



High-Impact, Low-Frequency Event Risk to the North American Bulk Power System



*A Jointly-Commissioned Summary Report of the
North American Electric Reliability Corporation
and the U.S. Department of Energy's November
2009 Workshop*



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

June 2010

www.nerc.com | www.doe.gov



About the High-Impact, Low-Frequency (HILF) Event Risk Effort

The North American Electric Reliability Corporation (NERC) and the U.S. Department of Energy (DOE) partnered in July of 2009 on an effort to address High-Impact, Low-Frequency risks to the North American bulk power system. In August, NERC formed a steering committee made up of industry and risk experts to lead the development of an initial workshop on the subject, chaired by Scott Moore, VP Transmission System & Region Operations for American Electric Power, and Robert Stephan, Former Assistant Secretary for Infrastructure Protection in the National Protection and Programs Directorate of the U.S. Department of Homeland Security (DHS). The workshop was held in Washington, D.C. on November 9–10, 2009.

The approximately 110 attendees at the closed session included representatives from the United States' Congressional Staff, Department of Defense (DOD), DHS, DOE, Department of Health and Human Services (HHS), EMP Commission, and Federal Energy Regulatory Commission (FERC). Representatives from each of the North American electric industry's major sectors, including investor owned utilities, cooperatives, and municipal utilities were also in attendance.

The workshop was divided into three tracks: Cyber or Physical Coordinated Attack, Pandemic, and Geomagnetic Disturbance / Electro-magnetic Pulse risk. Each track was given a set of questions to answer as part of a moderated, interactive dialog designed to identify next steps on each of these risks. Topics discussed during the working sessions included: approaches to measure and monitor HILF risks, potential mitigation steps, and formulating an effective public/private partnership to more effectively address these issues. Focus was given to determining the appropriate balance of prevention, resilience, and restoration.

Coming out of the session, NERC, DOE, and the Steering Committee agreed a summary report of the workshop should be developed in coordination with NERC stakeholders and that follow-on actions should be pursued. The Steering Committee agreed to oversee and support the development of the report.

The NERC Planning, Operating, and Critical Infrastructure Protection Committees (collectively referred to as the technical committees) generally support the HILF report and, on May 3, 2010, recommend that it be sent to the NERC BOT for their review and consideration. NERC's Board of Trustees approved the report on May 17, 2010.

Introduction

June 2, 2010

Dear Reader,

North America's electricity infrastructure is clearly one of our society's most important assets. As reliance on digital technology has increased, many North Americans have come to depend on the reliable delivery of electricity to their homes and businesses to power nearly every aspect of their lives.

The electric sector has a long history of successfully managing day-to-day reliability risk to the system. As a result, the North American electricity grid is one of the most reliable in the world. Today, however, we are focused on a class of rare risks with the potential to cause long-term, catastrophic damage to the bulk power system: High-Impact, Low-Frequency (HILF) events.

Examples of these events include a pandemic illness, coordinated cyber, physical, or blended attack on the system, extreme solar weather, and the high-altitude detonation of a nuclear weapon. While some of these events have never occurred and the probability of future occurrence and impact is difficult to measure, government and industry are working to evaluate and, where necessary, enhance current planning and operating practices to address these risks in a systematic and comprehensive fashion. Caution in mitigating HILF risks is warranted to ensure any unintended reliability consequences are avoided.

Today, collective action is needed to reconcile real and valid concerns about cost, labor, and the sector's shrinking workforce with the legitimate questions of national security posed by coordinated physical and cyber attacks and High-Altitude Electromagnetic Pulse weapons. Today, targeted action is required to define clear roles for the public and private sectors in ensuring appropriate protections are in place to deal with the effects of a pandemic disease or geomagnetic disturbance. Today, the government and industry must recommit themselves to supporting one another to enhance the protection, resiliency, and response capabilities for the North American bulk power system in the face of these rare events.

This report is part of that ongoing effort. As a result, many of the proposals for action in this report are not new. Experts familiar with HILF risks will notice echoes of statements made in many reports published over the past twenty years.¹ This report is designed to synthesize some of the best collaborative thinking on these risks to date, as brought together in the November 2009 HILF workshop, and provide input into next steps.

This comes at a time, however, when budgets are constrained and resources are limited. Both the public and private sectors must balance competing priorities like smart grid implementation, addressing climate change, and the growing need to expeditiously site and build new infrastructure. At the same time, it is crucial that electricity remains affordable for the average consumer. HILF risks are just one part of a much larger landscape of risks and concerns facing the sector.

¹ Refer to Appendix 4 for a non-exhaustive list of material published on these risks.

Introduction

The answers will not be found by simply filing this report away with its predecessors: there is much work ahead to meet these goals. This report is a beginning, not an end. We will need the support of all of our readers to realize the vision of this effort: effective public/private partnership to address HILF risks in a coordinated, systematic fashion.

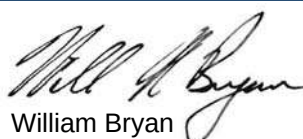
Thank you for getting involved.

High-Impact Low-Frequency Event Steering Committee

Executive Sponsors



Michael Assante
VP and Chief Security Officer
North American Electric Reliability Corp.

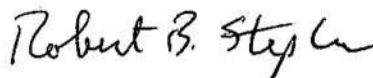


William Bryan
Deputy Assistant Secretary
U.S. Department of Energy

Chairs



Scott Moore
Vice President of Transmission
American Electric Power



Robert Stephan
Former Assistant Secretary for Infrastructure Protection in the National Protection and Programs Directorate
U.S. Department of Homeland Security

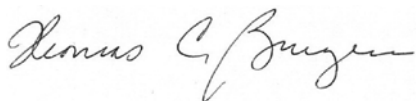
Members



Stuart Brindley
Former Manager - Training & Emergency Preparedness
IESO



Tom Bowe
Executive Director, Reliability Integration
PJM Interconnection



Tom Burgess
Director, FERC Policy & Compliance
FirstEnergy

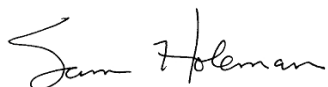


Jerry Dixon
Director of Analysis
Team Cymru Research

Introduction



Michael Frankel
Executive Director
U.S. EMP Commission



Sam Holeman
System Operating Center
Duke Energy Corporation



John Kappenman
Principal
Storm Analysis Consultants



Robert McClanahan
Vice President, Information Technology
Arkansas Electric Cooperative



Julie Palin
Partner
Business Recovery Solutions LLC



William Radasky
President and Managing Engineer
Metatech Corp.

Table of Contents

About the High-Impact, Low-Frequency (HILF) Event Risk Effort.....	2
Introduction.....	3
Table of Contents	6
Executive Summary	8
Summary of Proposals for Action	13
Coordinated Attack Risk.....	13
Pandemic Risk	16
GMD/EMP Risk.....	18
Common Framework Approach to HILF Risk.....	21
Coordinated Attack Risk.....	26
Risk Identification.....	26
Threat	26
Vulnerability	29
Consequence	34
Characteristics and Unique Attributes	34
Mitigations	35
Planning	36
Operations.....	41
Efforts Already Underway	44
Pandemic Risk.....	47
Risk Identification.....	47
Threat	47
Vulnerability	50
Consequence	53
Characteristics and Unique Attributes	53
Mitigations	54
Planning	55
Operations.....	59
Efforts Already Underway	60
GMD/EMP Risk.....	61
Risk Identification.....	61
Geomagnetic Disturbances	61
Threat	61
Vulnerability	68
Consequence	74
High Altitude Electromagnetic Pulse (HEMP).....	77
Threat	77
Vulnerability	82
Consequence	89
Intentional Electromagnetic Interference (IEMI)	89
Threat	89
Vulnerability	93

Table of Contents

Consequence	95
Mitigations	96
Planning	98
Operations	100
Efforts Already Underway	102
Appendix 1: HEMP Impacts on Distribution Infrastructure	103
Insulator Flashover and Failure	103
Distribution Transformers	106
Appendix 2: High Frequency Protection Concepts for E1 HEMP and IEMI.....	107
Appendix 3: Framework for Determining Pandemic Response Actions Based on Severity	109
Appendix 4: Additional References on GMD Events	113
HILF Steering Committee and Task Force Rosters	115
High-Impact Low-Frequency Event Workshop Steering Committee	115
High-Impact Low-Frequency Event: Coordinated Attack Ad Hoc Task Force	116
High-Impact Low-Frequency Event: Pandemic Ad Hoc Task Force	117
High-Impact Low-Frequency Event: GMD/EMP Ad Hoc Task Force	118

Executive Summary

The bulk power system is one of North America's most critical infrastructures, underpinning the continent's governments, economy and society. As reliance on electricity-dependent technology has increased, the reliability of the power grid has become more important each day. The electric sector has recognized the importance of the infrastructure it operates and has had a long history of successfully managing day-to-day operational and probabilistic risk to the reliability of the system to ensure the "lights stay on" for consumers.

A class of risks, called High-Impact, Low-Frequency (HILF) events, has recently become a renewed focus of risk managers and policy makers. These risks have the potential to cause catastrophic impacts on the electric power system, but either rarely occur, or, in some cases, have never occurred. Examples of HILF risks include coordinated cyber, physical, and blended attacks, the high-altitude detonation of a nuclear weapon, and major natural disasters like earthquakes, tsunamis, large hurricanes, pandemics, and geomagnetic disturbances caused by solar weather. HILF events truly transcend other risks to the sector due to their magnitude of impact and the relatively limited operational experience in addressing them. Deliberate attacks (including acts of war, terrorism, and coordinated criminal activity) pose especially unique scenarios due to their inherent unpredictability and significant national security implications. As concerns over these risks have increased, the electric sector is working to take a leadership position among other Critical Infrastructure and Key Resource (CIKR) sectors in addressing these risks.

The High-Impact, Low-Frequency (HILF) Event Risk Effort

To facilitate the development of a sector-wide roadmap for further public/private collaboration on these issues, the North American Electric Reliability Corporation (NERC) and U.S. Department of Energy (DOE) jointly sponsored a workshop on HILF risks in November, 2009. The approximately 110 attendees at the closed session included representatives from the U.S.'s Congressional Staff, Department of Defense (DOD), Department of Homeland Security (DHS), DOE, Department of Health and Human Services (HHS), EMP Commission, and Federal Energy Regulatory Commission (FERC). Representatives from each of the North American electric industry's major sectors, including investor owned utilities, cooperatives, and municipal utilities were also in attendance, as were many risk experts.

This report is intended to summarize the proceedings and discussions at the two-day session. Proposals for action and mitigating options discussed herein reflect the thoughts of the session participants, and, while they may represent a largely consensus-based view, they are not intended to be conclusive or exhaustive. Most of the proposals in this document identify areas where further work is needed and provide initial guidance on the kinds of efforts that must be undertaken.

As these proposals for action are considered, it is important to place HILF risks in context of the larger landscape of risk and concerns facing the electric sector over the coming years. NERC's 2009 Long-Term Reliability Assessment², for example, identified nine emerging issues expected to impact reliability by 2018 including climate legislation, smart grid, cyber security, transmission siting, variable generation issues, workforce issues, and reactive power. Several of these are reflective of other legislative and regulatory priorities. In addition, the sector is expected to require significant infrastructure additions³ to meet demand as economic recovery continues over the coming years.

Addressing HILF Risk

The interconnected and interdependent nature of the bulk power system requires that risk management actions be consistently and systematically applied across the entire system to be effective. The magnitude of such an effort should not be underestimated. The North American bulk power system is comprised of more than 200,000 miles of high-voltage transmission lines, thousands of generation plants, and millions of digital controls.⁴ More than 1,800 entities own and operate portions of the system, with thousands more involved in the operation of distribution networks across North America. These entities range in size from large investor-owned utilities with over 20,000 employees to small cooperatives with only ten. The systems and facilities comprising the larger system have differing configurations, design schemes, and operational concerns. Referring to any mitigation on such a system as “easily-deployed,” “inexpensive,” or “simple” is an inaccurate characterization of the work required to implement these changes.

As mitigating options are further considered, it is also important to note that it is impossible to fully protect the system from every threat or threat actor. Sound management of these and all risks to the sector must take a holistic approach, with specific focus on determining the appropriate balance of resilience, restoration, and protection. A successful risk management approach will begin by identifying the threat environment and protection goals for the system, balancing expected outcomes against the costs associated with proposed mitigations.

This balance must be carefully considered with input from both electric sector and government authorities. Building on the inherent resilience of the system and enhancing the response of the system as a whole to unconventional stresses should be a cornerstone of these efforts. Determining appropriate cost ceilings and recovery mechanisms for protections related to HILF risks will be critical to ensuring a viable approach to addressing them. The electricity industry and government authorities must also coordinate to improve two-way information sharing and communication practices relative to HILF risks. The sector is heavily reliant on information from the public sector for each risk discussed in this document.

² 2009 Long-Term Reliability Assessment, 2009-2018. NERC. Princeton, NJ. 2009.
http://www.nerc.com/files/2009_LTRA.pdf

³ “Transforming America’s Power Industry: The Investment Challenge 2010-2030,” Edison Foundation report prepared by the Brattle Group, November 2008. <http://www.edisonfoundation.net/reports.htm#transforming>

⁴ Data extracted from NERC’s 2009 Long-Term Reliability Assessment data.

Common elements of addressing HILF risk must also include a focus on raising awareness across the sector and creating opportunities to discuss specific issues in technical detail. In many cases, this will take the form of creating various task forces designed to bring together personnel from the risk community, electric sector, government, and equipment manufacturers. These task forces will provide a comprehensive view of technical implications and potential solutions to the challenges posed by these risks.

Additional research and development will also be needed in certain areas to ensure mitigating technology solutions are available to industry. This is particularly important with reference to cyber security and electro-magnetic pulse threats. Ensuring protections can be built-in to future products as opposed to being delivered as a “bolt-on” retrofit will greatly improve the cost-effectiveness of protections on a going-forward basis. Hardening of existing assets will also be important, as many assets have long life cycles.

HILF Risk Discussed in this Report

While HILF risks can include other extreme events like major natural disasters, meteor strikes, and deliberate attacks or acts of war, the November workshop focused on three specific threats as identified by the HILF Steering Committee in the planning process: Coordinated Cyber/Physical Attack, Pandemic Illness, and Geomagnetic and Electromagnetic Events. Each section identifies the threat to the system, the system’s vulnerabilities, and the consequences that could occur were these vulnerabilities to be exploited. This discussion is followed by a consideration of various mitigating options and *Proposals for Action*.

Highlights: Coordinated Attack Risk

The risk of a coordinated cyber, physical, or blended attack against the North American bulk power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to be reduced. The specific concern with respect to these threats is the targeting of multiple key nodes on the system that, if damaged, destroyed, or interrupted in a coordinated fashion, could bring the system outside the protection provided by traditional planning and operating criteria. Such an attack would behave very differently than traditional risks to the system in that an intelligent attacker could mount an adaptive attack that would manipulate assets and potentially provide misleading information to system operators attempting to address the issue. While no such attack has occurred on the bulk power system to date, the electric sector has taken important steps toward mitigating these issues with the development of NERC’s Critical Infrastructure Protection standards⁵, the standing Critical Infrastructure Protection Committee⁶, and a myriad of other efforts. More comprehensive work is needed, however, to realize the vision of a secure grid. Better technology solutions for the cyber portion of the threat should be developed, with specific focus on forensic

⁵ “Critical Infrastructure Protection (CIP)” section of NERC’s “Reliability Standards for the Bulk Electric Systems in North America” http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf

⁶ NERC’s Critical Infrastructure Protection Committee website at: <http://www.nerc.com/page.php?cid=1|9|117|139>

tools and network architectures to support graceful system degradation that would allow operators to “fly with fewer controls.” Component and system design criteria should also be reevaluated with respect to these threats and an eye toward designing for survivability. Prioritization of key assets for protection will be a critical component of a successful mitigation approach.

Highlights: Pandemic Risk

Pandemic risk differs from many of the other threats facing the system in that it is a “people event.” The principal vulnerability with respect to a pandemic is the loss of staff critical to operating the electric power system. Without these personnel, operational issues on the system would increase as less-trained or less-experienced individuals work to operate generation plants, address mechanical failures, restore power following outages caused by weather and other natural events, and operate the system. The sector recently experienced a mild pandemic through the 2009 A/H1N1 outbreak. This pandemic’s effects on society were very limited and are not representative of the scenarios of concern to the electric sector. While many entities within the sector have developed advanced pandemic plans, the sector is ultimately reliant on government health authorities for quality and timely information on the spread and severity of a pandemic. Clear triggers from these authorities are needed for the sector to make appropriate response decisions in the event of a severe outbreak.

Highlights: Geomagnetic Disturbances, High Altitude Electromagnetic Pulse Events, and Intentional Electromagnetic Interference Threats

Geomagnetic disturbances, the earthly effects of solar weather, are not a new threat to the electric sector. Recent analysis by Metatech and Storm Analysis Consultants^{51, 52, 53, 54} suggests, however, that the potential extremes of the geomagnetic threat environment may be much greater than previously anticipated. Geomagnetically-induced currents on system infrastructure have the potential to result in widespread tripping of key transmission lines and irreversible physical damage to large transformers.^{51, 52, 53, 54} The 1989 event that caused a blackout of the Hydro Québec system provided important lessons to the sector. Since that time, the sector has adopted operational procedures to reduce the vulnerability to geomagnetic storms and has installed certain protections in areas most prone to impact as recommended by Oak Ridge National Labs in their report on the March 1989 event.⁷ More work is needed, however, to consider the potential impacts larger storms may have and develop viable, cost-effective mitigations, potentially at lower geographic latitudes than previously thought necessary.

The high-altitude detonation of a large nuclear device or other electromagnetic weapon could have devastating effects on the electric sector, interrupting system operation and potentially damaging many devices simultaneously. A coordinated attack involving intentional electromagnetic interference (IEMI) could result in more localized and targeted impacts that may also cause significant impacts to the sector.

⁷ ORNL-6665: Electric Utility Industry Experience with Geomagnetic Disturbances”; 1991

The physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale, as could be effected by any of these threats, could result in prolonged outages as procurement cycles for these components range from months to years. Many of these components are manufactured overseas, with little manufacturing capability remaining in North America. The impacts of these events on the power system are not yet fully understood across the sector and warrant further collaborative work to identify the prioritized “top ten” mitigation steps that are both cost-effective and sufficient to protect the power system from the widespread catastrophic damage that could result from any of these events.

Next Steps

The *Proposals for Action* outlined in this report are intended to provide input into a formal action plan to address these issues. They do not, in and of themselves, constitute this plan. The effort needed to address these risks will require intense coordination and a significant resource commitment from all entities involved. The time needed to address these issues and complete the work contemplated herein will be measured in years. NERC and the U.S. DOE will work together with the electric sector, manufacturers, and other government authorities to support the development and execution of a clear and concise action plan to ensure accountability and coordinated action on these issues going forward.

Summary of Proposals for Action

While the November 2009 workshop provided an effective forum to share information and promote a better understanding of these very complex issues, an important objective was to explore next steps that could be taken to build on existing efforts to address these risks. During the breakout sessions, workshop participants brainstormed the ways and means to mitigate these threats and vulnerabilities. *Proposals for Action* throughout this report provide a summary of these discussions. Some proposals suggest ways that the likelihood of an event could be better understood and communicated across the public and private sectors, while others focus on how to prevent, mitigate, or respond to an event regardless of its likelihood. They are intended to describe a consensus view of the ideas discussed during the workshop.

These *Proposals for Action* were designed to provide input into an action plan that would be developed subsequent to the initial steps in the HILF effort. They do not, in and of themselves, constitute that plan, for important reasons. The proposals are only loosely prioritized and do not take cost or time constraints into account in a systematic fashion. The list of proposals is also not intended to be exhaustive. They also do not provide the level of clarity needed to ensure accountability for the many agencies, organizations, and committees who will be integral to successful coordinated action on these issues in the future. Finally, the proposals do not, in their present form, commit NERC, the electric sector, the U.S. Department of Energy (DOE) or any government authorities to take specific actions or expend resources. An action plan would ideally address each of these deficiencies.

The proposals do provide important insights into the issues and lay a strong foundation for next steps. It is anticipated that any steps to achieve the objectives outlined in the proposals would add significant value. The proposals listed below are loosely prioritized in order of importance, but all carry similar weight and consequence.

NERC, its committees, and the U.S. DOE have already begun considering and developing a multi-year action plan designed to synthesize common themes in the proposals below and achieve the greatest gains possible with respect to these risks given the many competing priorities facing the sector at the present time, as discussed elsewhere in this document.

Coordinated Attack Risk

Proposal for Action | Coordinated Attack 1

The U.S. DOE and Department of Homeland Security (DHS) and appropriate government authorities in Canada should work together to establish clearer and more direct lines of communication and coordination with the electric sector. Focus should be given to improving the timely dissemination of information concerning impending threats and specific vulnerabilities, and on the provision of information with sufficient engineering depth for private-sector entities to evaluate and deploy suggested mitigations. Increasing the number of security

Summary of Proposals for Action

clearances available to industry may facilitate this objective in the short term, but specific focus is needed to appropriately de-classify information needed by the private sector.

