and computers may be susceptible to HEMP and IEMI. The industry is already addressing how components perform during lightning strikes and surge events, but EMP presents higher levels and different frequencies, especially the E1 pulse.

P&C enclosures can be constructed to protect critical systems and components, per MIL-STD-188-125, which involves installing a Faraday cage around susceptible components, shielding, and minimizing or shielding points of entry including windows, vents, and doors.

Existing control house designs should be evaluated for EMP performance, with attention to concrete and layered steel construction. Also, since protective devices are installed in cabinets that provide some attenuation, testing should be conducted to assess the level of protection.

Of particular concern is electrical penetration. Thousands of cables enter the structure. The Mil-Std is not written to apply to components out in the yard. Changes may be required to meet the standard followed by testing to verify that the standard is met.

Reducing Copper

Copper cables running from the yard into the enclosure need to be protected. It may be desirable to replace some of this copper cabling with fiber optics. The IEC 61850 standard suite of protocols includes an Ethernet protocol for transmitting IED data, which can be done over fiber. One option is to digitize analog data outside and bring it into the enclosure via fiber optic cable.

Deploying copper rather than fiber also reduces the cost of copper and raceways, and also reduces points of penetration and vulnerability. Moreover it bolsters physical security.

Mil-Std-compliant control houses are expensive, by one estimate costing about $2 million dollars each, versus $200,000 for a conventional control house. However, existing house designs may be provide some protection, and with relatively inexpensive modifications could provide protection.

The conclusion: utilities should do all they can with multiple, relatively low-cost technologies and bring the whole system up, rather than do one $2 million installation.

Presentation 2: Utility Responses to EMP and Industry Needs

The presenter emphasized that the company serves many critical customers including government agencies, military installations, and telecommunications hubs. The company feels a great obligation and responsibility to prevent and mitigate threats to reliability.

Holistic, Layered Approach to Resiliency

The company is taking a holistic, layered approach to increasing resilience that encompasses substation, system, and cyber security. Regarding substation security the approach includes a layer of detection, a layer of mitigation, and a layer of recovery.

The company has invested in increased physical security including spare transformers. They are moving away from traditional bushings that could catastrophically fail. They have added additional recovery transformers and upgraded security at storage yards.

Because accurate data on HEMP burst magnitude and impact area is lacking, the company is focusing on E3 protection, which is similar to GMD. They have modeled transformers to better understand the effects of geomagnetically induced current (GIC) and changed major structural parts away from magnetic material to reduce hot spots. They are also testing transformers at the factory for GIC to validate the model.

The utility has two transformer suppliers with two designs, an arrangement that offers diversity in design and manufacturers in different countries with different currencies, providing redundancy and flexibility. The utility also aims for a high level of interchangeability, and has spares that can be moved among substations to provide redundancy in spares coverage at critical substations. Mobile transformers are valuable for all types of recovery, not just EMP and GMD.

E2 protection includes fundamentals: good lightning protection as well as adequate grounding.

E1 is the great unknown. They have tested EMP-enhanced control houses with improved attenuation. Testing showed the openings have leakage but propagation doesn't travel around corners very well, and window and door design can mitigate leakage. Improved fencing for increased physical security has also enhanced attenuation.

The utility has identified where they are vulnerable and is addressing those areas.

Concerns and Opportunities for Collaboration

The utility's efforts to increase resilience will defend against smaller blast, localized events, but a widespread event will be challenging. The industry needs to be working collectively on this.

Recent experience in earthquake recovery demonstrated that communication is a big problem as networks are overwhelmed by multiple service providers. How are we going to communicate with after an event?

Transportation is another major concern. Will vehicles work after an EMP?

There are several opportunities for industry collaboration:

- Defined Testing Protocols
- Recommendations on Installation Practices
- Emergency Communications (is a federal license needed for a special band for utilities to connect?)
- Impacts on Vehicle Transportation

The utility is testing vehicle impacts and will share results.

Increased coordination with government agencies and the military will be needed to obtain the necessary information in order to perform effective mitigation and restoration. This includes improving communication with state and local police to improve response plans for potential substation attack so they can work with utility operations.

System Operating Center

The utility plans to move its systems operating center to its own building, which will include EMP shielding, redundant power from two substations, redundant communications, cyber security, truck barriers, and remote parking.