Proposal for Action | Coordinated Attack 2

NERC's Board of Trustees should direct its technical committees to formalize initial efforts to evaluate the efficacy of current bulk power system planning and operating practices with respect to protecting the system from coordinated attack threats. The goal of these efforts should be to strengthen the general security posture of the North American electric sector. Similar efforts should be contemplated for smaller generation and distribution systems. The committees should:

- Recommend practices to enhance the efficacy of current planning and scenario criteria in addressing coordinated attack threats;
- Develop an accepted process to identify key facilities for protection and prioritized restoration, to include clear criteria for identifying critical loads;
- Seek and use stakeholder, government, and cross-sector input to develop clear protection goals, using the protection policy currently under development⁸ as a foundation;
- Conduct, coordinate, or sponsor an assessment of the North American bulk power system to identify areas where upgrades, modifications to operating procedures, or additional protective or adaptive measures may be needed and recommend actions as appropriate;
- Pursue cross-sector coordination to identify interdependencies and work with other sector coordinating councils to continuously improve security measures for all critical infrastructures; and
- Identify areas where additional and extraordinary costs may have to be incurred and evaluate whether cost-recovery mechanisms and regulatory support may be warranted.

As the committees proceed with their work, coordination with government authorities such as the U.S. DOE, the Federal Energy Regulatory Commission (FERC), and state regulatory authorities and appropriate government authorities in Canada must be brought into the discussion to ensure a widespread acceptance of the cost implications associated with proposed measures.

Proposal for Action | Coordinated Attack 3

NERC, the U.S. DOE, and appropriate government authorities in Canada should work with electric sector to improve the current spare equipment efforts for scarce or long-procurement-cycle assets such that spare equipment can be identified for response in a reasonable response window. Gaps in the inventory of available spare equipment should be identified and addressed, while considering the costs associated with retaining such inventory. Consider re-launching NERC's Spare Equipment Database (SED).

⁸ NERC Bulk Power System Critical Infrastructure Protection Policy Statement. Available at: <http://www.nerc.com/filez/essg.html>

Proposal for Action | Coordinated Attack 4

NERC should form a task force to support and promote the development of scenario-based analysis tools, to include robust system modeling scenarios of potential structured attacks, to assess system response capability. These models should be used to build on existing restoration plans and procedures to specifically address coordinated attack risk. In addition, scenario-based analysis supported by precise modeling will provide a better visibility of inventory requirements for spare equipment and associated cost recovery aspects. The committees should also support and promote the development and coordinated, regular exercise of restoration and recovery plans down to the field level to ensure all personnel are prepared to respond in the case of an attack. Consideration should be given to the potential for operating the system for extended periods without critical elements. These plans and drills should be coordinated with appropriate public-sector entities, such as local law enforcement, the U.S. DHS, and Department of Defense (DOD), and appropriate government authorities in Canada. Appropriate engagement with critical loads should also be pursued.

Proposal for Action | Coordinated Attack 5

NERC's Board of Trustees should direct its committees to support and promote the development of system operator training scenarios for physical and cyber attack. The group should consider recommendations to NERC's System Operator Certification and Continuing Education Program⁹ for potential training requirements.

Proposal for Action | Coordinated Attack 6

Working with its stakeholders either through a new task force or through existing structures, NERC should coordinate with the U.S. DOE, DHS, and FERC, and appropriate governmental authorities in Canada to develop a common lexicon for communicating about cyber and physical attack risk to ensure clear and concise communication is possible during an event. NERC and the electric sector should promote and support the integration of this lexicon into control centers across North America, giving consideration to whether modification is needed to NERC Reliability Standards¹⁰ to ensure the uniform adoption of this lexicon across the sector.

Proposal for Action | Coordinated Attack 7

NERC, the U.S. DOE, and appropriate government authorities in Canada should work with technology and software suppliers and the international community to encourage the development of forensic and adaptive network security tools for control systems. The authorities should specifically support research and development of protection and mitigation tools for cyber attack against the bulk power system. These tools should include enhanced forensic and cyber network monitoring capabilities, tools and protocols to allow for the graceful degradation of the system, and improved security for bulk power system components.¹¹ Consideration should be

⁹ NERC's "System Operator Certification" website: <http://www.nerc.com/page.php?cid=6%7C84>

¹⁰ NERC's "Reliability Standards" website: <http://www.nerc.com/page.php?cid=2%7C20>

¹¹ See page 28 for further explanation.

Summary of Proposals for Action

given to creating a testing or certification center and standards for products and software, taking potential cost implications into consideration. Consideration should be given to developing cost-effective mechanisms to better secure existing assets as well.

Proposal for Action | Coordinated Attack 8

Work begun in 2007 by the National Science Foundation and the Institute of Electrical and Electronics Engineers (IEEE) on workforce development for the electric sector should continue and be expanded to include the development of academic programs designed to train students on the planning, design, and operation of the bulk power system, as well as cyber and network security. The IEEE Education Society has produced two “Ready Now” modules on Cyber Security.^{12 13} Both the public and private sectors should support work with academic institutions to further develop these courses of study.

Proposal for Action | Coordinated Attack 9

The U.S. DOE, coordinating with government authorities in Canada as appropriate, should continue efforts to evaluate appropriate means to bring more of the supply chain and manufacturing base for high-impact system components, such as extra high-voltage transformers and system controls, back to North America to ensure these components are available and built in an uncompromised environment should a widespread attack or disaster occur.

Pandemic Risk

Proposal for Action | Pandemic 1

Sector entities should review their pandemic and business continuity plans to incorporate lessons learned from the 2009 A/H1N1 outbreak and consider much worse scenarios. Gaps in plans should be identified and rectified. Focus should be given to addressing “complacency” issues that may have arisen as a result of the relatively mild nature of the 2009 A/H1N1 pandemic. Entities should collaborate and share information, and consider materials developed by the Pandemic Influenza Working Group to promote excellence in pandemic planning across the sector.

¹² IEEE Expert Now Course Catalog, “Cyber Security of Industrial Control Systems (ICS)”, www.ieee.org/web/education/Expert_Now_IEEE/Catalog/power.html

¹³ IEEE Expert Now Course Catalog, “Cyber Security of Substation Control and Diagnostic Systems” http://www.ieee.org/web/education/Expert_Now_IEEE/modules.html#power

Proposal for Action | Pandemic 2

The U.S. Department of Health and Human Services and appropriate government authorities in Canada should improve the timeliness, granularity and quality of metrics used to measure and report on the emergence and spread of pandemic vectors and related illness. These measures should incorporate or be tailored to meet the needs of the electric sector and other critical infrastructure sectors. A new scale should be developed to provide authoritative information on the relative severity of the illness and outbreak. A draft scale was proposed to the U.S. DHS and Centers for Disease Control (CDC) by the NERC Pandemic Influenza Working Group in 2009 and has been included as Appendix 3 in this report. Focus should be given to better consolidating and reporting on leading indicators at a national, regional, and local level. Reports should be issued by government authorities weekly, at a minimum, and provide both leading and lagging indicators using current (no more than 7-day old) data in a concise and understandable format.

NERC should work with these entities to evaluate options for a communications mechanism to ensure this information is consistently available to all bulk power system entities. The U.S. DOE, as the sector-specific agency, should work with these entities to ensure appropriate feedback is provided and the work product meets sector needs.

Proposal for Action | Pandemic 3

NERC and the U.S. DOE should work with the U.S. Department of Health and Human Services and appropriate government authorities in Canada to ensure critical electric sector employees are given priority with respect to the distribution of vaccines and anti-viral medication and the ability to travel in the event of government-imposed travel restrictions. Consideration should also be given to employees of critical vendors and suppliers of the sector, to include natural gas pipeline operators, railway personnel, and urgent maintenance personnel.

Proposal for Action | Pandemic 4

NERC, the U.S. DOE, and appropriate government authorities in Canada should identify the kinds of information needed from the sector to effectively monitor critical workforce levels across the electric sector during a pandemic. A collaborative group of government and electric sector representatives should develop plans and procedures to efficiently meet information needs while limiting the data collection requirements where possible. This group should also develop mechanisms to share this information across the sector.

Proposal for Action | Pandemic 5

NERC, working with its stakeholders, should develop a proposal for relaxing regulatory requirements during a pandemic. NERC should collaborate with FERC, state regulators (possibly through the National Association of Regulatory Utility Commissioners (NARUC)), and appropriate government authorities in Canada to evaluate existing regulations and consider where appropriate recognition of circumstances may be warranted, without impacting overall

system reliability during a pandemic. An example of such requirements may be certain state-level regulations whereby utilities are subject to financial penalty if local distribution outages are not resolved within a given time window. Non-time-sensitive reporting requirements in NERC standards for bulk power system and generation operators may also be considered. Once developed, the process for relaxing regulatory requirements could potentially be applied to lengthened recovery from other HILF events, such as a major coordinated attack, electromagnetic pulse event, or geomagnetic disturbance.

GMD/EMP Risk

Proposal for Action | GMD/EMP 1

NERC, working with its stakeholders, the U.S. DOE, and appropriate government authorities in Canada should create a task force of industry, equipment manufacturers, and risk experts to evaluate and prioritize mitigation and restoration options for Geomagnetic Disturbances (GMD), High-altitude Electromagnetic Pulse (HEMP) events, and Intentional Electromagnetic Interference (IEMI) threats, while recognizing the similarities and differences of these three severe electromagnetic threats. Focus should be given to identifying the prioritized “top ten” mitigation steps that are cost-effective and sufficient to protect the power system from widespread catastrophic damage due to each of these threats. The task force should consider the options and concepts discussed in this workshop report, including:

- Acting jointly with the U.S. DOE, National Oceanic and Atmospheric Administration (NOAA), and other appropriate U.S. agencies and authorities in Canada, develop the design of an event monitoring network that can better capture the occurrence of a GMD event with sufficient detail (geographically-dispersed monitoring sites) to correlate an event to power system and equipment issues that arise, and that measures and captures the time-rate-of-change of magnetic flux that is critical to the electric sector. Develop a data sharing and funding plan that includes appropriate cost sharing by the North American governments and affected industries.
- Define the protection environment for each of the electromagnetic threats, considering the work recently completed by the U.S. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (U.S. EMP Commission)¹⁴, the National Academy of Sciences¹⁵, FERC and the Federal Emergency Management Agency (FEMA).
- Focus mitigation strategies on “high-impact” electric power facilities, wherein the loss of functionality will adversely and perhaps severely impact the delivery of power to the largest number of people for the longest period of time. Specifically consider remedial design corrections to reduce the vulnerability of the existing bulk power system. Focus

¹⁴ *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.* Commission to Assess the Threat to the United States from an EMP Attack. Washington, DC. April 2008. http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

¹⁵ *Severe Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report.* National Academies Press. Washington, DC. 2008. http://www.nap.edu/catalog.php?record_id=12507

should be given to the highest voltage portions of the transmission system and considering the growing vulnerability as this system is expanded.

- Consider the tradeoffs of economic efficiency and reliability of the power system with regard to these electromagnetic threats using risk-based analysis. Cost estimates of potential mitigations provided by the EMP Commission should be revisited to appropriately account for labor, engineering, installation, and associated operating costs.
- Identify the primary interdependencies with the other critical infrastructures that will impact restoration and reconstitution, with focus on telecommunications and fuel supply and delivery. Encourage cross-sector coordination to ensure the response of these assets to a GMD or HEMP attack is understood and that appropriate protections are put in place.
- Evaluate the role of spare equipment and sharing programs, such as NERC's Spare Equipment Database.
- Evaluate the effectiveness of existing blackstart procedures, and the need for exercises for a case where the blackout area is extremely large and other infrastructures have been damaged. Develop new procedures if required.
- Consider the need to develop a full "defense plan" that considers prevention, blackstart analysis, restoration, etc. to establish a model checklist/procedure for sector entities to deal with each of the threats.

Proposal for Action | GMD/EMP 2

Governmental authorities in the U.S. and Canada should continue to support industry efforts to address these risks. An executive order from government leaders, such as the President of the United States, would give additional weight to the importance of these issues relative to other priorities in both the public and private sectors.

Proposal for Action | GMD/EMP 3

Appropriate government authorities (to potentially include the U.S. DOE, FERC, DHS, NOAA, and National Aeronautics and Space Administration (NASA), and appropriate government authorities in Canada) should work with research organizations and the private sector to consider a roadmap for long-term research, development, and deployment on mitigating options for these threats. These efforts should be coordinated with NERC and the electric sector.

Proposal for Action | GMD/EMP 4

NERC, the U.S. FERC, DOE, DHS, NOAA, and NASA, and appropriate government authorities in Canada, together with subject matter experts, should work together to recommend the development of advanced methods to ensure system operators are given region-specific, timely, and accurate information regarding the expected duration, intensity, and geographic footprint of impending geomagnetic disturbances. Focus should be given to both extreme events and long-duration, low-intensity storms.

Proposal for Action | GMD/EMP 5

The U.S. DOE, DHS and appropriate government authorities in Canada, together with subject matter experts, should work together to establish an alert procedure to inform the electric sector that threat levels of an HEMP or IEMI attack have increased or that an attack is imminent. The communications method developed to distribute information concerning an impending geomagnetic storm or other critical infrastructure protection information could be used to disseminate these notices.

Common Framework Approach to HILF Risk

The North American bulk power system is the backbone for modern society. It only takes a few moments of reflection on how reliant society-at-large has become on electricity-dependent technology to recognize the potential impacts a prolonged loss of power could have on North America. In addition to the immediate loss of lighting and electric appliances in the affected area, the supply of food, water, and fuel would degrade within days. The facile communication of information to the general population would be greatly complicated by the loss of cell phones, internet access, and television. The economy would virtually shut down as electronic transactions could no longer be processed. After several days, widespread social unrest and confusion would ensue.

While highly dependent on other infrastructures for its efficient operation, the electric sector has been described as the “first among equals” of North America’s Critical Infrastructure and Key Resource (CIKR) sectors¹⁶, which include finance, transportation, oil and natural gas, and telecommunications. In recognition of its importance to society, the sector has taken a leadership position on risk management and has a long history of successfully managing operational risk to reliably “keep the lights on” and maintain reasonable rates for consumers. NERC Reliability Standards are just one element of the sector’s overall approach to reliability and are designed to ensure a consistent approach to reliability risk across the interconnected bulk power system.

HILF risks present unique threats to the electric sector; threats that fall outside of a traditional risk assessment framework. These risks have a number of characteristics in common:

- HILF risks have the potential to cause widespread or catastrophic impact to the sector—whether through impact to the workforce in the case of a pandemic, or through widespread physical damage to key system components in the case of a high-altitude electromagnetic pulse event.
- HILF risks generally originate through external forces outside the control of the sector. For example, actions can be taken to avoid vegetation contact with a transmission line. No amount of preemptive action on the part of sector will reduce the likelihood of a geomagnetic storm or pandemic, however.
- HILF events can occur very quickly and reach maximum impact with little warning or prior indication of an imminent risk. Effective response and restoration from HILF events require fast initiation and mobilization exercised through thorough prior planning.
- Little real-world operational experience generally exists with respect to responding to HILF risks, for the simple reason that they do not regularly occur.
- Probability of HILF risks’ occurrence and impact is difficult to quantify. Historical occurrence and severity do not provide a strong indicator of potential future impacts.

¹⁶ U.S. Department of Homeland Security’s “National Infrastructure Protection Plan” website:
http://www.dhs.gov/files/programs/editorial_0827.shtm#1

Understanding and effectively managing HILF risk therefore require a different approach to viewing risk. Given the sector's importance to society-at-large, considering appropriate risk management mechanisms, which could require substantial financial investment, necessarily involves input from both the private sector and government authorities. Where the private sector may be willing to assume a certain risk posture given sound cost-benefit analysis, government authorities may wish to consider a more conservative stance.

Many HILF risks fall into two primary categories: natural disasters and deliberate attacks or acts of war. These two types of HILF risk differ markedly and require different approaches and considerations to appropriately address them. Each risk presents unique, though sometimes overlapping, concerns and a different profile of existing preparedness across the electric sector. It may be useful to consider categorizing these risks into these two categories as further work on other HILF risks proceeds.

It is impossible to fully protect the system from every threat. Sound management of these and all risks to the sector must take a holistic approach, with specific focus on determining the appropriate balance of resilience, restoration, and protection.

Understanding HILF Risk

Successfully managing risk is one of the most challenging aspects of running a business. Broadly defined as the possibility of damage, injury, or loss, risk is driven by events that, whether predictable or not, have an uncertain outcome. Risk can be driven by events that occur every day, or events that may never occur.

Risk takes several forms in a business environment. Perhaps the most well-researched and understood is financial risk to the firm, particularly with respect to credit and investment risk in the financial sector. These risks are typically managed through a number of mechanisms, including diversification, hedging, transferring, and purchasing insurances.

Safety and operational risk are other well-understood risks, particularly in the electric sector. It is nearly impossible, for example, to walk into an electric sector facility without being reminded of an intense cultural focus on personnel safety. Senior managers have responsibility for ensuring employees follow preventative safety measures. Probabilistic operational risk is also well understood and managed. Operational events regularly occur on the system without any noticeable impact to consumers, as highly-skilled system operators quickly respond to restore the integrity of the system.

As mentioned earlier, HILF risks present unique challenges to risk managers. They fall into a category of "macro-prudential" risk, which behaves differently than most forms of business risk. Macro-prudential risk is non-transferrable and cannot be fully insured against, diversified, or hedged at the individual firm level. The strength of the individual firm also does not dilute the risk to the firm from these events. This form of risk must be considered on a sector-wide basis, particularly in sectors (like the electric sector) formed of entities that are highly interconnected and interdependent.

As HILF risks occur very infrequently, the success or failure of a response is more dependent on thorough planning and preparation than on operational experience. The ability to effectively respond to a changing threat environment—especially in the case of an adaptive attack—will be measured by the efficacy of the system operator’s initial response. The operator will rely on the sophistication of the tools under his immediate control and his training in those circumstances, neither of which can be provided in the minutes preceding an event. These tools and the training needed to ensure an appropriate response must be developed and deployed well in advance of the event.

Like other risks, HILF risks generally have three components: threat, vulnerability, and consequence. The threat is the external act itself; vulnerability, the portions or characteristics of the system that could be affected by the act; and consequence, the outcome of exploiting such vulnerability. Consideration must be given to each of these areas to ensure a full understanding of the risk is obtained.

Placing HILF Risk in Context

As mentioned earlier in this document, HILF risks are only part of a much larger list of priorities facing the electric sector over the coming decade. NERC’s 2009 Long-Term Reliability Assessment¹⁷ identified nine emerging issues expected to impact reliability by 2018 including climate legislation, smart grid, cyber security, transmission siting, variable generation issues, workforce issues, and reactive power. Several of these are reflective of other legislative and regulatory priorities.

Addressing HILF risk will require re-allocation of already strained human and financial resources available to the sector. A key objective in effectively managing HILF risk must therefore be to place these risks in an appropriate context and evaluate the priority given to these issues. A parallel goal must be to keep electricity affordable for the average consumer. The sector cannot expect to “gold plate” the system.

Any effort to mitigate a given vulnerability must be evenly applied across the entire system. The magnitude of such an effort should not be underestimated. The North American bulk power system is comprised of over 200,000 miles of high-voltage transmission lines, thousands of generation plants, and millions of digital controls. More than 1,800 entities own and operate portions of the system, with thousands more involved in the operation of distribution networks across North America. These entities range in size from large investor owned utilities with over 20,000 employees to small cooperatives with only ten. The systems and facilities comprising the larger bulk power system have differing configurations, design schemes, business models, and operational concerns. Referring to any mitigation on such a system as easily-deployed, inexpensive, or simple is a misnomer.

¹⁷ 2009 Long-Term Reliability Assessment, 2009-2018. NERC. Princeton, NJ. 2009. http://www.nerc.com/files/2009_LTRA.pdf

Assessing HILF Risk

The impact of HILF risks may be measured by several factors, including, but not limited to, population affected (number of people with no power), geographic area affected (region with no electricity in terms of square miles), time taken to restore power, potential for repeat incidents, intangibles (loss of perception of secure image), and various cost quantifiers (cost of repairing damage; cost of re-fortifying systems to ensure no repeat incidents; cost to consumers; cost to industry due to lost productivity, products, or services; cost to government and taxpayers; cost of increased insurance).

The threat environment itself must be well-defined so that protection goals can be established. How severe could a threat become? If historical events (e.g. the 1989 geomagnetic disturbance or 2009 A/H1N1 pandemic) do not sufficiently demonstrate the extremes of a HILF event, those extremes must be identified so that plans can be developed to appropriately respond to them.

Research on the potential infrastructure impacts of HILF risks on modern equipment installed on the North American bulk power system will be crucial to understanding the system's vulnerability to each risk. Several areas of HILF risk have not been recently or conclusively studied. Development of technologies to mitigate these risks should also be pursued so that a better understanding of the costs involved in their deployment can be evaluated opposite an assessment of their efficacy in addressing the issue at hand.

Measuring and monitoring HILF risk is another important element of the risk assessment process. Ensuring that the processes and metrics exist to provide visibility into the changing nature of these risks will be critical to risk management efforts. Identifying and monitoring leading indicators, where they exist, will allow the industry to enact plans to operate the system in a more conservative state and take other preventative measures as warranted.

Managing HILF Risk

Once a risk has been identified and assessed, effort turns to its management and mitigation. Risk management builds on the risk assessment process by seeking answers to three questions: What can be done and what options are available? What are the associated tradeoffs in terms of all costs, benefits, and risks? And what are the impacts of current management decisions on future options?

As mentioned earlier, managing HILF risk must take a holistic approach considering protection, resilience, and restoration mechanisms. Clear protection goals for the system must be established so appropriate thresholds for each of these three elements can be identified and planned to. Additionally, mitigation steps taken to address HILF risk should have no unintended reliability consequences that could increase risk from other, more common, threats.

The 2009 workshop asked participants to identify and evaluate existing viable mitigation options, considering financial implications, resource requirements, and the length of time that would be required to implement these changes. Participants were also asked to consider the

limitations of those strategies. The participants' responses to these prompts are included throughout the document.

A clear element of risk management for these threats is the construction of an effective public/private partnership between the electric sector and government authorities. Sector response to a geomagnetic disturbance, for example, is reliant on information obtained from government-owned satellites. Pandemics are also largely managed by government health authorities. Many of the proposals for action in this document center on improving information-sharing practices and enhancing joint decision-making processes.

Coordinated Attack Risk

One of the principal types of HILF events facing the bulk power system is a concerted, well-planned cyber, physical, or blended attack conducted by an active adversary against multiple points on the system. Such an attack, although never experienced in North America, could damage or destroy key system components, significantly degrade system operating conditions, and, in extreme cases, result in prolonged outages to large parts of the system. The rapid convergence of the electric power systems infrastructure with information and communications technologies, combined with a new awareness of the sophistication of adversary capabilities, require a fresh understanding of the risk and well-coordinated steps to improve the protection, resilience, and response capabilities of the bulk power system.

Risk Identification: Defining the risk in terms of the reliability impacts to the grid

Threat

Criminal threats to the bulk power system can range from those of minimal impact to those of high consequence. On the low-impact end of the spectrum are common events, such as copper theft and the types of routine cyber attack common to all business networks in the Information Age. In the intermediate-impact range are events that may involve damage to a single system component in an unsophisticated, unstructured attack. On the high-impact end of the scale are highly-coordinated, well-planned attacks against multiple assets designed to disable the system. The redundant design of the bulk power system provides a high degree of inherent resilience and protection against many threats in the low and intermediate range.

A highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes. Unlike “traditional,” probabilistic threats (i.e. severe weather, human error, and equipment failure), a coordinated attack would involve an intelligent adversary with the capability to quickly bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods.

Though no such attack has been successfully executed to date, the bulk power system remains an attractive target for acts of both physical and cyber terrorism. Goals of these adversaries are wide-ranging and could involve extortion, societal damage, and, in the case of state-sponsored attacks, acts of war.

.....

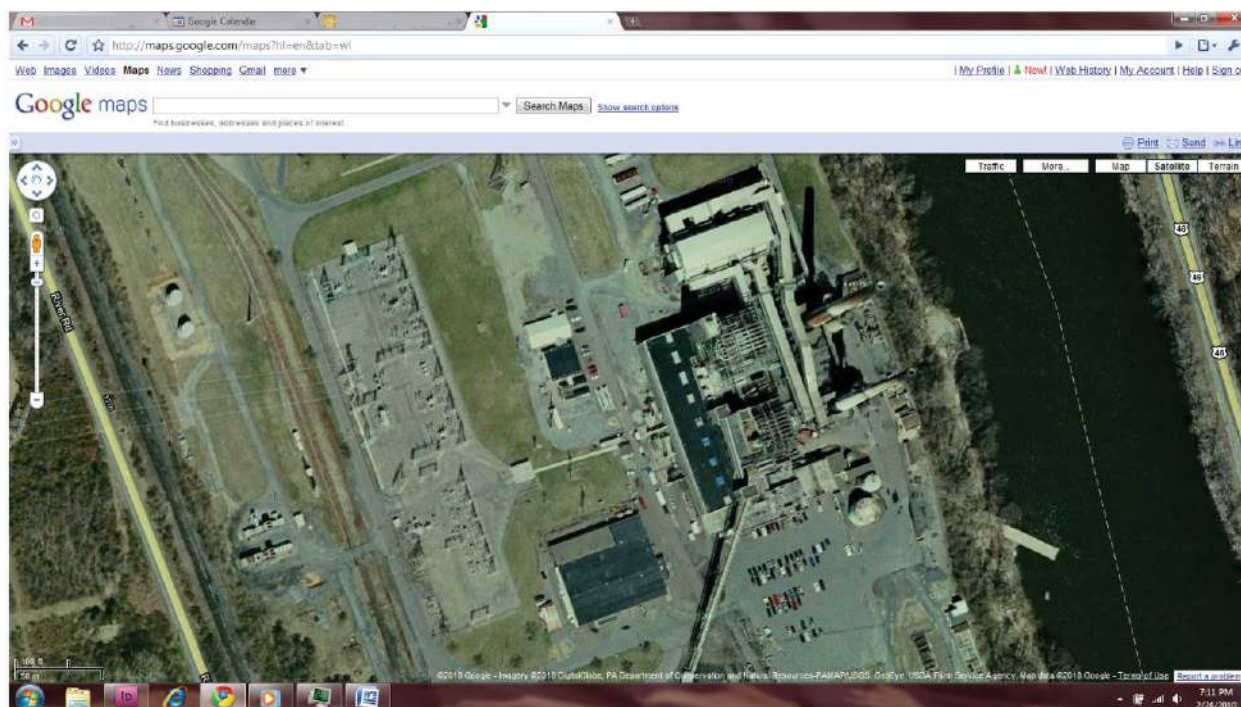


Figure 1: Screen Shot of Google Maps Satellite Imagery - February 24, 2010
Image copyright Google, Inc. 2010

The adversarial strategic advantage enjoyed by those targeting the bulk power system has been increased by the fact that sensitive information about critical bulk power system components and tools to carry out attacks are available and easily accessible in the public domain. For instance, a simple internet search may yield precise geo-tagged power plant locations complete with satellite imagery that can be used to assess security and defensive measures in support of attack planning (see Figure 1). While measures have been taken in the U.S. to protect some of this information as Critical Energy Infrastructure Information (CEII), much of the information is important to transparent market operation and is necessarily public.

Threat Actors

In the post-September 11, 2001 world, al-Qaeda and its affiliates and allies remain dangerous, adaptive, and motivated enemies and threats to North America's infrastructure. These and other foreign and domestic terrorist groups continue to pursue plans to attack the U.S. directly, likely focusing on prominent government, economic, and infrastructure targets.¹⁸

Plots and attacks overseas provide insight into these adversaries' capabilities and intent. In 2003, Lashkar-e Tayyiba affiliated violent extremists plotted to attack the Australian electric grid, including the Lucas Heights Research Center nuclear reactor, using improvised explosive devices (IED) and stand-off weapons. The suspects were charged with possession of detailed maps of the Australian electricity grid, U.S. military manuals on bomb-making, and the intent to

¹⁸ Director of National Intelligence Annual Threat Assessment (February, 2009).

purchase large amounts of explosives.¹⁹ The terrorists implicated in both the 2004 UK “Ministry of Sound” plot and the 2006 UK transnational aviation plot also discussed and planned on attacking energy targets, including the national electricity grid.

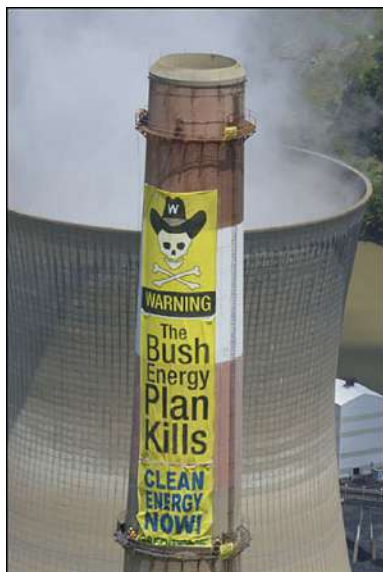


Figure 2: Greenpeace Activists Successfully Breach Security at U.S. Plant

Threats from environmental organizations have also been seen and thwarted by law enforcement officials in the UK over the past several years. Planned attacks on the Ratcliffe-on-Soar plant involved 114 arrests in 2009. 50 arrests were made during protests at E.ON’s Kingsnorth power plant, with protesters being pulled out of rafts by police while attempting to breach plant perimeter security. Successful breaches have occurred in the U.S., notably including the work of several Greenpeace activists who, unnoticed by security, scaled a 700 ft. smokestack at the Hatfield’s Ferry power plant and hung a 2500 sq. ft. banner from the top of the tower in 2004 (see Figure 2). Such protests have not resulted in severe damage to date, but the potential clearly exists to plot and execute a sophisticated attack against a system component.

Domestic extremists also pose a threat to the bulk power system. Though most security-related incidents in the U.S. are criminal in nature (e.g. copper theft), some extremists have targeted power plants, transmission lines, and substations using disruption operations, IEDs, stand-off weapons, and sabotage. Though these small-scale and unsophisticated attacks have occurred with little effect against grid targets within North America, separatists and rebels routinely conduct successful and damaging attacks against power systems throughout the rest of the world, especially in Europe and Latin America (e.g., FARC insurgent attacks on transmission towers in Columbia²⁰).

Complicit insider actors can provide an important attack vector to anyone attempting to attack the bulk power system. Insiders are malicious employees who work within the electric sector and have intimate knowledge of the functions, processes, systems, equipment, and personnel comprising the bulk power system. Using this knowledge, these actors could potentially identify critical systems and nodes and sabotage vital systems and components. Complicit insiders may feed critical information to outside attackers, greatly increasing their attack effectiveness, or may participate in mounting coordinated internal-external attacks. Insiders may also act of their own accord for motives ranging from dissatisfaction with their working environment to domestic terrorism.

¹⁹ *Plot to cripple energy network.* Sydney Morning Herald. June, 2004.
<http://www.smh.com.au/articles/2004/06/10/1086749842546.html>

²⁰ *FARC downs power lines 24 hours after electricity restored.* EFE World News Service. January 4, 2006.
<http://business.highbeam.com/436103/article-1G1-140492511/farc-downs-power-lines-hours-after-electricity-restored>

Infrastructure Implications

Threat actors armed with explosive devices have the potential to physically damage or destroy substation, transmission, distribution, control centers, or generation components. Physical threats can take the form of:

- Individuals armed with small handheld explosive devices
- An individual driving a vehicle rigged with explosives through a substation or generation facility fence
- Sabotage of equipment using stand-off weapons, long-range rifles, or shoulder-launched weapons
- Hijacking a control center and forcing individuals to cause damage or disruption to the system at gunpoint

Threat actors armed with knowledge of industrial control systems and cyber attack have the potential to take control of and misuse physical assets to cause service disruptions or even to physically damage system assets. Cyber threats can take the form of:

- Distributed Denial of Service (DDOS) Attack—attackers flood network resources to render physical systems unavailable or less than fully responsive for a period of time
- Rogue devices—an unauthorized device accesses the system, manipulating it or providing incorrect data to system operators
- Reconnaissance attacks—probing of a system to provide attackers information on capabilities, vulnerabilities, and operation
- Eavesdropping attacks—violations of confidentiality of communication within network
- Collateral damage—unplanned side-effects of cyber attacks
- Unauthorized access attacks—attacks where the adversary exercises a degree of control over the system and accesses and manipulates assets without authorization
- Unauthorized use of assets, resources, or information—attack in which assets, services, or data are manipulated by an authorized user in an unauthorized manner.²¹ This can result in system operators being given inaccurate information from a “trusted” source, and thereby being misled into making decisions based on this data that result in impacts to the system
- Malicious code (Malware)—viruses, worms, and Trojan Horses

Vulnerability

Like other Critical Infrastructures and Key Resources (CIKR), the bulk power system is a highly-complex interconnected system. The critical strategic assets that make up the grid include rotating machinery, transformers, circuit breakers, protective devices, transmission and distribution lines and towers, control centers, and substations. Distributed across thousands of

²¹ Weiss, Joe. *Control System Cyber Vulnerabilities and Potential Mitigation of Risk for Utilities*. Juniper Networks, Inc. 2009, 3-4.

square miles, three countries, and over complex terrain (from the remote plains and Rocky Mountains to major urban areas), the bulk power system is comprised of over 200,000 miles of high-voltage transmission, thousands of generation plants, and millions of digital controls.

Inherent Resilience, Current Practice

The bulk power system is highly redundant and planned with sufficient resources to accommodate expected loads, including a contingency/reserve margin to meet balancing and regulating needs. Each Balancing Area can maintain reliability even with the loss of more than the single largest generating unit in the area. Various planning tests stress the resilience of the grid to accommodate a wide range of severe multiple contingency conditions without resulting in cascading outages. From a physical security perspective, this planned resilience affords significant protection from many physical threats; however, a highly-structured physical, cyber, or blended attack could potentially target multiple assets at once, pushing the system outside the protection provided by system design criteria.

This resiliency also provides a degree of protection from cyber vulnerabilities. System design principles often ensure that primary and backup relays and devices are of different make and model, such that the second would not necessarily be affected by the same vulnerability or failure as the first.

The distributed nature and diversity of the system, while providing a degree of protection in itself, presents important defense challenges to both the public and private sector. Varying levels of security surround bulk power system assets, ranging from heavily guarded and monitored generators to geographically remote substations with little to no physical protection. Installing additional protection elements around these assets comes with an important set of tradeoffs. Fences, for example, may provide a deterrent to access by a malicious actor, but also make it more difficult for personnel and emergency workers to access the substation in an emergency. Lights may discourage subversive activity, but also provide better visibility to those who would attack the station from afar.

Supply-Chain Vulnerability

Reduced on-site supplies and the difficulties involved in securing replacement components present complications to full and seamless recovery. The bulk power system is dependent on long supply chains, often with non-domestic sources and links. Throughout the sector there is an increased reliance on foreign manufacturers, with critical components and essential spare parts manufactured abroad (e.g. HV transformers), and a trend toward lower overall inventory levels. Furthermore, spares may be stored in close proximity to operating assets due to difficulty in transportation and installation, increasing the probability that both the operating asset and the spare could be destroyed in a single event. The supply chain itself represents an important potential vulnerability.

Workforce Vulnerability

Attacks against the bulk power system workforce also present a challenge. The continued successful operation of the bulk power system relies on the workforce that operates, maintains, responds to, and repairs it. Both the management and skilled laborer aspects of the workforce may be said to constitute a component of the bulk power system itself. The industry currently faces a higher rate of engineers becoming eligible for retirement than in the past. Availability of the necessary personnel during all-hazards scenarios may also present challenges, since insufficient personnel on site can significantly delay recovery efforts. Resource sharing agreements among utilities require personnel to travel—sometimes great distances—to support other entities. National security emergencies where restrictions are placed on population movement may restrict ability to travel. Appropriate credentials to distinguish these individuals from the general population during an emergency do not presently exist.

Cyber Vulnerability

Cyber vulnerability presents a growing and increasingly sophisticated threat. As the industry has taken advantage of the benefits of automation and remote monitoring and control in recent years, the grid has become increasingly dependent on the use of digital, communicating controls and systems to operate. The increased use of IP networks for Supervisory Control and Data Acquisition (SCADA) and other operational control systems, in particular, creates potential vulnerabilities. Executives with SCADA/ICS responsibilities reported high levels of connections of those systems to IP networks including the Internet—even as they acknowledged that such connections create security issues. Sector experts express grave concern about the security implications of this development, and security specialists stress the need to address this threat.²²

Cyber vulnerability extends far beyond the control room into communicating devices across the bulk power system and distribution systems. Roughly 85 percent of all system relays are now digital. Other potentially vulnerable devices can include remote terminal units, circuit breakers, static var compensators, capacitor bank controllers, demand response systems, meters, plant control systems, plant emission monitoring systems, and Energy Management Systems (EMS) within major facilities. Vulnerabilities can be inherent to the products industry purchases and installs, highlighting the importance of ensuring a holistic approach to protection: vendors and equipment manufacturers must ensure products are secure prior to purchase. The industry, for its part, should include security requirements in purchasing specifications and decisions.

Smart Grid Devices

New “smart grid” devices create another potential path for cyber vulnerability. The smart grid represents an important innovation in grid management that may ultimately benefit reliability and grid operations. These systems may enable increased grid reliability with better measurement and execution of energy efficiency initiatives, enable demand response, and

²² *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. Stewart Baker, Shaun Waterman, George Ivanov, McAfee, 2009

facilitate the integration of distribution-level assets, such as rooftop solar panels, local wind generation, and plug-in hybrid electric vehicles. The mass deployment of these assets redefines the nature of the traditional protection perimeter with respect to cyber security by extending the network into homes and businesses. The concern is not with the attack or manipulation of a single smart meter or device—as one might imagine billing fraud—but the potential for sabotage of an entire smart meter network or a significant portion thereof, as was demonstrated by ioActive at the 2009 Black Hat Conference²³. While individually these assets may not have an impact on bulk power system reliability, in aggregate the system may control a significant amount of load. The potential for remote disconnect and manipulation of demand response programs needed for reliability is of most concern, followed by the provision of additional access points to distribution and transmission systems via communications channels. Similarly, manipulating data stream from Phasor Measurement Units (PMU) may have significant impact on bulk power system reliability.

All of these communicating devices have enabled unprecedented situation awareness and efficiency gains in system and market operations. These efficiencies have enabled the electric sector to optimize the reserve-carrying requirements of the system and overall infrastructure redundancies over the past 15 years. While these advances have resulted in many benefits to the reliability and economic efficiency of the grid, they have presented an important trade off from a security perspective: redundancy can reduce vulnerability by increasing the number of viable assets.

Physical Aspects of Cyber Threats, Common Modal Failure, Advanced Persistent Threats

An important and often underappreciated aspect of cyber risk is that assets controlled by a communicating intelligent device are themselves made vulnerable to damage or destruction. Idaho National Laboratories ran a test that exhibited such a vulnerability in 2007. Dubbed the “Aurora” vulnerability, it demonstrated the potential for remote control, misuse, and damage to a small generator. This attack did not use any Internet connections or traditional IT vulnerabilities.

Additionally, the potential now exists in the cyber sphere for common modal failure of assets, meaning that a single exploitation of a vulnerability can be propagated across a cyber or power system network and potentially affect an entire class of assets at once. While current system design practices do provide a measure of protection from such a threat, this potential essentially redefines “single points of failure” from a system planner’s perspective, distributing the effects of a single attack across an entire system or network.

Advanced Persistent Threats (APT) are becoming a significant concern across all sectors. These threats involve sophisticated, determined, coordinated attackers who systematically compromise government and commercial computer networks. These attackers typically install multiple backdoors into a cyber network they are attempting to infiltrate, under the “radar” of even the most sophisticated anti-virus protections, thereby establishing a secure foothold into the network. They then install utilities to exfiltrate data to external servers. Attackers respond to attempts to

²³ Davis, Mike. SmartGrid Device Security: Adventures in a new medium. Presented at BlackHat U.S.A. 2009. <http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf>

eradicate infection and remediate network security by establishing additional footholds and improving sophistication. These infiltrations can persist, untraced, for months and even years. The extent to which these infiltrations have spread through electricity-sector networks is not clearly known, but analysis of several networks shows thousands of compromised computers. Unconfirmed reports of APT threats were the subject of an April 2009 article in the Wall Street Journal.²⁴

Forensic and Response Tools

Part of the reason these threats are able to go untraced is that software-based forensic tools to seek out, identify, and eradicate these infections on system assets simply do not exist today. This represents a significant vulnerability in lack of visibility and response capability that extends into virtually all critical infrastructure sectors—including the defense industrial base and U.S. government. Another reason is the difficulty in detecting malware that is designed to be concealed. When scanned, they have the ability to change to avoid detection. This requires a new level of system or network administration skills. Cyber forensics for legacy control systems are minimal at best even to identify primitive cyber attacks.

Knowledge and Process Vulnerability

The physical and cyber vulnerabilities discussed above are compounded by immature processes and knowledge-development programs. As a coordinated attack has not been experienced to date, an operator faced with such an attack would have no real-life experience to draw on when responding to it. Further, little training presently exists to drill responses to these events, though certain organizations have recently begun to incorporate this material into their training programs. The Western Area Power Administration's Electric Power Training Facility, for example, has created a blended attack scenario in its simulator and has added this scenario to its operator training course.

In many cases, however, the knowledge of how to defend against cyber attacks cannot keep pace with technological innovation and adversary capabilities, as the newest technology implemented is never as well understood by those trying to guard it as its predecessor. This vulnerability is best summed up by the statement that “we only know what we already know; we don't know what we're missing.” Though there are some personnel within the sector who have expertise in planning for and against such contingencies and actors, these individuals are relatively few in number and the capability of individual entities varies widely. This issue can be compounded by vendors who are either unprepared or unable to quickly remedy newly-identified vulnerabilities. Vendor staff with intimate knowledge of the control system components can be just as critical to the operation of the system as the operators themselves.

Processes to disseminate threat and early warning information to personnel also require maturation. NERC launched a formal alerts system in 2007 and has been working to improve the system's reach, efficacy, and security over the past two years. The new system, due to be

²⁴Gorman, Siobhan. *Electricity Grid in U.S. Penetrated By Spies*. The Wall Street Journal. April 8, 2009. <http://online.wsj.com/article/SB123914805204099085.html>

commissioned in the second quarter of 2010, adds significant functionality, allowing entities to securely acknowledge receipt of the alert, protects private information, and limits the amount of information being exchanged via e-mail; nevertheless more work is needed to create a common lexicon for efficiently communicating about physical and cyber risk and developing and exercising the communications protocol with reference to these events from the affected entities to their Balancing Authority and Reliability Coordinator to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).

Important gaps also exist in information-sharing between the public and private sector. Today, a limited number of sector personnel have security clearances that enable them to receive the kind of information needed to address newly identified vulnerabilities. In order to appropriately mitigate an issue, engineers in the private sector need detailed, timely, and actionable engineering information regarding the threat. Relevant tactics, techniques, and procedures drawn from terrorist attacks on electric sector assets abroad could also be integral to addressing certain threats. Much of this information has typically been classified and not readily provided to industry. Asset owners and operators are ultimately the only entities able to mitigate vulnerabilities. Further, a clear, coordinated source of information and communication path is needed from the public sector to the electric sector.

Consequence

The consequences associated with a coordinated cyber and/or physical attack could result in the physical damage or destruction of critical assets, such as generators, substation components, and large transformers. If conducted on a large enough scale, it is possible that the bulk power system could not recover in its present form, but would need to be restored in islands or using rotating outages where enough equipment was still available to operate the system.