This protected building reflects the utility's holistic approach to strengthening resilience that encompasses GMD, EMP, cyber attack, system restoration, and day-to-day operations.

Presentation 2: Utility Response to EMP and Industry Needs

The presenter emphasized a pragmatic approach to defending against electromagnetic attack.

The focus was on physical security and Intentional Electromagnetic Interference (IEMI) attack, which may involve:

- Electricity interference
- Gas interference
- Corporate IT systems
- Communications networks
- Electronic wiring

IEMI mechanisms are concealable, and they can enter your building and you won't even know it. Would you know what to look for?

The utility performed technical visual assessments of sites; reviewed policies and standards and performed gap analyses of electromagnetic compatibility specifications. They also performed active testing of equipment. Results will be shared.

"The industry as a whole will benefit from what we have done."

Primary recommendations were:

- New Data Center
- Control Room
- Urban and rural Substations
- Gas
- Gas Import

It was discovered during testing is that urban sites (e.g., substations, control room) are most at risk. You need to prevent uncontrolled, close vehicle access around the perimeter. Also, antennas can invite an attack, so move them around the back to a less visible and less vulnerable location. What makes good sense from a physical security standpoint is also helpful regarding IEMI.

Remember your primary asset might be the target. You might be trying to protect your asset, but it's at risk. You are only as good as your weakest link.

A key question is how to determine how much to spend to achieve a given level of protection? It is necessary to strike a balance between security and running a business smoothly.

Presentation 3: Legislative Observations

The presenter noted that the EMP threat has drawn the attention of the media, novelists, and activist groups, and legislators. As a result, utilities are under pressure to demonstrate their preparation for the threat, which in many cases has been sensationalized and distorted.

Utilities have to fight hyperbole. A key challenge is to communicate the message that utilities have long been taking action on many of the EMP Commission recommendations, including:

- Blackstart Plan
- Related Reliability Standard Requirements
  - Identify and Protect Critical Assets
  - Prioritize and Protect Communications
  - Backup Emergency Power at Critical Facilities
  - Prioritize and Protect Fuel Supply Facilities

"My message is simple: this is stuff we are already doing—and we need to get this message across to people."

The presenter stressed the importance of effective communication between technical staff and corporate communications staff so the latter can get the message across to politicians and the public, so the discussion can be based on facts rather than hyperbole.

Recommendations (not yet implemented):

- Develop and Deploy system test standard & equipment
- Emergency "Universal" replacement equipment
- Redundant backup diagnostics and communication

Presentation 4: EMP Shielding Efforts

The utility has taken the position that the E1 environment poses the most significant threat to electronic substation protection and control devices.

The first major vulnerability is the direct radiation/illumination of the protection equipment. Mitigation is increasing the shielding effectiveness of the control building to help reduce the impact to protection devices and other critical components. For the first vulnerability, the development of a modular control building standard will help. The purpose is to gradually replace protection and control assets as time and budgets permit.

The second major vulnerability, and most predominant, is the coupling of current onto outdoor control cable coming into the control building. Mitigation includes proper grounding techniques and the use of sufficient cable shields to reduce overall impact to protection devices.

Drop-In Control Module

In 2010, the utility started development of a modularized control building standard whose purpose is to gradually replace protection and control assets as both time and budgets permit. Each building module contains project-specific protection and control system components that have been installed and tested prior to delivery. This gives the utility the flexibility to pay and plan for assets that are only needed today, rather than risking the under or oversizing of a control building for future needs.

The control building consists of a Base Module and an Expansion Module. The Base Module houses all the static components found in all control buildings (battery, charger, RTU, Telecom Equipment). The Expansion Module houses all the variable components depending on size of the facility (relay and control panels).

In 2010, a joint committee with NERC and the DOE published a popular report, *High-Impact Low Frequency (HILF)*, which brought to light some possible vulnerabilities associated with EMP phenomena and P&C systems.

With the Drop-in Control Module being a three-dimensional metal structure, this provided much of the ground work for a fairly complete shielded facility. Starting in 2011 baseline EMP susceptibility tests have been performed on these building solutions to assess their shielding effectiveness (SE) performance.