In addition, some energy sources used for electric generation are imported. A disruption to one of these energy sources or the mode of transportation that provides it can produce delays within the electric sector. These supply chains create external dependencies on non-bulk power system support infrastructure that is vulnerable to attack.

Characteristics and Unique Attributes

Coordinated attacks have a very different profile from higher frequency (better understood) and probabilistic outages. For example, a typical severe weather event could result in the temporary loss of transmission components over a relatively bounded geographic area. A coordinated attack could potentially affect specific key assets over a broad geographic area, such as an entire RC footprint, an entire interconnection, or even multiple interconnections.

Coordinated attacks may also be planned for when the system is most vulnerable to attack: a hot summer weekday afternoon. An adversary with enough knowledge of how the system operates may also be able to plan an attack to capitalize on periods of the day when system frequency is

most volatile. The planned significant increase in variable generation, with its characteristic morning and evening ramps, may also provide windows of opportunity to a would-be attacker.

Coordinated attacks are also adaptive in nature, meaning the adversary can anticipate and respond to efforts by grid operators to restore the system. This is particularly concerning with respect to a cyber attack, where operators could be given spurious information from a typically trusted source, causing them to make decisions that may worsen the situation.

Coordinated attacks also have the potential to recur or be launched in a sequential fashion. Operators may be able to restore service and begin to operate the system in a conservative mode. A subsequent attack could occur hours or days later, however, causing instability or additional outages. Such an action could thwart restoration efforts by creating a new list of restoration priorities. This is an important concern when it comes to the management of nuclear reactors, which can take days and even weeks to restore to service after a major outage, as was noticed in Ontario in August 2003.²⁵

A coordinated cyber attack may also result in the loss of visibility and control of the system, severely complicating restoration efforts. The capability to operate the bulk power system without certain systems exists, but would result in severe restrictions on market operation and reliability measures.

Mitigations

Perhaps the first step to adequate mitigation is the acknowledgment that fully protecting the system from a coordinated attack is not possible. As noted earlier in this section, the bulk power system is literally comprised of hundreds of thousands of miles of high-voltage transmission lines, over 150 Balancing Authority Areas, and millions of digital controls. Conducting regular patrols of the entire grid and ensuring immediate and sustained protection of each and every relay, control system component, and communicating device on the system from an ever-changing threat is neither feasible nor cost-effective. In the case of a physical attack, September 11, 2001 serves as an important reminder of how vulnerable North America's infrastructure can be to those with malicious intent. On the cyber security side, roughly 25 million new strains of malware were identified as threats to business networks across the economy in 2009.²⁶ Protection efforts, no matter how robust, will always be lagging behind this incredibly effective innovation cycle. Additionally, control systems have long lifetimes and may not be able to be modified to meet new cyber threats.

As a result, effectively mitigating the effects of a coordinated attack on the system will require a strong mix of preventative measures designed to build on the inherent resilience of the system

²⁵ *Final Report on the August 14th Blackout in the United States and Canada: Causes and Recommendations*. Chapter 8: *Performance of Nuclear Power Plants Affected by the Blackout*. U.S.-Canada Power System Outage Task Force. 2003. <http://www.ferc.gov/industries/electric/indus-act/blackout/ch7-10.pdf>

²⁶ Annual Report, PandaLabs 2009. Panda Security. January 2010. http://www.pandasecurity.com/img/enc/Annual_Report_PandaLabs_2009.pdf.

and preparatory measures that will enable system operators to recognize an attack and respond to it when it does occur.

Planning

As noted earlier in this section, the bulk power system is inherently highly-resilient to threats. Probabilistic planning criteria consider a wide range of potential contingencies and consider probabilistic failure (i.e. equipment failure, human error, and weather events) yet do not consider a structured, coordinated, and intelligent attacker. Additionally, the definition of a “single asset” under this criterion is often based on the probabilistic failure of a given system component (i.e. a single bus or circuit breaker or a single unit at a generating plant) and may not cover the loss of every component at multiple given physical locations (i.e. several entire substations or generating plants), as could be effected by a physical attack. Cyber attacks take this one step further by creating the possibility that an asset could be misused to affect assets connected to it. Consider the example of a large substation with multiple generating units connected to it. Though this capability has not been successfully demonstrated to date, an experienced cyber attacker could use relays and breakers within that substation to affect the operation of each of those plants.

In order to accurately evaluate the system’s resilience to structured attacks, the sector should work to incorporate these new perspectives and take a broader view of the system than is generally provided by traditional system planning and operating criteria. Entities within the sector have conducted such analyses with results that indicate the system would retain its integrity were certain targeted attacks conducted, however this practice should be considered more widely as planning methods evolve. Priority should be given to designing for survivability, such that the system could withstand and recover from a structured multi-node attack. At a minimum, system planners and operators should be able to model the effects of such an attack and drill restoration measures.

Though the system is highly redundant, certain key nodes, if damaged or destroyed in a coordinated fashion, would have a greater impact on system restoration than others. Key loads, such as military installations and other critical infrastructure components (i.e. major natural gas hubs or telecommunications facilities), are other important elements of the system from a societal perspective that must be considered. In order to build on the inherent resilience of the system with respect to a coordinated attack, these key nodes should be identified and prioritized for protection within the sector.

Likewise, other infrastructures should take electric sector needs into consideration as their attack response plans are developed. Ultimately, a holistic approach will provide the most effective protection to North America’s critical infrastructures. Protection goals and risk-based planning thresholds should be defined and developed in a cross-sector framework, taking interdependencies into account. Focus should be given to making security a design principle. The following questions will need to be answered as these goals are developed:

- How much risk is the private sector willing to accept?
- How much risk is the public sector willing to accept?
- How much are consumers (or society at large) willing to pay to reduce this risk?
- Who makes the determination for society's tolerance for risk and the cost of employing protections?
- How should the costs of employing protections be paid for?
- How is damage measured: cost to replace damaged equipment, number of people-hours without power, number of other critical infrastructure nodes affected?
- Where are interdependencies most critical?

Once protection goals have been developed, an assessment of the system as designed today should be undertaken to ascertain whether modifications to operating procedures, additional protective measures (i.e. fencing, isolating networks), or additional backup assets are needed to ensure the goals are met. The strengthening and expansion of backup equipment sharing programs may be a critical component of needed improvements, particularly with respect to high-voltage transformers. Almost all of these assets are currently manufactured offshore and procurement can take 12-24 months. The "Spare Transformer Equipment Program" (STEP) run by the Edison Electric Institute²⁷, NERC's Spare Equipment Database, and the U.S. DHS Science and Technology Directorate's Recovery Transformer Project²⁸ are important steps, but ongoing efforts to improve these programs should continue.

Ultimately, efforts should be considered to bring more of the supply chain and manufacturing base for these critical assets back to North America. This is also true for digital and solid-state devices such as relays and system controls on the cyber-security side, where the potential could exist to pre-install malicious code or vulnerability into the device prior to shipping to North America. Once a built-in vulnerability is uncovered, it may be too late to address the issue with the supplier. Unfortunately in many cases, this may not be possible. Therefore, alternatives must be considered, such as modifying acquisition practices, developing new quality assurance testing methods, and assessing practices from other sectors, such as the Defense Industrial Base sector.

Changes may also be required to the configuration of cyber systems and services within the operating environment. Enhanced "defender actions" should be developed, giving system operators more tools to combat an attack and isolate and maintain core functions were other auxiliary functions compromised. The system should be designed to gracefully degrade in terms of capability without a material effect on operational reliability. This might mean, for example, that non-essential tools and functionality are shed, but control and communication with generating plants is maintained. If not already in place, this would require clear separation between core system reliability functionalities and business and market systems, external networks, and non-essential inputs. Networks should be designed such that these services can be

²⁷ Edison Electric Institute's "Spare Transformer Equipment Program" (STEP) website:
<http://www.eei.org/ourissues/ElectricityTransmission/Pages/SpareTransformers.aspx>

²⁸ U.S. DHS Science and Technology Directorate's "Recovery Transformer Project" website:
http://www.dhs.gov/files/programs/gc_1218480826191.shtm#14

quickly and easily disconnected from critical reliability functions at a moment's notice without affecting operational reliability. This will essentially allow system operators to “fly with fewer controls.”

Capabilities must also be developed to identify, contain, and eradicate a cyber intrusion. Systems should be designed such that control system forensics are incorporated into the control system design and containment points and firewalls are built into the network architecture: viruses should not be able to “jump” easily from one area of the system to another. Work begun to establish physical and electronic security perimeters as part of compliance with NERC Reliability Standards CIP-005 and CIP-006²⁹ should be continued and refined as more is learned. Qualified personnel must be able to access all points on the system within a reasonable timeframe to resolve issues that may arise. Infected nodes may need to be thoroughly disconnected from the remaining network to avoid the spread of an infection. Operational procedures must take these kinds of outages into account.

Proposal for Action

Coordinated Attack 7

NERC, the U.S. DOE, and appropriate government authorities in Canada should work with technology and software suppliers and the international community to encourage the development of forensic and adaptive network security tools for control systems. The authorities should specifically support research and development of protection and mitigation tools for cyber attack against the bulk power system. These tools should include enhanced forensic and cyber network monitoring capabilities, tools and protocols to allow for the graceful degradation of the system, and improved security for bulk power system components. Consideration should be given to creating a testing or certification center and standards for products and software, taking potential cost implications into consideration. Consideration should be given to developing cost-effective mechanisms to better secure existing assets as well.

Adequately addressing vulnerabilities will also require close coordination with technology vendors and developers. Ensuring protections are “built-in” to system components purchased by asset owners as opposed to requiring a “bolt-on” solution in the future will significantly enhance the security of the system. The bulk power system is ultimately only as strong as its weakest link. All components should undergo rigorous security testing prior to installation on the system. A national testing and certification center should be considered, particularly with respect to new smart grid technologies.

All of the cyber-security-related capabilities mentioned above will depend on having the qualified personnel available to execute these efforts. There is presently a shortage of such personnel as no formal training or certification programs are available that will simultaneously train potential candidates on both power system design and cyber security. Both the public and private sectors should work with academia to develop and support such programs.

²⁹ *Critical Infrastructure Protection (CIP) Reliability Standards* section of NERC's *Reliability Standards for the Bulk Electric Systems in North America* at: http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf

Proposal for Action

Coordinated Attack 8

Work begun in 2007 by the National Science Foundation and the Institute of Electrical and Electronics Engineers (IEEE) on workforce development for the electric sector should continue and be expanded to include the development of academic programs designed to train students on the planning, design, and operation of the bulk power system, as well as cyber and network security. The IEEE Education Society has produced two “Ready Now” modules on Cyber Security. Both the public and private sectors should support work with academic institutions to further develop these courses of study.

Response and recovery plans should also be developed down to the field level to ensure all layers of an asset owner are prepared to respond to a coordinated attack. Coordination with local, state, and federal law enforcement—as well as the military—must be planned and tested in order for an effective response to be mounted. Plans should be developed to provide for the reliable operation of the system for extended periods of time with critical elements out of service due to physical damage.

Information sharing practices between government authorities, the intelligence community, and the private sector will be critical to any plan to improve response capability to cyber and physical attack. The present structure does not allow the electric sector to receive timely, actionable, and detailed information relative to emerging threats and vulnerabilities.

Proposal for Action

Coordinated Attack 1

The U.S. DOE and Department of Homeland Security (DHS) and appropriate government authorities in Canada should work together to establish clearer and more direct lines of communication and coordination with the electric sector. Focus should be given to improving the timely dissemination of information concerning impending threats and specific vulnerabilities, and on the provision of information with sufficient engineering depth for private-sector entities to evaluate and deploy suggested mitigations. Increasing the number of security clearances available to industry may facilitate this objective in the short term, but specific focus is needed to appropriately de-classify information needed by the private sector.

Proposal for Action

Coordinated Attack 2

NERC's Board of Trustees should direct its technical committees to formalize initial efforts to evaluate the efficacy of current bulk power system planning and operating practices with respect to protecting the system from coordinated attack threats. The goal of these efforts should be to strengthen the general security posture of the North American electric sector. Similar efforts should be contemplated for smaller generation and distribution systems. The committees should:

- Recommend practices to enhance the efficacy of current planning and scenario criteria in addressing coordinated attack threats;
- Develop an accepted process to identify key facilities for protection and prioritized restoration, to include clear criteria for identifying critical loads;
- Seek and use stakeholder, government, and cross-sector input to develop clear protection goals, using the protection policy currently under development as a foundation;
- Conduct, coordinate, or sponsor an assessment of the North American bulk power system to identify areas where upgrades, modifications to operating procedures, or additional protective or adaptive measures may be needed and recommend actions as appropriate;
- Pursue cross-sector coordination to identify interdependencies and work with other sector coordinating councils to continuously improve security measures for all critical infrastructures; and
- Identify areas where additional and extraordinary costs may have to be incurred and evaluate whether cost-recovery mechanisms and regulatory support may be warranted.

As the committees proceed with their work, coordination with government authorities such as the U.S. DOE, the Federal Energy Regulatory Commission (FERC), and state regulatory authorities and appropriate government authorities in Canada must be brought into the discussion to ensure a widespread acceptance of the cost implications associated with proposed measures.

Proposal for Action

Coordinated Attack 3

NERC, the U.S. DOE, and appropriate government authorities in Canada should work with electric sector to improve the current spare equipment efforts for scarce or long-procurement-cycle assets such that spare equipment can be identified for response in a reasonable response window. Gaps in the inventory of available spare equipment should be identified and addressed, while considering the costs associated with retaining such inventory. Consider re-launching NERC's Spare Equipment Database (SED).

Proposal for Action

Coordinated Attack 4

NERC should form a task force to support and promote the development of scenario-based analysis tools, to include robust system modeling scenarios of potential structured attacks, to assess system response capability. These models should be used to build on existing restoration plans and procedures to specifically address coordinated attack risk. In addition, scenario-based analysis supported by precise modeling will provide a better visibility of inventory requirements for spare equipment and associated cost recovery aspects. The committees should also support and promote the development and coordinated, regular exercise of restoration and recovery plans down to the field level to ensure all personnel are prepared to respond in the case of an attack. Consideration should be given to the potential for operating the system for extended periods without critical elements. These plans and drills should be coordinated with appropriate public-sector entities, such as local law enforcement, the U.S. DHS, and Department of Defense (DOD), and appropriate government authorities in Canada. Appropriate engagement with critical loads should also be pursued.

Proposal for Action

Coordinated Attack 5

NERC's Board of Trustees should direct its committees to support and promote the development of system operator training scenarios for physical and cyber attack. The group should consider recommendations to NERC's System Operator Certification and Continuing Education Program for potential training requirements.

Proposal for Action

Coordinated Attack 6

Working with its stakeholders either through a new task force or through existing structures, NERC should coordinate with the U.S. DOE, DHS, and FERC, and appropriate governmental authorities in Canada to develop a common lexicon for communicating about cyber and physical attack risk to ensure clear and concise communication is possible during an event. NERC and the electric sector should promote and support the integration of this lexicon into control centers across North America, giving consideration to whether modification is needed to NERC Reliability Standards to ensure the uniform adoption of this lexicon across the sector.

Operations

Much of the work needed in the operations realm involves making use of the plans and procedures developed by system planners and ensuring system operators are prepared to respond in the event of an attack. Just as system planners must design the system for survivability, operators must learn to make use of available defender actions to ensure seamless response should an attack occur. Integrated training simulations should be developed for personnel ranging from system operators to field technicians, training personnel to respond to an adaptive attack. Situations where operators can no longer trust the output of key diagnostic systems due to cyber compromise should be regularly drilled to ensure operators are able to recognize an

attack and deal with its effects appropriately. These scenarios should be routinely drilled with the full range of affected staff and functional entities: asset owners and operators should drill communications with their Reliability Coordinator and Balancing Authority, as well as the ES-ISAC and government authorities. Focus should be given to restoration and response.

Asset owners and operators must also continue to improve basic security practices such as those outlined in NERC's Critical Infrastructure Protection Reliability Standards and the NIST FISMA³⁰ standards. Conducting background checks on all personnel with access to critical systems, ensuring appropriate protections such as anti-virus programs are in place, establishing physical and electronic security perimeters, and basic incident reporting are all important components of protecting the system from possible physical, cyber, and blended attack.

Better cyber intrusion detection methods should also be developed and integrated into all system networks to ensure attacks are quickly and accurately identified and notifications given to information technology personnel and system and plant control room operators. Priority should be given to collapsing the amount of "free time" an attacker has within the system (See Figure 3 on the following page). Forensic and detection tools in place today require improvement, but that improvement will require close coordination between government, vendors, and asset owners and operators to be successful.

³⁰ NIST's "Federal Information Security Management Act (FISMA) Implementation Project" page at: <http://csrc.nist.gov/groups/SMA/fisma/index.html>

Coordinated Attack Risk

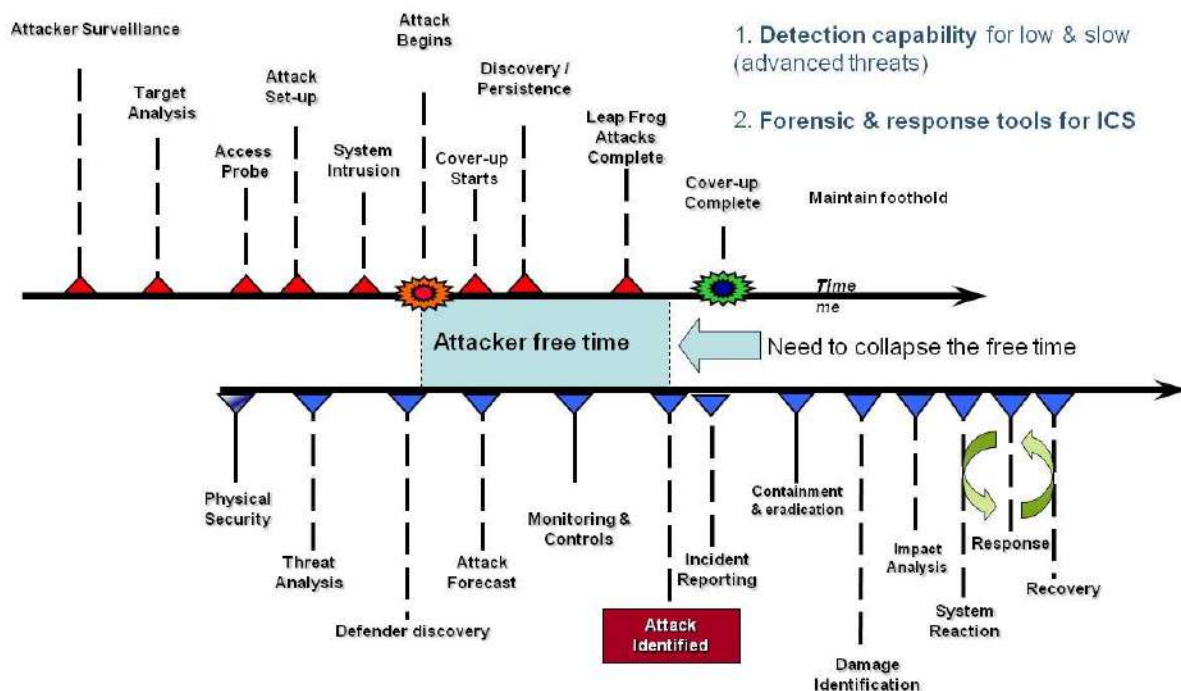


Figure 3: Typical attack time cycle

The ability to accurately flag suspicious activity will be contingent upon asset owners' ability to access up-to-date information on known and emerging attacker signatures, IP addresses, and intrusion characteristics. For a physical threat, a communications channel must be developed between asset owners and the intelligence community to warn asset owners of credible threats. Much of this information presently exists only in a classified environment, precluding public-sector entities from accessing needed information. Information sharing between the public and private sectors will also be critical to the electric sector's ability to mitigate known vulnerabilities. As vulnerabilities are researched and uncovered, this information should be shared with the private sector to ensure mitigations can be speedily evaluated and deployed. Mitigating measures cannot be put into place until a thorough understanding of the problem at hand is obtained. Systems and assets across the bulk power system have unique configurations and it is crucial that system engineers understand all potential consequences of deploying a solution prior to putting it in place. Current information-sharing restrictions have severely limited the sector's ability to address both threats and vulnerabilities. Existing information sharing protocols and procedures must expand and mature in order to effectively mitigate this risk.

A common lexicon must be developed so that system operators are able to clearly and efficiently communicate with one another, their Reliability Coordinators, the ES-ISAC, and government officials regarding the current physical and technological status of the system. A regular reporting protocol, using this defined lexicon, should also be established to improve overall situation awareness on an ongoing basis. Such a language and reporting protocol could be

modeled off of the U.S. Navy's Casualty Reports, a highly-structured system designed to keep the naval fleet at the highest possible state of readiness. Officers in charge of a ship, unit, activity or base submit a casualty report to report the status of a unit with reduced combat readiness due to a casualty, loss of capability, and material damage. The regular review and analysis of this data can identify operational, maintenance, and supply problems, making these reports a key element of the improvement of the fleet's material condition.

Confusing or unclear communication during such a situation would hamper response efforts and lead to potentially dangerous consequences for first-response personnel.

A new role of a security coordinator may be considered as information sharing needs like this increase. Not to be confused with the traditional bulk power system definition of security, which essentially refers to operating reliability, this new security coordinator would be the single point of contact charged with monitoring the cyber and physical security of the bulk power system within a given footprint. This individual could operate at the Reliability Coordinator or Balancing Authority level and would receive and monitor information from government authorities and the intelligence community and communicate potential concerns as appropriate. The individual would also be charged with monitoring the status of the system under their purview and communicating that status to the ES-ISAC to contribute to a broader system-wide situation awareness capability.