<u>Neutral Environment Tests</u>

- Low-Level Characterization Tests (LLCT) performed on the Drop-in Control Module designs in 2011/2012 were done in a neutral environment
- No control cables were connected
- Few conduit penetrations were created
- Average attenuation ~40-50dB across wide frequency range

<u>Live Environment Tests</u>

Follow up tests in 2014 were performed on a Drop-in Control Module using both LLCT and Continuous Wave Immersion (CWI) methods on an in-service EHV 345/138kV substation

- All control cables were connected
- Several conduit penetrations had been created
- Average attenuation ~30-40dB across frequency spectrum

Legacy Building Assessment

The follow-up testing in 2014 also included the evaluation of a 30yr old metal control building

Differences included:

  - Poured concrete floor
  - Several dozen conduit penetrations from years of construction and maintenance
  - Metal walls not as robust
- All control cables were connected
- Average attenuation ~20-40dB across frequency spectrum

While the drop-in control module's complete metal structure makes for a better performing shield than a brick and mortar structure, it will not protect all equipment from exposure to high levels of electromagnetic radiation

Improvements to facilities would include the following:

- Removal of wall penetrations
- Elimination of cable risers on the outside of buildings
- Removal of antennae for communication systems
- Installation of conductive door gaskets
- Installation of EMI screens on ventilation and exhaust fans for stationary battery systems

Control Cable Protection (Mitigation of Vulnerability #2)

Control cable can pose a significant problem as transmission facilities require copper cable runs in excess of 1000' or more for EHV installations that can cover several acres.

USE SHIELDED CABLE. Common types of cable shields:

  - Aluminum/Copper Foil
  - Helically Wrapped Aluminum/Copper Tape
  - Braided Wire Shields
  - Longitudinally Wrapped Corrugated Copper

The appropriate grounding methodology must be used with the type of shield selected. Improper grounding of shields could result in shield failure

Following proper industry standard procedures as outlined in IEEE 525, *IEEE Guide for the Design and Installation of Cable Systems in Substations* can also reduce the impact on electronic equipment and provide guidance on grounding methodology and when to use shielded cable.

Metal Oxide Varistors (MOVs) and other surge protection devices (SPDs) can also be used to in conjunction with proper grounding methodologies to protect equipment. Burying cables in pre-cast trench systems and removing exterior cable risers will also provide additional protection.

At this time, the utility is evaluating data obtained from assessments to determine if levels found on control cable would significantly exceed transients inherent within a substation environment.

The utility's current practice is to use a shielded cable, grounded at both ends. The typical level of protection for this type of configuration can supply a reduction in common mode voltage by 400 times vs the use of unshielded cable *(Kotheimer, Control Circuit Transients)*. Given the utility's implementation of this methodology, they are trying to confirm this claim with the assessments done in a live substation environment.

Industry Best Practices

Each utility has its own way of protecting sensitive protection components. Arcs drawn from Air-Blast Breakers, switching transients from Trip/Close coils on breakers, capacitor bank switching all require the need for proper grounding and shielding within a substation.

What needs to be determined is whether or not the best practices used within the utility industry against environments inherent within transmission substations, are sufficient to mitigate catastrophic failures in a widespread EMP event. If not, what additional measures need to be taken and to what impact to the customer?

"We truly want to share the learning we've done, and once we get our final reports, we will share our recommendations. We will also share, confidentially, what we can with FERC, the DOD and the DOE."

Presentation 5: EMP Concerns and Response

This presentation focused on IEMI concerns and included a description of a high field IEMI detection system under development. The system would provide information on electromagnetic weather and feature user-definable alerts, remote data access, and can provide source directionality when multiple detectors are used to enable triangulation.

Alarms from the detector go to the control center by fiber.

Concerns associated with such a system include

- Proper Settings
  - Determination of ambient noise, including sources of commercial radio and TV broadcast stations to avoid nuisance alarms
- Pinpointing source of IEMI
  - Multiple detectors
  - Triangulation

- Follow-Up Actions
  - Notification of Law Enforcement or Corporate Security
  - Development of Procedures for reporting to agencies
- Detection vs. Hardening: MIL-STD-188-125-1. Will the devices be in a shielded environment or will they be affected by the phenomena they are detecting?

Presentation 6: EMP Mitigation Experience

This presentation addressed one utility's experience in attempting to understand and mitigate high frequency (E1) risks. The experience includes EMP mitigation in a new backup control center.

The utility relocated its transmission control center in 1990 to an access-controlled site that is hardened against severe weather and physical security threats. EMP mitigation was not a design consideration when the facility was being planned in the 1980s, but locating the facility to an access-controlled site provides some mitigation against portable devices.

An assessment did, however, identify some potential vulnerability. Retrofitting an existing facility is problematic. However, shortly after receiving the assessment, the utility had made a decision to build a new back-up control center facility. EMP mitigation can be, and is, a design feature of the new facility.

Design considerations for the new control center included the following:

- EMP mitigation affects design of HVAC system.
- Need to determine mission critical portions of the facility that need to be protected, which may include the following:
  - Computers
  - Control rooms
  - UPS and generators
- Communication vulnerability should be considered as part of a holistic all hazards approach
  - Fiber optic vs. microwave and POTS
  - Private versus public facilities
  - Probably do not need all communication systems to work in order to monitor and control

Risk Assessment

The utility engaged two different consultants and has received two materially different assessments of risk. The utility has also collaborated with transmission companies attempting to assess and mitigate E1 risks.

The utility believes E1 risk assessment and mitigation practices for substations are generally less developed, less transparent, and more likely to involve divergent proprietary approaches than GMD assessment and mitigation practices, even though GMD practices are not in a mature state.

Lack of transparency and consensus E1 approaches are somewhat understandable, given that E1 threats are a security matter.

Some possible E1 mitigation practices introduce new reliability risks and may or may not be necessary and effective.

Substation Mitigation

Substation mitigation issues include the following:

- E1 Frequency to mitigate
- Control house building can be hardened, but may not be effective due to electrical connections from apparatus in the yard
  - Differing views of the effectiveness of underground burial of cables in trenches, perhaps with metallic covers
  - Filtering adds complexity, perhaps increased relay misoperations
- Control house versus electrical apparatus in the yard (circuit breakers, transformers, etc.)
  - If control house is mitigated but yard equipment is not, may have situation of a protected control house with nothing to control
  - PT and CT inputs could be transformed to fiber optic signal in the yard, but does that just move the problem from the control house to the yard?

The utility is presently adding another layer of EMP protection for control center functions. Substation EMP assessment and mitigation efforts are a work in progress

Presentation 7: EMP Concerns, Issues and Future Plans

The EMP issue is driven by fear. Fear about technology that is not understood. Fear of impacts not anticipated and fear of inadequate preparation. The media are taking advantage of the opportunity to sensationalize the issue to add to viewership.

Nobody really knows what to do if we have an EMP and that is translating over to our government—they don't know what they don't know. Leadership will focus on asking whether we are prepared. As we've seen in recent storms, even the best preparation isn't good enough.

The threat is real. Nuclear attack capability with EMP impact is real. Portable EMP devices are real, and nation state weapons are real. An EMP attack is a highly unlikely event, but like a nuclear meltdown the consequences are severe.

The utility's EMP challenges are

- Process
- Politics
- Priority

The utility's process regarding EMP is as follows

- Harden
  - Identification of key blackstart pathways
  - Coordination of battery backup and hardened diesel/gas generation support
  - Research hardening technologies
- Survive
  - Design tweaks to improve general protection
- Recover
  - Analog solutions and backups
  - Training and drills on recovery
  - Adequate and protected inventory
  - Communications and transportation backup capability

Politics may be a bigger challenge. EMP is not just a utility threat, but a national threat. Politicians who are involved in this are passionate about protecting the people of the United States. We can expect the government to impose some sort of requirements on the utility industry at some point.

Priority: How much is enough? Utilities are good at prioritizing reliability, but it may be at the expense of resilience. How do we prioritize an EMP expense? It's hard to put resiliency into standard reliability protocols.

The utility's EMP priorities are

- Reliability
- Resiliency
- Recovery

The utility recognizes it faces multiple threats in addition to EMP, including GMD, cyber attack, physical attack, severe weather and aging infrastructure. The strategy is to take actions that will deliver the most benefits for the most people at the least cost.