Efforts Already Underway

NERC presently has nine Critical Infrastructure Protection Reliability Standards³¹ in place, which are designed to provide a foundation of sound security practices across the bulk power system. The standards are some of the first mandatory cyber security standards put in place in any critical infrastructure sector. Audits began on initial requirements in July 2009. These Standards are not designed to protect the system from specific and imminent threats. Legislation to enhance emergency authority is currently under consideration in the Energy and Commerce and Homeland Security Committees of the U.S. House of Representatives.

NIST also has an effort under way to develop cyber security standards for smart grid components. The work conducted so far is promising, and should continue. The NIST-led Cyber Security Working Group has more than 350 members.³² Focus must be placed on designing secure architectures; developing embedded security, wireless network security and smart grid systems security; and developing appropriate business and privacy strategies on a harmonized platform between the U.S., Canada, and Mexico.

In its role as the ES-ISAC, NERC has also developed an alerting mechanism that it has used to alert asset owners and some government authorities to emerging threats and vulnerabilities. Ten CIP-related alerts were issued to industry in 2009. An enhanced delivery system has been

³¹ *Critical Infrastructure Protection (CIP) Reliability Standards* section of NERC's *Reliability Standards for the Bulk Electric Systems in North America* at: http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf

³² SGIP/NIST "CyberSecurity Working Group" collaboration site: <http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG>

developed that will allow recipients to log into a secure portal to view and respond to alerts. The new tool is due to be commissioned shortly and will be exercised regularly.

NERC has also done important work over the past year to reach out to entities and develop more robust information sharing opportunities. NERC's Network Hydra provides a mechanism for very fast coordination between NERC, asset owners, and vendors.

NERC also began a series of Cyber Risk Preparedness Assessments in 2009 that focused on detection, response, and mitigation capabilities for cyber incidents. Coordinated by NERC, the assessment looked beyond NERC's current cyber security standards for practices, procedures, and technologies that contribute to cyber preparedness across the industry. Generalized, aggregated results from the assessment will be used to inform standards development activities, alert the industry to potential areas of concern, and identify areas where research and development investment is needed. For security reasons, specific results of the assessment will remain confidential, a key condition of participation in the program.

DOE participates in the federal government effort on global supply chain risk management in The Comprehensive National Cybersecurity Initiative (CNCI)³³. The federal government has realized that managing this risk requires a greater awareness of threats, vulnerabilities, and consequences for acquisition decisions, and the need to develop new policies and best practices in partnership with industry. DOE started a project to evaluate supply chain vulnerabilities on several levels. DOD has led the effort to reduce supply chain vulnerabilities in the Defense Industrial Base sector. This project will leverage DOD's and other sectors' efforts under CNCI to develop tools and resources to mitigate risk across the lifecycle of products, and develop new acquisition policies and practices. DOE will evaluate the current state for gaps, and apply the lessons learned to the Smart Grid architecture, systems, and components.

Proposal for Action Coordinated Attack 9

The U.S. DOE, coordinating with government authorities in Canada as appropriate, should continue efforts to evaluate appropriate means to bring more of the supply chain and manufacturing base for high-impact system components, such as extra high-voltage transformers and system controls, back to North America to ensure these components are available and built in an uncompromised environment should a widespread attack or disaster occur.

NERC's standing Critical Infrastructure Protection Committee³⁴, established nearly a decade ago, also deals with security and cyber security related matters, issuing guidance and providing opportunities for information sharing within the industry.

³³ The Comprehensive National Cybersecurity Initiative, National Security Council, <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>, accessed March 10, 2010.

³⁴ NERC's Critical Infrastructure Protection Committee website: <http://www.nerc.com/page.php?cid=19|117|139>

Additionally, NERC formed a Smart Grid Task Force³⁵ in July 2009 to provide a high-level review of the reliability impacts of integrating smart grid technology on the bulk power system. The task force is actively preparing a report that reviews smart grid characteristics, identifies reliability concerns including cyber-security vulnerability, and provides recommendations to NERC and the industry.

³⁵ Smart Grid Task Force website: <http://www.nerc.com/filez/sgtf.html>

Pandemic Risk

The world has just experienced a mild pandemic influenza in the form of the 2009 A/H1N1 or “Swine Flu” virus. The 2009 pandemic has been the mildest in terms of mortality rate and severity of symptoms of any pandemic recorded in the past century. The potential exists for a much more severe event to occur; an event that could affect the operation of the power grid by making a significant portion of the workforce ill or unavailable to come to work due to family illness or school closings. This presents a unique threat to the bulk power system as the system is heavily reliant on critical personnel to operate reliably. Without proper planning, the loss of critical personnel will place the system at higher risk of operational events occurring. As learned through the 2009 A/H1N1 event, planning for and responding to a pandemic is not a task the sector can take on alone: it will require close coordination with government and health authorities to ensure appropriate and coordinated steps are taken in a timely fashion.

Risk Identification: Defining the risk in terms of the reliability impacts to the grid

Threat

A pandemic is defined as a global outbreak of a new virus or disease with sustained and efficient human-to-human transmission. Generally little or no immunity exists to the disease and it causes illness and, in some cases, death. The severity and duration of pandemics vary significantly and will be difficult to predict, as each virus carries its own unique set of characteristics. Several pandemics occur each century, with the best known case being the bubonic plague (or “black death”), which is estimated to have killed 40-60 percent of Europe’s population in the 14th century. Relatively recent advances in medical care have helped limit the scope and impact of pandemics in North America over the past 50 years, though concern in the health care community persists regarding multi-drug resistant strains and new viruses with the potential to be both highly-infectious and deadly. While this section primarily focuses on the potential for pandemic influenzas, the principles and issues discussed are generally applicable to all acute infectious agents.³⁶

The effects of a pandemic on the electric sector will differ from other HILF events in that pandemics are “people” events. Unlike in a coordinated attack, the initial impact to the bulk power system isn’t physical damage to the grid but rather the absence of critical personnel who operate the grid and those who support them.

The potential exists for severe workforce reduction either due to personal illness, widespread fear of contracting the illness, family issues (lack of day care, school closings), or possible sequestration or confinement as a result of government intervention. A reduction in the availability of highly specialized grid and plant operators may make operating the system reliably increasingly challenging.

³⁶ *Pandemic*. Wikipedia. <http://en.wikipedia.org/wiki/Pandemic>

The threat of a pandemic influenza merits careful consideration. It differs from most other threats for the following reasons:

1. **Worldwide Impact** — unlike many threats that are localized, a pandemic has the potential to impact operations simultaneously across North America and around the world. It will affect employees and the availability of resources and services the electric sector depends upon.
2. **Duration** — an influenza pandemic could severely disrupt operations through multiple waves that could last six to eight weeks and span several seasons or even years. Some level of fear would spread through the population prior to the actual outbreak and the actual “sickness” period would range from a day to a week for most individuals.
3. **Mortality** — mortality rates vary. Even a low-end mortality rate would cause severe disruption for employees who lose family members and friends.

Pandemic influenza differs from seasonal (or common flu) in important ways. The common flu has predictable seasonal patterns, occurs annually and usually in the winter months. Healthy adults are usually not at risk for serious complications and immunity builds up from previous exposures. Vaccines are typically developed commercially and are widely available. The health and human services sector is typically well-equipped to handle the common flu and seasonal changes do not result in any particular societal response.

A pandemic influenza, on the other hand, would have very different impacts. Once human-to-human transmission of a pandemic has begun, the disease will spread very rapidly around the world, likely within three to eight weeks. Infection rates vary widely from pandemic to pandemic, as do the relative health impacts and segments of the population most at risk. Absentee rates for employees will be exacerbated by the need to take care of other family members and the inability to get to work. Individuals who contract the virus are not generally expected to contract it a second time due to a buildup of immunity. However, if the virus mutates, the possibility of recurrences would exist.

Although influenza is highly unpredictable, it is expected that a pandemic will strike in at least two waves, each lasting six to eight weeks. The first wave will typically peak in three to four weeks. The second wave will likely occur three to six months after the first wave and could be more severe than the first due to mutation of the virus. A third wave may also occur with characteristics similar to the second. Employees will need to be managed differently to conduct critical functions and ensure appropriate infection control measures are implemented. The pandemic could last from six months to as many as three years.

Vaccine development must be specific to the viral agent and requires time to grow the virus in a growth medium and subsequent testing for efficacy and safety. Therefore, meaningful availability of vaccines is expected to lag behind the pandemic emergence of the virus by many months. In addition, the availability of anti-viral medication may be limited and will likely be insufficient to supply the needs of the entire population. Also, viruses may or may not be responsive to particular antiviral medications and, even if initially responsive, may develop

resistance. Without appropriate planning, very limited quantities of anti-virals will be available in the early stages of the illness. Limited quantities will then slowly become available for select portions of the population.

Active Threats

In March 2009, the world experienced a “mild” influenza pandemic (A/H1N1) originating in Mexico and spreading throughout the globe within weeks. Though initial reports indicated a high mortality rate, symptoms associated with the outbreak were generally mild, with a nearly negligible mortality rate in developed countries. According to mid-range estimates published by the U.S. Centers for Disease Control³⁷, roughly 57 million people in the U.S. were infected with the virus between April 2009 and January 2010. Of those, it is estimated that nearly 15,000 people were hospitalized and roughly 10,000 died. A resurgence of the disease occurred between mid-October and mid-November, with influenza-like-illness peaking nationally at 7.7 percent of the population (including seasonal flu) during the week ending October 24, 2009.

The 2009 A/H1N1 outbreak did not exhibit many of the characteristics most concerning to critical infrastructure sectors, nor did it provide an opportunity to fully test critical portions of pandemic response plans. While initial reaction to the virus did result in scattered school closings and general public concern, as more was understood about the virus fewer and fewer precautions were deemed necessary. One observation is unmistakable: the speed at which this virus spread throughout the world should be an indicator for future occurrences. While the 2009 A/H1N1 outbreak was relatively mild in terms of severity, future pandemics are expected to be more severe.

Another active pandemic threat is the H5N1 (Avian or bird flu) virus, an especially dangerous strain that closely resembles the 1918 strain discussed below. In 2005, fatal human cases occurred in Asia and Turkey while migratory birds carrying H5N1 were found in Europe (Ukraine, Turkey, and Greece) and Australia. The H5N1 strain originated in birds and has been transmitted from birds to humans, but human-to-human transmission has not yet been confirmed. Due to viruses’ ability to mutate and combine with other viruses, it is possible that the H5N1 virus may evolve into a highly-transmissible, highly-lethal virus. Health officials believe human-to-human transmission will occur, but cannot predict when. The human mortality rate in Asia for those infected has been above 50 percent. While the antiviral drug Tamiflu may be partially effective in treating the illness, a vaccine has not yet been developed.³⁸

Other Historical Examples

Several pandemics have occurred in North America over the past century, with the most recent event being the outbreak of the A/H1N1 virus in April 2009. Pandemics have occurred with a wide variation of symptoms and mortality rates.

³⁷ CDC Estimates of 2009 H1N1 Influenza Cases, Hospitalizations and Deaths in the United States. U.S. CDC. http://www.cdc.gov/h1n1flu/estimates_2009_h1n1.htm

³⁸ United States Centers for Disease Control. <http://www.cdc.gov/flu/avian/outbreaks/current.htm> (As viewed on 4/28/10)

The 1918 “Spanish Influenza” lasted from approximately March 1918 through June 1920. An estimated one third of the human population was infected with the disease. It is estimated that 10-20 percent of those infected died as a result of the disease. Between 50 and 100 million people died worldwide, with 500,000 deaths recorded in the U.S. alone. The virus targeted young adults, whose stronger immune system actually began to attack the body during the disease in what is known as a “cytokine storm”. The spread of this disease was heightened due to increased worldwide travel, especially as troops returned home from World War I. The second wave of the virus was much more deadly than the first.³⁹

The 1957-1958 “Asian Influenza” was a type A/H2N2 virus and proved to be far less virulent and deadly than the 1918 pandemic. The virus was responsible for approximately 70,000 deaths in the United States. This virus later mutated to a type A/H3N2 virus which spread in 1968-1969 (known as the “Hong Kong Influenza”). The initial outbreak reached maximum intensity in 2 weeks, lasting 6 weeks in total. H3N2 was responsible for 34,000 deaths in the U.S. The virus can be transmitted between birds, swine, and humans.⁴⁰

Vulnerability

Similar to other critical infrastructures, the day-to-day operation of the bulk power system is highly-dependent upon the availability of a uniquely-trained and specialized workforce. Significant reductions and impacts to that workforce could have serious and negative consequences for reliability, as it can be assumed that sector employees will be just as vulnerable to the disease as the general public, absent any intervening measures. A severe pandemic could result in workforce impacts that could endure for weeks or even months. Were the impacts significant enough, loss of institutional knowledge could occur with loss of key employees. A pandemic outbreak will simultaneously have similar deleterious effects on all sectors of society around the globe. The failure to maintain the reliable delivery of electricity to consumers would have serious and immediate impacts to society, national security and the ability to manage the event.

Utilities and other users, owners and operators of the bulk power system face many of the same challenges other large corporations would face during a pandemic. Execution of pandemic and business continuity plans will change the “rules” of the working environment, including social distancing procedures, modifications to sick-leave and absentee policies, and addressing family and human needs of staff. The electric sector, however, will face unique threats due to the real-time operating environment of the system and the high degree of specialization required to complete key job functions. Certain functions, such as system operators, require special certification and others may only be well understood by one or very few individuals within a given organization. The loss of these critical employees, even for a short time, can result in reliability impacts, delays in storm restoration, and delayed resolution of key technical issues.

³⁹ *Pandemic*. Wikipedia. <http://en.wikipedia.org/wiki/Pandemic>

⁴⁰ *Pandemic*. Wikipedia. <http://en.wikipedia.org/wiki/Pandemic>

Nuclear refueling provides one illustrative example of an area requiring significant specialization with stringent processes and procedures not easily transferable from employee to employee. 18-month cycles dictate specific refueling schedules using specialized vendors on site to aid in the process. Refueling can take an entire generating unit offline for several weeks as outside vendors and employees perform maintenance and prepare the unit to come back online. Hundreds of steps are necessary for a successful refueling and lack of those critical vendors would prevent the refueling from taking place. Workforce impacts could delay or impair the entity's ability to restore the unit to service on schedule, potentially impacting other scheduled maintenance across the system.

The electric sector also faces unique challenges in mitigating the effects of a pandemic. While non-critical business functions can be curtailed, common social distancing and mitigation practices may not be effective where their impacts would be most important: in system operations centers and among restoration crews. Common working areas and close interaction with colleagues create opportunities for infection and can aid in the spread of the virus across the organization. Immovable workspaces such as control centers and plant control rooms where multiple employees are sharing or rotating to the same work stations can further exacerbate this issue, as can close contact in the cab of a utility truck or van.

Highly-efficient operations across the sector, following general business trends, have resulted in a reliance on "just-in-time" procurement and delivery of needed assets or resources. While fuel stockpiles and on-site storage generally provide generation plants with some "cushion" relative to fuel supply disruptions, other areas of sector operations may have a greater exposure to a pandemic's impact on their supply chain. Many organizations in the electric sector are highly-dependent on contracted employees and vendors for essential support functions. Breach of contract situations may occur during a pandemic, which would further impact affected entities. Cross-sector interdependencies will also affect the electric sector in the event of a pandemic.

The electric sector has a long history of relying on mutual assistance and resource sharing agreements among entities, designed to provide additional support during an emergency. These agreements typically govern the provision of shared crews and equipment to restore the system after a major weather event or operational issue and allow entities to maintain much smaller workforces than might otherwise be required to maintain reliability at the levels expected today. In the event of a pandemic, entities may not be able to make use of these agreements as they may not have the human resources available to honor them or may be hesitant to send employees to help another entity if it places their staff at a higher risk of infection. This makes awareness of current infection rates and outbreak "hotspots" particularly important to the sector.

The sector would also be vulnerable to government actions during a pandemic, which may impact sector operations and workforce mobility. Closure of state or international borders, quarantine and restriction of movement could impact both fuel and supply chains. These impacts were well understood by government and health officials during the 2009 A/H1N1 event. The cautious treatment of these options should be continued in the future.

NERC and industry participants have completed important steps towards developing industry-wide planning criterion for pandemic planning. However, the successful execution of such a plan is highly dependent on the adoption of a clear and specific severity-based index at the federal level. The lack of clear triggering mechanisms could unnecessarily complicate industry coordination during a pandemic and unevenly affect how entities fulfill reliability obligations. Consistency across the industry will support the tracking of the event and identification of high-risk areas.

The 2009 A/H1N1 outbreak identified a number of key lessons-learned. Key response activation points in plans were designed to correspond to changes in classification of the WHO Pandemic scale. As was so clearly illustrated in 2009, however, a change in the scale did not necessarily correspond to a change in the disease's societal impact in North America. The WHO scale was designed to assess spread of the disease worldwide, not severity of symptoms or mortality rates. As such, a relatively low-impact disease such as the 2009 A/H1N1 can achieve Pandemic status without having a material impact on daily life or day-to-day business operations.

Table 1: Comparison of the 2009 Revised World Health Organization and U.S. Federal Government Response Stages from early in 2009. Both scales focus on a global impact and do not provide adequate severity evaluation to industry.

	Revised 2009 WHO Influenza Planning Phases	Federal Government Response Stages
Preparedness	Phases 1-3: Predominantly animal infections, few human infections	Stage 0: New Domestic Animal outbreak in At-Risk-Country
Response & Mitigation	Phase 4: Sustained human to human transmission Phases 5-6: Widespread human infections	Stage 1: Suspected human outbreak overseas Stage 2: Confirmed human outbreak overseas Stage 3: Widespread human outbreaks in Multiple locations overseas Stage 4: First Human Case in North America Stage 5: Spread throughout the U.S.
Recovery	Post-Peak Possibility of recurrent events (multiple waves) Post Pandemic Disease activity at seasonal levels	Stage 6: Recovery & preparation for subsequent waves

Consequence

The primary consequence of a severe and prolonged pandemic would essentially be the lack of enough qualified personnel to reliably operate the power system. As critical staffing levels are reached and exceeded, power system operations would degrade from full operations. Initially, the grid would be operated less efficiently; transmission elements would be operated further from their limits, and generators would be operated at increased levels of availability in an effort to mitigate the unexpected loss of generation capacity due to increased levels of human error and reduced efficiency in responding to unexpected events. Planned equipment maintenance would be deferred. In time, these actions would become counter-productive as the amount of increasingly important work builds, and the consequences of deferring actions become apparent through decreasing reliability and operational efficiency. Eventually, human error would increase as operators were forced to work longer shifts (and more hours per week) and less experienced personnel were required to take the reins from absent experts. In the field, workforce impacts and travel restrictions may result in slower restoration from weather-related outages.

Characteristics and Unique Attributes

A pandemic affects a critical asset not typically considered in reliability planning (where much of the focus is on infrastructure elements and systems): people. It therefore requires a different way of thinking about this risk and a fundamentally different response. In preparing for a pandemic, focus should be given to planning, coordination, education, and ongoing training.

Unlike other risks discussed in this document, a pandemic would require the industry to rely heavily on the health care and human services sector for support, guidance, and effective action. Clear, direct, timely, and actionable information will be needed from this sector to guide the industry as to available pharmaceutical and non-pharmaceutical intervention options.

The impact of this particular risk is also tied very closely to the severity, duration, and breadth of the disease itself. Each outbreak will be unique and the consequences unknown. Unlike other risks which are typically characterized by a single event or series of discrete events, a pandemic occurs over time and requires adaptive response to appropriately manage its effects.

A highly-virulent pandemic would also leave society with a limited capacity to control or limit exposure to the disease. Once the outbreak has started, health care providers may be able to treat its medical effects, but will likely be unable to stop the disease from spreading.

Due to the wide-reaching, societal effects of a pandemic, cross-sector situation awareness will be essential to response. Today, the threshold for coordinated action is uncertain, similar to other risks discussed in this report. More can be done to better define where this threshold will be, but it will be ultimately dependent on the severity and scope of the disease itself.

Mitigation of the event will be highly dependent on the quality, timeliness, and availability of infection control information from health authorities external to the sector. A communications mechanism to ensure adequate information is provided to all users, owners, and operators of the bulk power system will be important to effective response.

A pandemic also calls into question the viability of mutual assistance agreements to deal with this kind of event. Personnel may simply not be available anywhere in the system to support entities in need. Adequately responding to a pandemic event may require different, non-traditional approaches.

Regulatory relief may also play a more important role in the sector's response to this threat than in others. Especially with respect to administrative requirements, regulations may need to be relaxed to allow entities to prioritize available workforce to maintain operational reliability. Other areas that may be considered are the requirements for active system operator certification as defined in NERC's PER standards. Recently retired or re-assigned system operators whose certification expired fewer than six months prior to the issue may be appropriate alternatives if critical staffing levels are reached. State-level regulations, such as those governing requirements for the amount of time given to restore service to a customer following an outage, may also need to be evaluated and relaxed as restoration times increase due to reduced staffing.

Mitigations

Mitigating the effects of a pandemic will ultimately be focused on maintaining essential reliability services as workforce reductions impact entities' abilities to continue normal operations. Many entities already have extensive business continuity plans in place to deal with the effects of a pandemic. These plans vary widely across the sector, with some entities keeping stocks of personal protection equipment and anti-viral medication and medical staff on hand and others depending on government and health care support for these services.