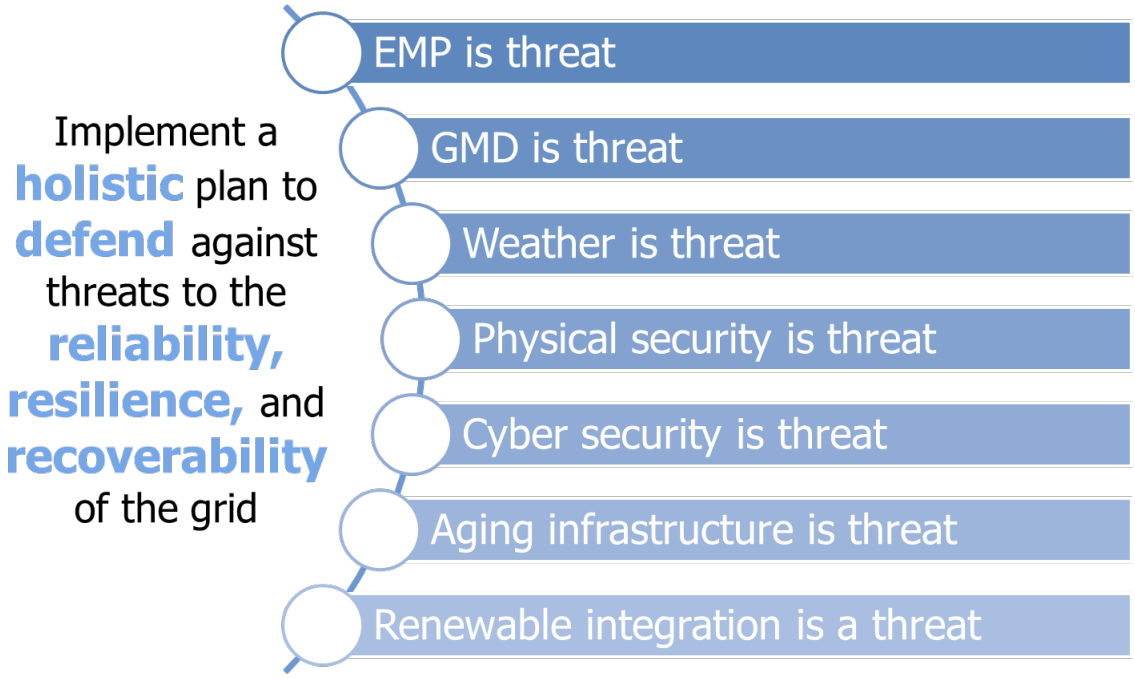

Figure 3-1
Holistic Approach to Support Grid Reliability, Resilience and Recovery

Participant Comments

Summit participants offered many excellent comments regarding good practices and industry needs. Some of these are summarized below. Many participant comments are distilled in the following chapter to reveal research gaps and next steps.

Good Practices

Participant comments regarding good practices are presented in three categories.

1. Robustness / hardening (prior to an event)
2. Resourcefulness / survivability (during an event)
3. Recovery (after an event)

Robustness and Hardening:

- Physical barriers, access control, equipment design and hardening. Review and update access control policy.
- A new data center can be hardened for an additional cost of $500K. Retrofitting is more expensive. There are organizations available that can assess vulnerability provide component and system shielding. One participant quoted $10 million for completely shielding a control house.
  - Hot site earthing and bonding transformers and generators close to building
  - Well designed physical security
  - Perimeter control to keep the public away from the site.

- Monitoring for detection and deterrence: IT and security. Materials bonding control procedure to provide modest shielding attenuation. Note that extra bonding may start additional ground loops. Use a single company for bonding and an organized approach.
- Wireless communications when possible to eliminate EMP path to sensitive equipment

Resourcefulness / Survivability

- Employ IEMI detectors. Can we or should we develop and implement an IEMI detector that would run in the background? If there is an anomaly, we can go back and determine if there was an attack.
- Communicate and coordinate with local law enforcement and other agencies

Recovery

- Spares strategy: A participant revised their spares strategy for resiliency. At electrically critical substations, they store three single-phase spares, rather than one transformer for medium criticality substations.
- Harden the black start path (identify, backup, harden)
- Recovery plan – analog solutions, backups, training and drills, spares (protected).
- Communication and transportation backup capability

Utility Industry Needs

Improved Understanding of Component Vulnerability. Which components will suffer permanent damage? Which will fail temporarily but recover? Which will ride through undeterred?

Information Sharing and Coordination. Can we find out what are other industries and organizations are doing (military, airline industry, telecommunications, etc.)?

Clarity on Responsibility. What are the utility industry's responsibilities regarding preparation, mitigation, restoration and recovery?

Guidance for Hardening and Recovery. Is there a logical guide for hardening and recovery from EMP?