Planning for and responding to a pandemic outbreak is not a task the sector can take on alone. It requires close coordination with government and health services providers to ensure appropriate and coordinated steps are taken in a timely fashion to contain and limit the spread of the outbreak and ensure employees and their families have access to medications, personal protection equipment, and quarantined living arrangements if necessary.

A better understanding of government (federal, state, and local) actions (e.g. sequestering, quarantining, and travel restrictions) during a pandemic and its potential impact on critical services would improve the sector's ability to manage the event. The need to receive timely and accurate information from public health organizations (e.g. the U.S. CDC) relating to the severity and spread of the pandemic will be necessary to ensure appropriate infection control measures and employee workforce reductions plans are activated. In addition, a clear determination of vaccine availability, priority and distribution would ensure critical function personnel are available to operate the bulk power system.

Planning

Planning to respond to a pandemic involves two basic components: entity-specific planning and sector-wide planning. Entity-specific plans are developed by individual entities to plan that specific organization's response to a pandemic. Sector-wide planning considers the coordination points needed between specific entities, their Reliability Coordinators, NERC, and government partners.

Entity-specific plans essentially have two components. The first is best described as the traditional business continuity plan that focuses on human resource concerns, IT, and other "internal" operations policies. These plans govern how the entity treats issues such as absenteeism, telecommuting, and infection control. Sound entity-specific business continuity plans should consider the following points at a minimum:

- Identifying "critical" staff
- Employee education, including outreach to families
- Travel restrictions
- Infection control in workplace / social distancing
- Access controls to critical work spaces
- Employee / workplace self-screening
- Reporting of medical conditions
- Personal protection equipment stocks
- Identify thresholds for "Critical Staffing Levels"
- Curtailment of non-critical functions
- Alternative sources of personnel for essential functions (roster depth)
- Leave of absence, personal time-off and attendance control policies, taking illness of the employee or a close family member and potential school closings into account
- Alternative modes of delivery, telecommuting & IT capability, remote work sites
- Legal, regulatory waivers for reduced personnel (OSHA, Unions, etc.), "force majeure" contracts, supply chain disruptions
- Visitor restrictions, even for staff who work in different portions of a de-regulated utility
- Impacts to mutual assistance agreements
- "Complacency" issues that may have arisen as a result of the relatively mild nature of the 2009 A/H1N1 pandemic, including resistance to vaccination (as was observed in the fourth quarter of 2009)
- Recovery strategies
 - Unwinding pandemic-specific policies and practices – procedures for bringing people back to work
 - Conduct post-impact analysis then document and share lessons learned
 - Long-term operations with reduced workforce

Many of these efforts are focused on the employee and will therefore require close coordination between human resources, planning, and management personnel. Once the plan has been developed, a training program should be executed to ensure employees and managers across the

organization are familiar with policies and procedure. Drills should be evaluated for portions of the plan involving critical personnel.

The second form of entity-specific planning can be described as governing the entity's operational response to changing workforce conditions. These plans must be highly-coordinated across the sector to ensure reliability can be maintained as entities are affected by workforce reduction. Issues that should be considered as these plans are reviewed and developed include:

- For entities performing dispatch functions (i.e. Reliability Coordinators, Balancing Authorities, and Transmission Operators):
 - Consider thresholds for whether and when market-driven operations and competitive drivers should be suspended and conservative operations put into place
 - May consider specially crafted “cost plus” agreements as the system enters a “self-preservation” mode where reliability is given priority over cost drivers
 - In extreme cases, consideration for operating the system in islands as resources are no longer available for operation
- For generation owners and operators:
 - Consider thresholds for when operation of a given plant should be suspended and the plant taken offline
 - Consider prioritizing staffing levels at “reliability must run” units
 - Consider impacts to maintenance and re-fueling schedules
- For transmission owners and operators:
 - Consider weather-related restoration priorities as they may change due to changing availability of generation

Proposal for Action

Pandemic 1

Sector entities should review their pandemic and business continuity plans to incorporate lessons learned from the 2009 A/H1N1 outbreak and consider much worse scenarios. Gaps in plans should be identified and rectified. Focus should be given to addressing “complacency” issues that may have arisen as a result of the relatively mild nature of the 2009 A/H1N1 pandemic. Entities should collaborate and share information, and consider materials developed by the Pandemic Influenza Working Group to promote excellence in pandemic planning across the sector.

Sector-wide planning and coordination should provide a common framework under which these plans can operate. Plans should be designed to respond to a common and consistent set of triggers in a coordinated and predictable fashion. Information sharing, both from government to private entities and from private entities to government, will be a cornerstone of success in these efforts.

Specifically, a new scale should be developed to provide authoritative information on the relative severity of the illness and outbreak. This new scale could complement the current scale in use by

the WHO, which is based solely on the geographic spread of the outbreak. The 2009 A/H1N1 influenza clearly identified a weakness in the current practice of using the WHO scale as a trigger for business continuity planning: while the A/H1N1 influenza reached the pandemic phase relatively quickly, the symptoms were so minor that the sector did not need to activate portions of their plans that had previously been tied to the progression of the outbreak along this scale. A draft concept was proposed to the U.S. DHS and CDC by the NERC Pandemic Influenza Working Group in 2009 and has been included as Appendix 3 to this report. The draft concept focuses on measuring the severity of the pandemic based on impact to employee absentee rates. The concept focuses on the following parameters as key drivers of rising absentee rates:

- The likelihood of worker contact with the virus, either in the community or at work (e.g. rate at which the virus is spreading, contagion period)
- Severity of the illness and symptoms (intensity, duration, extent to which hospitalization is required)
- Mortality rate (provided by the U.S. CDC)
- Broader societal worry and fear
- Social distancing measures (e.g. school closures, travel restrictions)

The timeliness and granularity of outbreak information as recorded by the U.S. CDC and government authorities in Canada should also be improved. Weekly reports identifying “hot spots” where outbreaks have occurred will be critical to the sector’s response, as will advanced notification regarding school closings and travel restriction recommendations. Asset owners and grid operators rely on this information to trigger actions in their entity-specific plans and appropriately respond to growing threats. This information will also drive the sector’s ability to honor mutual assistance agreements with entities in affected areas.

Leading indicators for illness should also be developed and reported on. Metrics reported to industry today are typically “lagging indicators,” which are only capable of highlighting issues once they have already developed. Leading indicators could provide a useful means identifying predictive patterns, allowing entities to better protect their employees and make smarter decisions about when to take aggressive steps to ensure critical staff are quarantined. The State of Michigan presently has a robust program in place⁴¹ where information such as thermometer and anti-flu symptom medicine sales are tracked and reported to health officials and shared with industry and employers. Similar programs should be considered in other jurisdictions.

⁴¹ *Influenza Surveillance and Avian Influenza Update Reports*. Michigan Department of Community Health. http://www.michigan.gov/mdch/0,1607,7-132-2940_2955_22779_40563-143382--,00.html#2009-2010_MIFF

Proposal for Action

Pandemic 2

The U.S. HHS and appropriate government authorities in Canada should improve the timeliness, granularity and quality of metrics used to measure and report on the emergence and spread of pandemic vectors and related illness. These measures should incorporate or be tailored to meet the needs of the electric sector and other critical infrastructure sectors. A new scale should be developed to provide authoritative information on the relative severity of the illness and outbreak. A draft scale was proposed to the U.S. DHS and CDC by the NERC Pandemic Influenza Working Group in 2009 and has been included as Appendix 3 in this report. Focus should be given to better consolidating and reporting on leading indicators at a national, regional, and local level. Reports should be issued by government authorities weekly, at a minimum, and provide both leading and lagging indicators using current (no more than 7-day old) data in a concise and understandable format.

NERC should work with these entities to evaluate options for a communications mechanism to ensure this information is consistently available to all bulk power system entities. The U.S. DOE, as the sector-specific agency, should work with these entities to ensure appropriate feedback is provided and the work product meets sector needs.

Clear policies should also be established to ensure that electric sector critical staff and their families are given priority with respect to personal protection equipment, vaccines, and anti-viral medication as appropriate. This priority should be made clear in correspondence from government to health service providers. A coordinated mechanism to provide these services to sector employees should also be developed. For example, credentials do not presently exist that would enable health and human services professionals to distinguish critical staff from the rest of the population.

Proposal for Action

Pandemic 3

NERC and the U.S. DOE should work with the U.S. HHS and appropriate government authorities in Canada to ensure critical electric sector employees are given priority with respect to the distribution of vaccines and anti-viral medication and the ability to travel in the event of government-imposed travel restrictions. Consideration should also be given to employees of critical vendors and suppliers of the sector, to include natural gas pipeline operators, railway personnel, and urgent maintenance personnel.

For their part, entities must identify critical staffing levels and protocols to notify their Reliability Coordinator and the ES-ISAC when these levels have been reached. This information will be important to ensuring the sector is able to respond and support entities in need of assistance. This information will also provide an important notification to government officials that the sector may experience difficulty maintaining reliable operations or responding to storms and/or routine outages.

Proposal for Action

Pandemic 4

NERC, the U.S. DOE, and appropriate government authorities in Canada should identify the kinds of information needed from the sector to effectively monitor critical workforce levels across the electric sector during a pandemic. A collaborative group of government and electric sector representatives should develop plans and procedures to efficiently meet information needs while limiting the data collection requirements where possible. This group should also develop mechanisms to share this information across the sector.

Reliability Coordinators and NERC should develop plans to monitor the overall status of the system's workforce during a pandemic to ensure resources can be allocated in the most effective manner possible. This consolidated information should be reported back to entities to ensure broad awareness of the current state of the pandemic's effect on the power system. NERC should develop and issue alerts containing this information and any guidance or specific reporting instructions and issue these to industry on a regular basis during a pandemic outbreak.

Options for regulatory relief during a pandemic should also be considered by NERC and other regulators. The potential, for example, to make use of recently retired staff whose certifications may have expired in the event a critical staffing level has been reached, could be considered. Allowance for temporary suspension of "administrative" requirements could also be considered.

Proposal for Action

Pandemic 5

NERC, working with its stakeholders, should develop a proposal for relaxing regulatory requirements during a pandemic. NERC should collaborate with FERC, state regulators (possibly through the National Association of Regulatory Utility Commissioners (NARUC)), and appropriate government authorities in Canada to evaluate existing regulations and consider where appropriate recognition of circumstances may be warranted, without impacting overall system reliability during a pandemic. An example of such requirements may be certain state-level regulations whereby utilities are subject to financial penalty if local distribution outages are not resolved within a given time window. Non-time-sensitive reporting requirements in NERC standards for bulk power system and generation operators may also be considered. Once developed, the process for relaxing regulatory requirements could potentially be applied to lengthened recovery from other HILF events, such as a major coordinated attack, electromagnetic pulse event, or geomagnetic disturbance.

Operations

Much of the effort needed in the operating realm involves periodic drills of response actions and being aware of the triggers, information, and data needs discussed in the planning section above.

Procedures will need to be trained on and drilled to ensure operations and field personnel are familiar with social distancing, infection control, and self-screening practices.

Cross-training options may also be pursued to ensure designated backup personnel from other areas are better able to seamlessly take over responsibilities when needed.

Operators should also take into account the potential for reduced consumer demand scenarios due to absenteeism impacts across the economy.

Efforts Already Underway

NERC has a standing working group focused on responding to pandemic outbreaks: the Pandemic Influenza Working Group. During the 2009 A/H1N1 outbreak, this group was instrumental in developing guidance in the form of NERC Advisories to alert the sector of emerging developments and providing specific guidance relative to the current state of the threat. The work of this group should continue in the event of another pandemic outbreak.

As discussed above, this group developed and provided a draft concept to the U.S. CDC for consideration in 2009.⁴² This concept, if developed and implemented, would help provide guidance to sector entities by recommending a set of actions based on the relative severity of the outbreak and an assessment of other societal measures and concerns related to the illness (e.g. broader absentee rates, school closings).

Many entities in the sector have developed robust pandemic response plans and are well-prepared to deal with the human impacts of such an outbreak.

On March 29, 2010, the World Health Organization announced an effort to evaluate the handling of the 2009 A/H1N1 outbreak. The organization has formed a review committee to assess the global preparedness and the response to the A/H1N1 influenza pandemic. The committee will also review the functioning of the International Health Regulations (IHR), both in relationship to the pandemic and in terms of other functions not related to the pandemic.⁴³ This effort holds promise and should consider critical infrastructure needs and impacts.

⁴² See Appendix 3 of this report.

⁴³ Transcript of press briefing at the Palais des Nations, Geneva. Dr Keiji Fukuda, Special Adviser to the WHO Director-General on Pandemic Influenza. March 29, 1020.

http://www.who.int/mediacentre/multimedia/pc_transcript_29_march_10_fukuda.pdf

GMD/EMP Risk

Geomagnetic Disturbance, High-Altitude Electromagnetic Pulse, and Intentional Electromagnetic Interference risks are important concerns to the North American electric sector. These risks present the potential for simultaneous damage to system components across wide areas of the continent, which could result in system disturbances and, in extreme cases, severe outages. The electric sector is working to gain a better understanding of these risks in order to evaluate, support the development of, and deploy cost-effective and viable mitigations.

Risk Identification: Defining the risk in terms of the reliability impacts to the grid

Geomagnetic Disturbances

Threat

Intense solar activity, particularly large solar flares and associated coronal mass ejections can create disturbances in the near-Earth space environment when this activity is directed towards the Earth. The coronal mass ejection's solar wind plasma can then connect with the magnetosphere causing rapid changes in the configuration of Earth's magnetic field, a form of space weather called a geomagnetic storm. Geomagnetic storms produce impulsive disturbance of the geomagnetic field over wide geographic regions which, in turn, induce currents (called geomagnetically-induced currents or GIC) in the complex topology of the North American bulk power system and other high-voltage power systems across the globe. For many years it has been known that these storms have the potential to pose operational threats to bulk power systems; both contemporary experience and analytical work support these general conclusions.^{51, 52, 53, 54} The electric sector has taken some meaningful steps to mitigate this risk as outlined in the January 2009 Report by National Academy of Sciences "Severe Space Weather Events—Understanding Societal and Economic Impacts Workshop Report," but more work is needed.

More recently, a number of investigations have been carried out under the auspices of the EMP Commission and also for FEMA under Executive Order 13407 and FERC in partnership with the Departments of Energy, Homeland Security, and Defense. These investigations have been undertaken to examine the potential impacts on the U.S. electric power grid for severe geomagnetic storm events and EMP threats. In addition, this analysis was formative in the National Academy of Sciences "Severe Space Weather Events—Understanding Societal and Economic Impacts Workshop Report." These assessments indicate that severe geomagnetic storms have the potential to cause long-duration outages to widespread areas of the North American grid.

For these investigations, Metatech developed detailed new analysis using much more systematic forensic analysis and analytical simulation techniques to examine geomagnetic storms and how they impact the bulk power system. This has allowed for new perspectives to be developed on geomagnetic storms and the nature of how these storms may interact with the bulk power system.

Historic Events

Perhaps the most illustrative means of reviewing the threat posed by large geomagnetic storms is to briefly review the important impacts observed during previously observed geomagnetic activity.

Most well-known in North America is the March 13-14, 1989 geomagnetic storm. Among other impacts, this storm led to the collapse of the Hydro Québec system in the early morning hours of March 13, 1989. Starting at 2:44 AM (EST), operations on the Hydro Québec power grid were normal. At that time a large impulse in the Earth's geomagnetic field erupted along the U.S./Canada border (Figure 4). This started a chain of power system disturbance events that only 92 seconds later resulted in a collapse of the Québec Interconnection.⁴⁴ The rapid manifestation of the storm and impacts to the Québec power grid did not allow system operators sufficient time to fully assess the situation or meaningfully intervene. As described by Blais and Metsa of Hydro Québec:

Telluric currents induced by the storm created harmonic voltages and currents of considerable intensity on the La Grande network. Voltage asymmetry on the 735-kV network reached 15%. Within less than a minute, the seven La Grande network static var compensators on line tripped one after the other... With the loss of the last static var compensator, voltage dropped so drastically on the La Grande network (0.2 p.u.) that all five lines to Montréal tripped through loss of synchronism (virtual fault), and the entire network separated. The loss of 9,450 MW of generation provoked a very rapid drop in frequency at load-centre substations. Automatic underfrequency load-shedding controls functioned properly, but they are not designed for recovery from a generation loss equivalent to about half system load. The rest of the grid collapsed piece by piece in 25 seconds.⁴⁵

The bulk power system operated as designed to limit physical damage to equipment during the event. As a result, power was restored to 83 percent of the customers affected in Québec within nine hours of the system's collapse. However, two large generator step-up transformers were damaged due to overvoltage conditions. The outage was contained in the Québec Interconnection and the service of electricity to consumers in the remainder of North America was not affected. Though no additional widespread outages occurred as a direct result of the storm, roughly 200 significant anomalies were experienced across the bulk power system over the next 24 hours as the storm extended south into the New England, Mid-Atlantic, Midwest U.S., and Pacific Northwest.⁴⁶

⁴⁴ Denis Larose, "The Hydro-Quebec System Blackout of March 13, 1989", IEEE Special Publication 90TH0291-5 PWR, Effects of Solar-Geomagnetic Disturbances on Power Systems, 1989, pg. 10-13.

⁴⁵ Blais, G. and P. Metsa. *Operating the Hydro-Québec grid under magnetic storm conditions since the storm of March 13, 1989*, Proc. Solar-Terrestrial Predictions Workshop, Ottawa, May 18-22, 1992, ed. J. Hruska, M.A. Shea, D.F. Smart, G. Heckman, vol 1, 108-130, 1993.

⁴⁶ NERC Disturbance Analysis Working Group Report, The 1989 System Disturbances: March 13, 1989 Geomagnetic Disturbance, pages 8-9, 36-60, 1990.

During the March 1989 storm, large GIC's also caused damage to a large GSU transformer located at a nuclear plant in New Jersey.²³ This storm proved that individual transformers may be damaged from overheating due to this unusual mode of operation as described in the vulnerability section below, which can result in long-term outages of key transformers in the network.

Following the March 1989 storm, industry took a number of actions to improve its response to future storms. Hydro-Québec instituted a number of measures, including:

- Desensitization of the protection of Static Var Compensators (SVC) to amplification of the voltage wave asymmetry and harmonics;
- Even though this was not the primary objective, significant reduction of low frequency current flow (North - South) in the 735-kV lines during a GMD event with the addition of series compensation on the entire 735 kV network;
- Significant reduction of low frequency current flow (East - West, northern system) in the 735 kV lines during a GMD event with the addition of blocking capacitors in the neutral of the most vulnerable high power transformers;
- In southern Québec, installed an automatic load shedding scheme to counter slow voltage collapse in 2004. This scheme's primary objective is to respond in the event of the loss of multiple lines (extreme event), but could also respond to a voltage collapse due to a GMD event;
- 22 substations where 735 kV reactors are automatically switched out as a defense plan against rapid or slow voltage collapse;
- Put operating procedures in place to increase transmission system margin for high GMD forecasted conditions;
- Installed real-time asymmetry monitoring at several substations to complement K-index forecast.

The Northeast Power Coordinating Council (NPCC) also took measures to respond to GMD events. The group contracted with Solar Terrestrial Dispatch (STD) for a solar notification and communication system used by the five Reliability Coordinators in the region, called the Geomagnetic Storm Mitigation System (GSMS). An active communications software package installed on the system operator's console provides each of the NPCC Reliability Coordinators with geomagnetic storm alerts and the status of solar activity. Upon receipt of a geomagnetic storm alert of Kp 6 or higher, the GSMS simultaneously provides:

- Visual and / or audible alarms;
- A main screen providing the system operator with all information currently known about possible solar activity; and
- A dialog box permitting instantaneous communication among all NPCC Reliability Coordinators of any observed solar magnetic phenomenon.

Complementing the notification system, NPCC also established its Document C-15, “Procedures for Solar Magnetic Disturbances Which Affect Electric Power Systems,”⁴⁷ establishing protective measures which can be taken to minimize the vulnerability of the system to solar phenomenon. After reviewing the available data provided by the GSMS, the system operator may choose to enact one or more of the actions presented in Document C-15. Special operating procedures were also developed by a number of the other ISO’s, including PJM Interconnection.