Collaboration. R&D and information exchange between the utility industry and the federal government would be valuable.

Understanding the Impacts on Communications and Transportation. Every major event impacting reliability in past ten years has demonstrated the criticality of communications. Will vehicles operate after an EMP or IEMI attack? Communications and transportation will be critical to restoration and recovery. For emergency communications, do we need federal licensing for special bands? We also need to assess the vulnerability of satellites and the effect of a potential loss of satellite communications.

Improved Understanding of Failure Mechanisms

Change design and procurement specifications to increase EMP performance. This is a low cost, prudent response.

Better understanding of the reference testing waveform.

Spares strategy. How does a utility determine what, and how many spares, e.g., transformers, are required? Are spares sitting on a shelf impacted as well by IEMI? Some results show that the out of service equipment is less susceptible, but still susceptible.

Recommendations on control cable installation practices.

Mutual Aid / Sharing of Resources, e.g., relay technicians and staffing. This is a much more complicated issue than sharing lineman for physical damage. Disruption to communications and transportation will complicate recovery efforts. EEI has a national recovery effort. Sharing of resources may fit there.

4
RESEARCH GAPS AND NEXT STEPS

Introduction

The EMP Summit revealed a number of knowledge gaps, opportunities for collaborative research and information sharing.

This chapter summarizes research and information sharing opportunities, and defines the highest priority gaps and next steps.

Ideas for Collaborative Research

Develop the design basis for the E1 event. This would help in the assessment of vulnerability and the value of mitigation approaches.

Criticality analysis. How is the criticality assessment for EMP attack different than traditional planning (n-1, n-2) assessment? Would we get a different list? Probabilistic planning may support the criticality classification. Doing these studies is more complicated than many think. We need to do static and dynamic studies.

Develop multiple classes of design basis based on substation criticality level.

Assess vulnerability of different generation sources. What sources will be available for black start generation?

Update test data on shielding and protection of copper systems. Existing data is decades old. Fiber optics may be a long transition strategy.

Develop a spares strategy for critical substation equipment.

Examine non-electric utility factors that may impact the length and breadth of the outage, including transportation and communication.

Capture the differences in mitigation approaches—for example, between retrofitting an existing component or site and designing hardening into a new design of the component or site.

Test and compare vendor equipment for breakdown threshold to help utilities target their application.

Explore situational awareness for EMP, e.g., attack detection. Can the industry coordinate with military early warning systems (e.g., NORAD) to provide advance warning to system operators?

Information Sharing Opportunities

Technical information on the nature of the threats. Some of this information resides in the military and government. Need to gain access to it and develop an information repository. There is some older ORNL research and reports from the 60s and 70s that may still be relevant. There are available repositories of EMP test results and studies for review.

Develop a response plan with police and other entities.

Consider an electric utility-wide alert system that would inform other companies when one is attacked.

Collect and distribute good practices that strengthen resiliency and help alleviate multiple threats.

Develop a coordination plan with the telecommunications industry, which already has systems hardened to Mil Spec. Utilities will need access to telecommunications post-attack. Perhaps arrangements can be made to ensure the electricity industry has appropriate priority.

There is value in promoting that the industry is seriously looking at the issue. Much is being done, although there may be a perception that the industry is doing little. If the industry can inform regulators of all that we are doing it can create space for the industry to intelligently and sensibly address the issue and avoid adverse regulatory action.

Highest Priority Gaps and Requested Next Steps

Gaps

A guide for identifying and hardening the black start path.

Common messaging for interested stakeholders.

A well thought out design basis for EMP

Decision support related to hardening, surviving, and recovering. Considering these together gets most value for the dollar.

An analysis to determine the cost to fully protect every device.

Recovery planning that considers a range of scenarios—e.g., with a system collapse but generation available next door for black start. Or with all generation off line.

A coordinated spares strategy.

Suggested Next Steps

Develop a white paper on what the utility industry is doing in regard to EMP and IEMI.

Provide training and outreach to members of NATF and EPRI.

Engage standards committees (IEEE, IEC, etc.) to help define goals and targets.

Develop a good practices guide for construction of a new control house or retrofitting an existing house.

Develop a training scenario that includes EMP and IEMI.

Develop an appropriate test protocol and plan. Identify components and configurations that have been tested and those that need to be tested. Identify lab capability.

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity

3002004027

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com