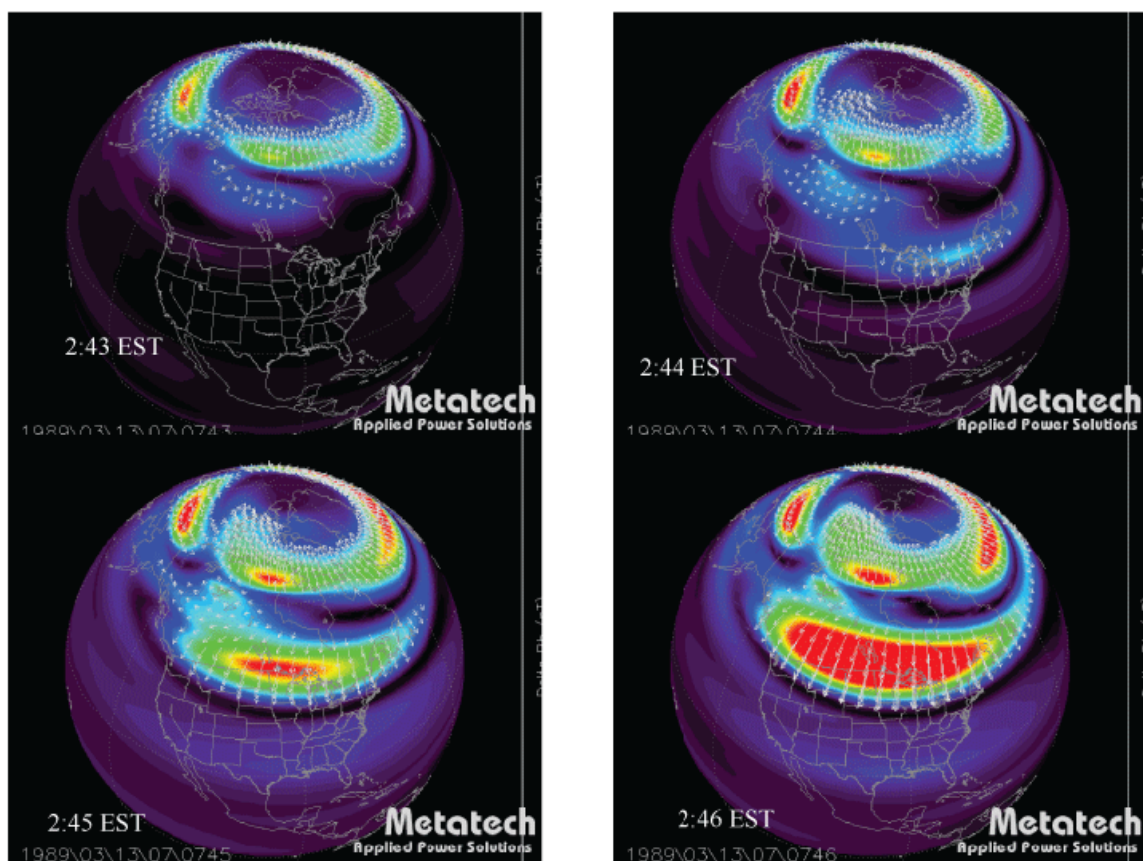


Figure 4: Rapid development of electrojet conditions over North America and principally along U.S./Canada border lead to Hydro Québec collapse and other reported problems in Minnesota, Manitoba and Ontario at these times. These images depict the ground level geomagnetic intensification over four minutes from 2:43 to 2:46 EST.

Large geomagnetic storms can have a global reach and produce impacts to other developed power grids around the world. For example in England, the March 1989 storm is suspected to have caused damage to two 400kV transformers. The operators of the power grid in England also understand that, since 1989, their power grid has become significantly more dependent on transmission system static var and switched capacitance devices for system voltage regulation,

⁴⁷ At: <http://www.npcc.org/viewDoc.aspx?name=c-15.pdf&cat=regStandProced>

thus making their system more vulnerable to future geomagnetic storms.⁴⁸ Even recent and much lower intensity storms, such as those in late October 2003, provide evidence of increasing vulnerability. A regional blackout in Southern Sweden, for example, and reports of high operating temperatures in transformers were reported due to storm intensity reaching ~300 nT/min.^{49 50} Even lower intensity, but long duration GIC disturbances in South Africa caused permanent damage and loss of 15 EHV transformers in the Eskom system during the October 2003 storms.⁵¹

Forensic Analysis

The ability to forensically examine the March 1989 storm has provided new perspectives on this storm and the rapid evolution of the geomagnetic disturbance environment that caused the Québec blackout and other impacts. For instance, Figure 4 provides a synoptic map of four minutes of the disturbance centered around the Québec collapse and illustrate the large footprint and rapid evolution that can occur in this threat environment.⁵² This analysis capability also provides the ability to perform comparative evaluations of this storm and many others.

One of the most useful means to describe geomagnetic storm intensity from a perspective of GIC flows in exposed power grids is to consider the rate-of-change of the disturbed geomagnetic field. GIC levels are primarily driven by an impulsive disturbance (the rate of change of the geomagnetic field or dB/dt in units of nT/min) of local geomagnetic fields, the higher the rate of change the higher the relative levels of GIC. Determining exact levels of GIC require extensive models of power grid and deep earth conditions. However, knowing impulsive geomagnetic disturbance levels across regions can allow empirical comparisons of the relative intensity of geomagnetic field disturbances and their inherent ability to cause large GIC flows and potential impacts to the bulk power system. For instance the impulsive disturbance intensity that triggered the Québec bulk power system collapse was ~500 nT/min at time 2:45 AM EST.²³

⁴⁸ I.A. Erinmez, J.G. Kappenman, W.A. Radasky, "Management of the Geomagnetically Induced Current Risks on the National Grid Company's Electric Power Transmission System", Journal of Atmospheric and Solar Terrestrial Physics (JASTP) Special Addition for NATO Space Weather Hazards Conference June, 2000.

⁴⁹ Pulkinen, et.al., "Geomagnetic storm of 29-31 October 2003: Geomagnetically induced currents and their relation to problems in the Swedish high-voltage power transmission system", SPACE WEATHER, VOL. 3, S08C03, doi:10.1029/2004SW000123, 2005

⁵⁰ J.G. Kappenman, "An overview of the impulsive geomagnetic field disturbances and power grid impacts associated with the violent Sun-Earth connection events of 29-31 October 2003 and a comparative evaluation with other contemporary storms", SPACE WEATHER, VOL. 3, doi:10.1029/2004SW000128, 2005

⁵¹ Makhosi, T., G. Coetzee, GENERATOR TRANSFORMER DAMAGE IN ESKOM NETWORK, EPRI Workshop on Transformers and Geomagnetic Currents, Washington DC, Sept 23, 2004.

⁵² J. G. Kappenman, Chapter 16 – "Geomagnetic Disturbances and Impacts Upon Power System Operations", The Electric Power Engineering Handbook, 2nd Edition, edited by Leonard L. Grigsby, CRC Press/IEEE Press, pages 16-1 through 16-22, published 2007.



Time (EST)	Area	Event	Time (EST)	Area	Event
1600	Atl. Elec.	MVAR	1658	WAPA	Line
1602	Va. Pwr.	Capacitor	1658	WKPL	Alarm
1610	PJM	Noise	1658	BPA	Capacitor
1615	PJM	Generator	1658	BPA	Transformer
1625	PJM	Oscillograph	1700	UPA	Voltage
1626	PJM	Oscillograph	1700	LILCO	Voltage
1630	SC Edison	Current	1700	IIGE	Voltage
1630	SC Edison	Current	1700	WEP	Noise
1630	SC Edison	Noise	1701	PJM	Capacitor
1640	PJM	Voltage	1701	NIMO	Capacitor
1644	PJM	Alarm	1701	Va. Pwr.	Capacitor
1644	PJM	Capacitor	1701	Va. Pwr.	Capacitor
1645	WPL	Voltage	1701	OH	Voltage
1649	PJM	Recorder	1701	OH	Oscillograph
1651	NIMO	Capacitor	1703	Va. Pwr.	Capacitor
1653	NIMO	Capacitor	1708	UPA	Capacitor
1654	PJM	Alarm	1709	WAPA	Converter
1655	Minn. Power	Voltage	1709	WAPA	Transformer
1655	Atl. Elec.	Voltage	1709	WAPA-Fargo	Voltage
1665	Atl. Elec.	MVAR	1709	WAPA	Line
1658	BC Hydro	Voltage	1709	WAPA	Relay
1658	OH	Demand	1711	NIMO	Capacitor
1658	WAPA	Converter	1720	UPA	Voltage
1658	BPA	Noise	1723	Va. Pwr.	Capacitor

Figure 5: Reported North American power system impacts, March 13, 1989 time 16:00-17:23 EST (21:00-22:23 UT)

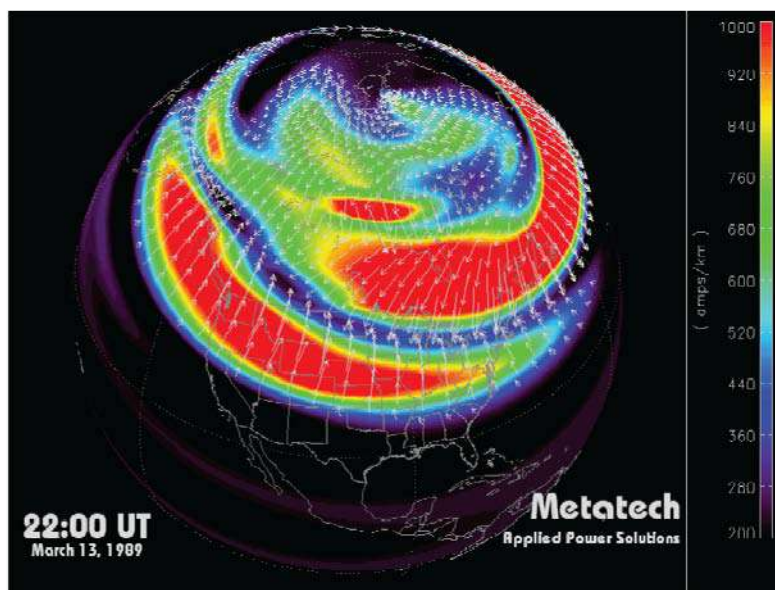


Figure 6: Synoptic map of geomagnetic field disturbance conditions at 22:00UT (17:00EST), March 13, 1989

This ~500 nT/min disturbance level provides a useful threshold for analysis. Over the course of March 13-14, 1989 storm, impulsive disturbance levels of 300 to 500 nT/min were observed as far south as Bay St. Louis, Mississippi on the Gulf of Mexico and from Colorado to Washington state. As the storm re-intensified at this time, it became larger in geographic footprint and expanded down to mid-latitude regions of North America. Storm activity over the time interval of 16:00-17:23 EST produced some of the largest and most widespread impacts observed across the bulk power system (Figure 5). Figure 6 provides a synoptic map of the geomagnetic field disturbance conditions at 17:00 EST (22:00UT) on March 13, 1989 that triggered many of the power system impacts during this intense substorm.

Using the traditional NOAA geomagnetic storm indices, the March 1989 storm was ranked as the third largest storm of all time (since rankings started in 1932), lagging the next two larger storms by just a few percentage points using this scale.⁵³ Until recently, many in the electric sector and scientific community therefore believed this storm was representative of the worst-case threat that could be posed by geomagnetic storms to North America.

Recent and more systematic analysis of impulsive disturbances that cause large GIC flows has allowed re-examination of the March 1989 storm and other historical storms. This analysis of both contemporary and historic storm data and records indicates dB/dt impulsive disturbances larger than 2000 nT/min have been observed on at least three occasions since 1972 at latitudes of concern for the North American bulk power system. This is an intensity roughly four times

⁵³ Kappenman, J. G. An overview of the impulsive geomagnetic field disturbances and power grid impacts associated with the violent Sun-Earth connection events of 29–31 October 2003 and a comparative evaluation with other contemporary storms, *Space Weather*, 3, S08C01, doi:10.1029/2004SW000128. 2005.

larger than the levels experienced in March 1989. In extreme scenarios, available data suggests that disturbance levels as high as 5000 nT/min may have occurred during the geomagnetic storm of May 1921, an intensity roughly 10 times larger than the disturbance levels observed in 1989.⁵⁴ Were a storm to occur with these intensity levels, it is reasonable to expect that the bulk power system would experience major impacts.

Vulnerability

Designing for robust and resilient performance of the bulk power system in the face of familiar and well-understood threats has been an important emphasis of the electric sector since its inception. As a result, the system is highly reliable and resilient to the more familiar design threats such as equipment failure, human error, severe wind, lightning and ice loading exposures.

Geomagnetic Storms are unlike terrestrial weather threats to the power grid. These storms not only can develop rapidly but also have continental footprints that can result in widespread, simultaneous impact to many points on the system. The system is not designed to operate through the simultaneous loss of many key assets and such an impact could quickly bring the system outside the protection provided by traditional planning and operating reliability criteria, resulting in potential system instability and, in some cases, widespread disturbances and outages.

In view of the new awareness of the possible extremes of the geomagnetic storm environment, a new look and perspective on the role of the design and operation of the bulk power system with respect to these threats should be considered. Recent analysis has shown that both the manner in which systems are operated and the accumulated design decisions engineered into present-day networks around the world have tended to significantly enhance vulnerability and exposure to effects of a severe geomagnetic storm and the very similar threat environment caused by E3 (or slow pulse portion) of the High-Altitude Electromagnetic Pulse (HEMP) threat.⁵⁵

⁵⁴ Kappenman, J. G. Great Geomagnetic Storms and Extreme Impulsive Geomagnetic Field Disturbance Events – An Analysis of Observational Evidence including the Great Storm of May 1921, *Advances in Space Research*, Volume 38, Issue 2, 2006, Pages 188-199,

⁵⁵ Kappenman, J.G. “Electric Power Grids and Evolving Vulnerability to Space Weather”, feature article for AGU International Journal of Space Weather, 2, S01004, doi:10.1029/2003SW000028.

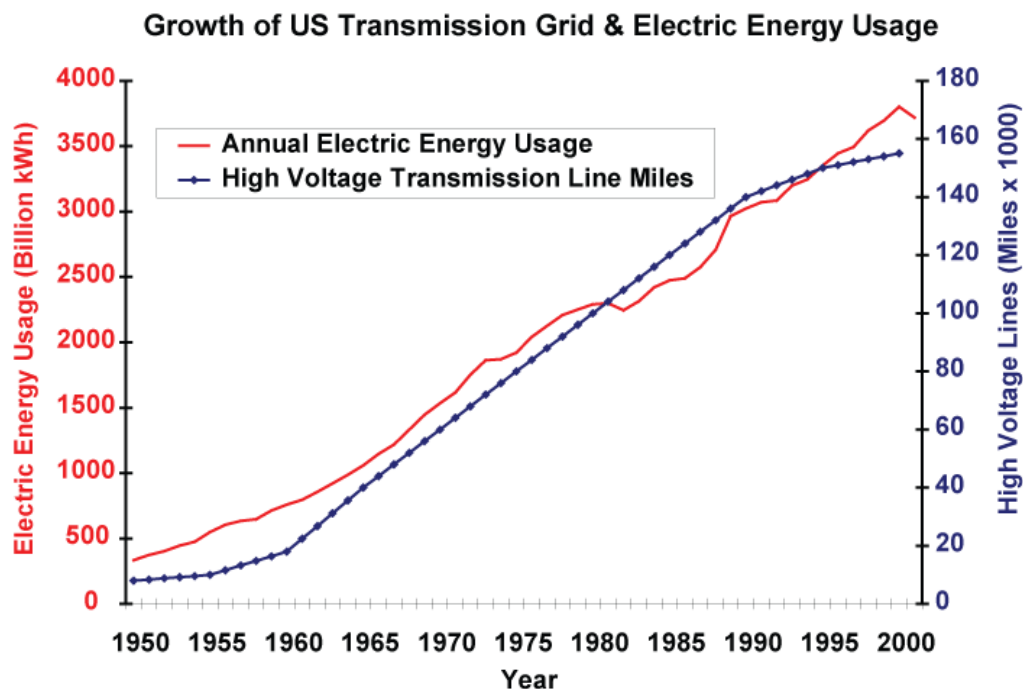


Figure 7: Growth of the High Voltage Transmission Network and annual electric energy usage in the United States over the past 50 years. In addition to increasing total network size, the network has grown in complexity with introduction of higher kV-rated lines that tend to carry larger GIC flows. (Data from NERC and U.S. DOE-EIA)

The demand for electricity in North America has grown dramatically over the past 50 years. To support these energy demands, the EHV infrastructure has grown as well, as shown in Figure 7. The high-voltage transmission grid presents a complex network topology that couples almost like an antenna through multiple ground points to the geo-electric field produced by disturbances in the geomagnetic field. From Solar Cycle 19 in the late 1950's through Solar Cycle 22 in the early 1980's, the high-voltage transmission grid and annual energy usage grew nearly tenfold. In short, the antenna that is sensitive to impulsive geomagnetic disturbances is now very large. This issue is not unique to North America: similar development rates of transmission infrastructure have occurred simultaneously in other developed regions of the world. This antenna effect is but one of many design and cost factors that must be considered when adding transmission to the bulk power system.

As the bulk power system has grown in size, it has also grown in complexity, which has further compounded risks due to geomagnetic disturbances. Some of the more important system changes that can increase impacts from GIC events include higher design voltages and the behavior of transformers as voltage ratings increase. The operating levels of high-voltage networks have increased from the 100-200 kV design thresholds of the 1950's to the 345 to 765 kV extra-high-voltage levels of today's networks. As a result, the ratio of resistances varies significantly with voltage class, as the resistance is approximately 10 times lower for the 765 kV

than for the 115 kV lines (Figure 8). In general, the higher the voltage rating, the lower the resistive impedance per unit distance (in ohms per km), which will in turn produce ~10 times larger GIC flows in the 765kV elements for the same geomagnetic disturbance environments.

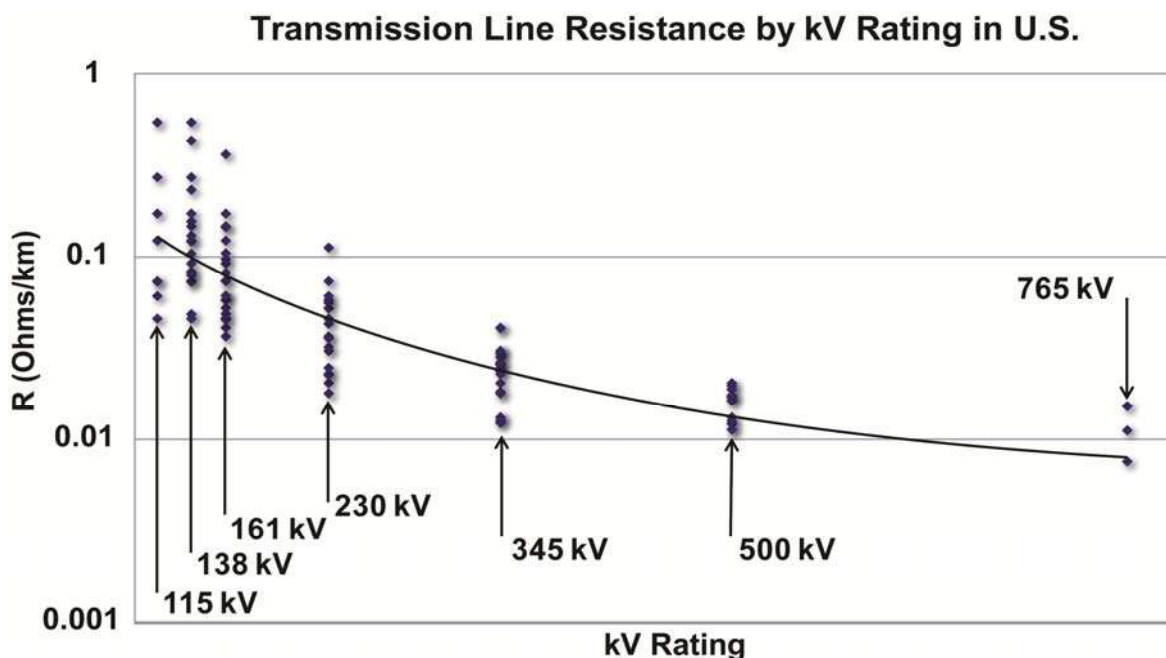


Figure 8: Range of transmission line resistance for the major kV-Rating classes for transmission lines in the U.S. electric power grid infrastructure population. Also shown is a trend line of resistance weighted to population averages. The lower R for the higher voltage lines will also cause proportionately larger GIC flows in this portion of the power grid. (Derived from data in EHV Transmission Line Reference Book and from U.S. DOE-Energy Information Agency and FERC Form 1 Database)

In combination, these design attributes will tend to collect and concentrate GIC flows in the higher kV-rated portions of the bulk power system. Were a large enough storm to occur, it could result in the simultaneous loss of multiple major transmission lines, which could cause widespread outages. Operational procedures to reduce loading on heavily loaded lines and more evenly distribute the flow of power across the system during a GMD event have been developed in many regions and may provide some mitigation to this issue.

The design of transformers also acts to further compound the impacts of GIC flows in the high-voltage portion of the power grid. While proportionately larger GIC flows occur in these large high-voltage transformers, saturation of EHV transformers occurs at the same level of GIC current as those of lower-voltage transformers. Transformers experience excessive levels of internal heating brought on by stray flux when GICs cause the transformer's magnetic core to saturate and spill flux outside the normal core steel magnetic circuit. Previous well-documented cases have noted heating failures that caused melting and burn-through of large-amperage copper windings and leads in these transformers (Figure 9). These transformers generally cannot be repaired in the field, and if damaged in this manner, need to be replaced with new units, which have manufacture lead times of 12–24 months or more in the world market. In addition, each

transformer design (even from the same manufacturer) can contain numerous subtle design variations. These variations complicate the calculation of how and at what density the stray flux can impinge on internal structures in the transformer. Therefore the ability to assess existing transformer vulnerability or even to design new transformers to be tolerant of saturated operation is not readily achievable.



Figure 9: This is a picture of the Salem New Jersey Nuclear Plant GSU Transformer (~1200mVA, 500/22kV single phase transformer) and permanent damage caused by the March 13, 1989 Geomagnetic Storm. Photos courtesy of PSE&G.

Another compounding of risk occurs as these higher voltage transformers produce proportionately higher power system impacts than comparable lower-voltage transformers. Because reactive power loss in a transformer is a function of the operating voltage, proportionately higher reactive power losses will occur in the higher voltage transformers due to GIC. For example, a 765 kV transformer will have approximately six times larger reactive power losses for the same magnitude of GIC flow than a 115 kV transformer (Figure 10).

Severe GMD events can also cause harmonic currents on the system, which, in turn, cause over-current relays to trip capacitor banks because capacitors offer a lower impedance path for harmonics. Protection systems can and have operated in direct response to harmonic currents. Therefore, when shunt capacitor and static var compensators trip for over-current protection due to harmonics, it exacerbates system voltage regulation issues caused by the GIC-related increases in transformer reactive power losses.

A distorted sinusoidal waveform can also cause HVDC converter commutation failures.⁵⁶ System frequency can become erratic, and generators, which are not immune to harmonic

⁵⁶ N. Mohan, V. D. Albertson, T. J. Speak, J. G. Kappenman, M. P. Bahrman, "Effects of Geomagnetically-Induced Currents on HVDC Converter Operations," IEEE PAS Transactions, Vol. PAS-101, November 1982, pp. 4413-4418.

currents, can be tripped by negative sequence protection systems. Units that do not trip are susceptible to damage from torsional stress or rotor heating.

These effects can occur near simultaneously over a large geographic area, resulting in a multiple-contingency outage that has the potential to cascade across the system.

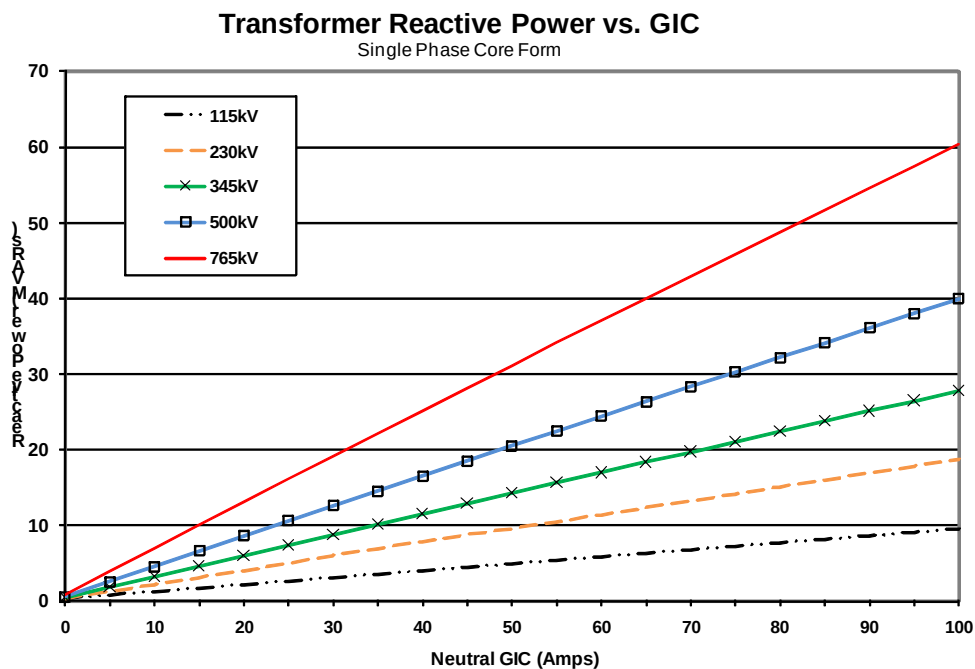


Figure 10: Larger GIC flows will tend to occur in the higher kV-Rated transformers. As shown above these transformers also produce proportionately larger reactive power consumption on the grid compared to the same level of GIC flow in lower kV-Rated transformers.⁵⁷

Aspects of operation of the bulk power system can also add to the vulnerability of this infrastructure to geomagnetic field disturbances. As the application of digital controls has increased the efficiency of the network over the past twenty years, the electric sector has been able to reduce excess capacity needed to ensure reliable operations, often resulting in significant cost-savings to consumers. Heavier loading of key transmission lines to facilitate the transfer of power between demand centers and key generation assets does not generally result in reliability impacts, but could potentially complicate response procedures to a sudden or un-announced geomagnetic disturbance.

After March 1989, the electric sector put procedures in place to operate the system in a conservative state with sufficient advanced notice of a geomagnetic disturbance. These plans are discussed further in the mitigations portion of this section and have been largely effective at

⁵⁷ Image courtesy of Storm Analysis Consultants.

avoiding widespread blackouts to the system during the smaller and lower intensity GMD events which have occurred since 1989. These procedures were not designed for the extreme levels of disturbance that are now being considered.

This highlights the importance of ensuring that proper forecasting, monitoring, and measurement tools are available to industry. Present limitations to these systems should be improved. The most familiar means of characterizing the severity of geomagnetic storms is the K-Index. Dating back to 1932, it is one of the oldest of geomagnetic storm classification indices. This index varies over a range from 0 (minimal or no geomagnetic disturbance) to 9 (highest class of geomagnetic disturbance) in threshold steps. This index was derived in an era of paper charts used for recording geomagnetic disturbances at remote observatories and with minimal data communication capability. This approach allowed a simple numerical classification to be collected from multiple observatories to describe not only the local variation in the geomagnetic field but also to develop a global sense of the severity of the storms. NOAA and other agencies around the world primarily focus their geomagnetic storm forecast and alert products on the K-Index.

The design and use of the K-Index has limitations in its application, some of the most important of which are summarized as follows:

- The index saturates at K9 at a low threshold and is not able to indicate levels of severity and intensity that would be important to power system operators. Therefore it blurs intensity and is unable to communicate the extremes of the storm environment.
- The index is only determined once in each 3 hour time block (e.g., eight times per day). Therefore, it also blurs the time-specific details of impulsive disturbances and does not provide sufficiently granular time information to power system operators.
- At U.S. latitudes, the K9 threshold is reached at only a minimum 500 nT variation over a three hour window. This means for slow variations, the dB/dt could be as low as three nT/min, while for very fast and intense variations, the dB/dt is infinite. Therefore the K9 intensity in terms of dB/dt is highly ambiguous.
- The K-Index also cannot be reverse engineered to derive dB/dt from prior storms, therefore it has limited forensic value to provide meaningful comparisons with older storms.

The K-Index is subject to saturation and widening dB/dt ambiguity at high K levels. It is only a reliable indicator of less-severe geomagnetic disturbance levels and periods of very low dB/dt and essentially no GIC. In contrast, the K-Index becomes increasingly ambiguous with respect to the GIC or dB/dt threat as the storm increases in intensity. Additional clarity and granularity of information about these threat levels in intense environments will be vital to improving situational awareness by infrastructure operators that are concerned about GIC.

When evaluating the design and performance of power systems, the design challenge is one of countering the severe threats and, for these purposes, a clear definition of the maximum threat environments cannot be readily derived from any historical K-indices. The rate of change of B (or dB/dt in at least a cadence of nT/min) is a reliable proxy for GIC, in that, all other things

being equal, the larger the absolute value of the dB/dt the larger the relative levels of GIC. The K-Index cannot be reliably tracked to dB/dt , especially for intense storm levels.

Consequence

Contemporary models of large power grids and the electromagnetic coupling to these infrastructures by the GMD environment have matured to a level in which it is possible to achieve accurate benchmarking of geomagnetic storm observations and the resulting GIC.^{58 59 60} These efforts have allowed additional insights into the potential impacts to today's infrastructure that could result from large historically-observed events.

Depending on the location and pattern of the geomagnetic disturbance, there are a number of plausible consequential outcomes for a severe geomagnetic storm of a strength roughly ten times what was observed in 1989. Metatech conducted a simulation based on a 4800 nT/min disturbance, shown in Figure 11 which calculated the pattern of GIC flows in the U.S. power grid and the boundaries of regions of power grid that could be subject to progressive collapse, such as what occurred to the Québec Interconnection in March 1989. The simulation results indicate that more than a thousand EHV transformers will have sufficient GIC levels to simultaneously be driven into saturation. Further, this would suddenly impose an increase of over 100,000 MVARs of reactive demand on the system, a scenario that could trigger a widespread voltage collapse, resulting in system instability and, likely, a short-duration blackout.⁶¹

The analysis also indicates that the GIC in over 350 transformers will exceed levels where the transformer is at risk of irreparable damage. Figure 12 provides an estimate of "Percent Loss" of EHV transformation capacity by state for the same 4800 nT/min threat environment. Such large-scale damage could lead to prolonged restoration and long-term chronic shortages of electricity supply capability to the impacted regions, arguably for multiple years.

While the electric sector has performed reliably through all K9 storms since the March 1989 by using specialized geomagnetic storm operating procedures, all these storms were much lower in dB/dt intensity than the March 1989 storm. The storms of concern could potentially be four to ten times more intense than March 1989 and could entail the potential for widespread damage to EHV transformers and other key assets of unprecedented proportions.

⁵⁸ J.G. Kappenman, L.J. Zanetti, W.A. Radasky, "Geomagnetic Storms can Threaten Electric Power Grid", *Earth in Space*, American Geophysics Union, Vol. 9, No. 7, pp. 9-11, March 1997.

⁵⁹ J.G. Kappenman, W.A. Radasky, J.L. Gilbert, I.A. Erinmez, "Advanced Geomagnetic Storm Forecasting: A Risk Management Tool for Electric Power Operations", *IEEE Plasma Society Special Issue on Space Plasmas*, December 2000, Vol 28, #6, pages 2114-2121.

⁶⁰ J.G. Kappenman, "Advanced Geomagnetic Storm Forecasting for the Electric Power Industry", *American Geophysics Union Press Book "Space Weather" Geophysical Monograph #125*, July 2001, pages 353-358.

⁶¹ J. G. Kappenman, Chapter 16 – "Geomagnetic Disturbances and Impacts Upon Power System Operations", *The Electric Power Engineering Handbook*, 2nd Edition, edited by Leonard L. Grigsby, CRC Press/IEEE Press, pages 16-1 through 16-22, published 2007.

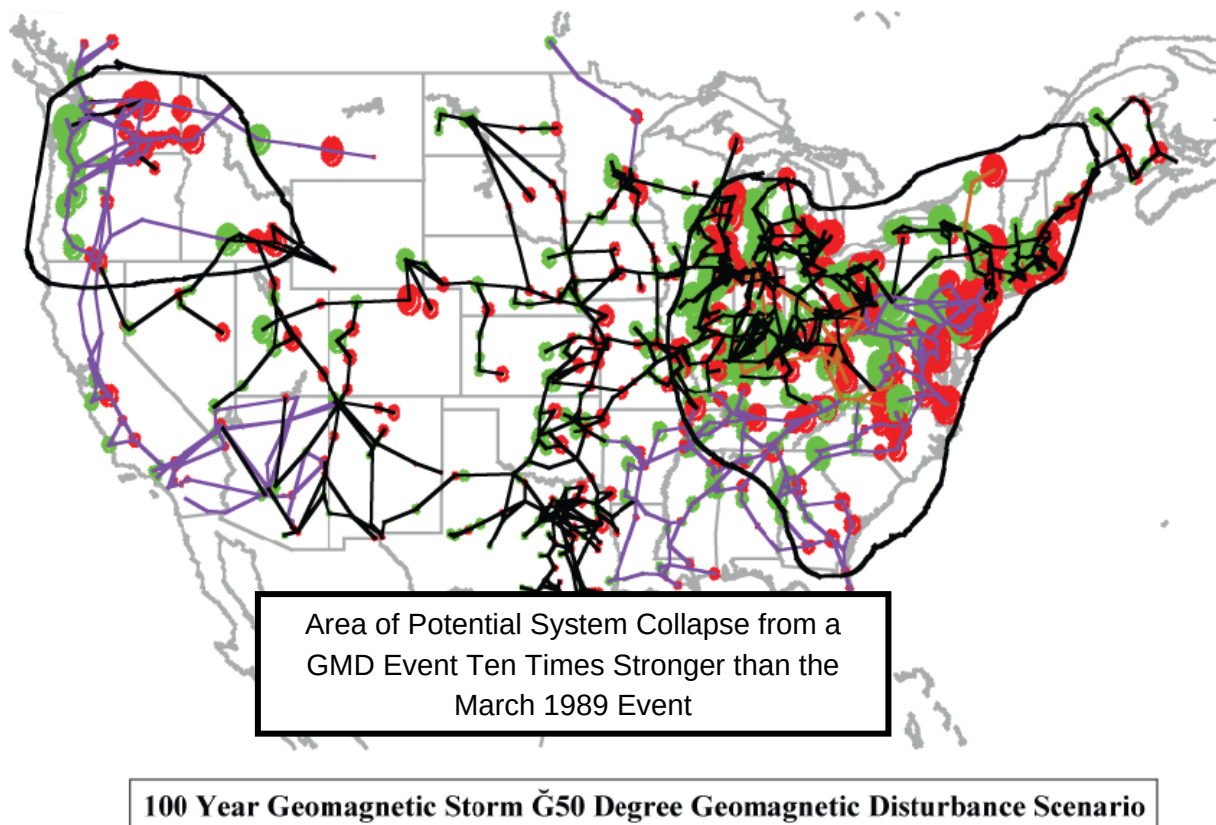


Figure 11: The simulation results showing the pattern of GIC flows in the U.S. grid for a 4800 nT/min geomagnetic field disturbance at 50° geomagnetic latitude. The above regions outlined are susceptible to system collapse due to the effects of the GIC⁶²

⁶² Image provided courtesy of Storm Analysis Consultants.

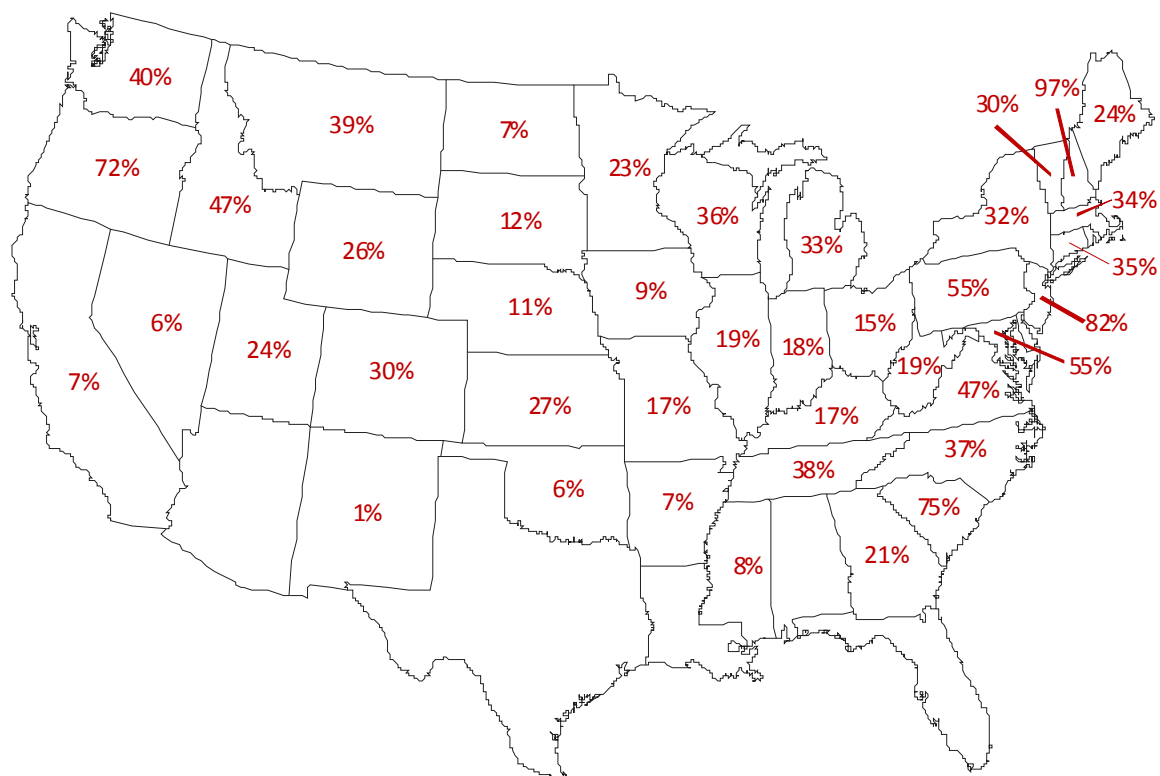


Figure 12: A map showing the At-Risk EHV Transformer Capacity by State for this disturbance scenario, regions with high percentages could experience long duration outages that could extend multiple years.⁶³

⁶³ Image provided courtesy of Storm Analysis Consultants.

High Altitude Electromagnetic Pulse (HEMP)

Threat

A high-altitude electromagnetic pulse (HEMP) is defined as a series of electromagnetic waveforms that are generated from a nuclear detonation at altitudes above 30 km and propagate to the Earth's surface. While the existence of HEMP has been known since the early 1960's, improvements in the understanding of HEMP and increases in the susceptibility of electronics to HEMP have raised new issues for commercial equipment and systems that are part of the civil infrastructure. In addition, two important reports by the Congressionally-appointed EMP Commission were published in 2004⁶⁴ and 2008⁶⁵, clearly indicating that the U.S. infrastructure is vulnerable to a single high-altitude nuclear burst.

While it is extremely challenging to place a probability on the occurrence of such a deliberate attack on the North American continent, military thought places the continent at greater risk for such an attack today than in the past. As the military landscape has changed from nation-state threats to a greater concern over terrorist and rogue-nation threats, the risk for the use of weapons of mass destruction (such as a EMP weapons) has increased. Adversaries are more likely to resort to asymmetric means, using unconventional approaches that avoid or undermine North America's strengths and instead exploit vulnerabilities. This means that the future target of HEMP may well be the civil infrastructure of the United States as opposed to military systems, which have considered the HEMP threat for many years.

The term "EMP" has been used since the late 1960s to describe the electromagnetic pulse generated by a nuclear detonation at any altitude. To discriminate between different types of EMP, additional acronyms were defined such as HEMP (high-altitude EMP), SREMP (source region EMP: for the EMP very near a surface or air burst where radiation is also present), SGEMP (system-generated EMP: for the EMP generated when x-rays strike a satellite or missile in space) and so on. It is therefore important to use the term HEMP when referring to the EM fields produced by a nuclear burst in space and affecting systems on the Earth.

High-Altitude Nuclear Tests in 1962

On the evening of July 9, 1962 the U.S. performed a high-altitude nuclear test known as Starfish; it was publicized in advance and was observed by the public in Honolulu, Hawaii. The U.S. government indicated that the device had a yield of 1.4 MT and was detonated at an altitude of 400 km at a distance of approximately 1400 km from Hawaii. While there were no noticeable direct impacts to individuals on the ground (no blast, shock, radiation, etc.) some electrical

⁶⁴ "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack," Vol. I: Executive Report, 7 April 2004. <http://www.empcommission.org>

⁶⁵ "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures," April 2008.

systems were still affected by the electromagnetic fields. Reports included the facts that some streetlights were extinguished, microwave communications were disrupted, and burglar alarms had sounded. While these system effects were not very dramatic in 1962, the level of technology used in electronic equipment has changed significantly since: from analog to digital, with operating frequencies increasing from megahertz to gigahertz, and with the operating voltages of chips reaching ever lower levels. These changes have increased the potential of malfunction of present-day commercial equipment during a HEMP event.

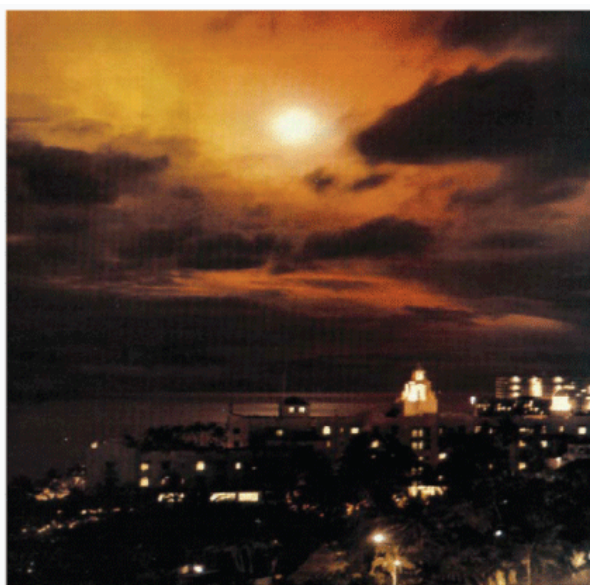


Figure 13. Photograph of the Starfish explosion from Honolulu on the evening of July 9, 1962.⁶⁶ Widespread red air glow (6300 Å) amid dark clouds, caused mostly by x-ray-excited atomic oxygen (i.e., oxygen by photoelectrons liberated by Starfish X-rays). The moon is shown in the center of the sky.

Later in October 1962, the Soviet Union performed a series of three high-altitude nuclear tests over Kazakhstan. In these tests many more impacts were noted in electrical systems including physical damage to power line insulators, outages of long communications lines (both buried and above-ground), damage to diesel power systems, and impacts on radar systems.⁶⁷ As the Soviet tests were performed over land, electrical systems were more directly exposed. Russian scientists indicated that, in nearly all situations, the observed system impacts were due to the interaction of the HEMP fields with long metallic lines (on the order of 100 meters or longer), which then conducted disabling transient voltages and currents into the affected systems. Later

⁶⁶ *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*. Volume 1: Executive Report. Commission to Assess the Threat to the United States from an EMP Attack. Washington, DC. April 2008. http://www.empcommission.org/docs/empc_exec_rpt.pdf

⁶⁷ V.M. Loborev, "Up to Date State of the NEMP Problems and Topical Research Directions," *Electromagnetic Environments and Consequences: Proceedings of the EUROEM 94 International Symposium*, Bordeaux, France, 30 May – 3 June 1994, pp. 15-21.

work by Russian scientists examining the specific outages of one communication line⁶⁸ provided a clear indication that these outages were due to the late-time HEMP, which lasts for tens of seconds after the detonation.

HEMP Time Waveform

HEMP is not described as a single pulse, but rather as a series of waveforms covering times from nanoseconds to hundreds of seconds. After years of research it has been determined that three main waveforms are generated due to different nuclear generation and atmospheric mechanisms (see Figure 14). The detailed description of the mechanisms is beyond the scope of this report, but more information can be found in the references below.^{69 70}

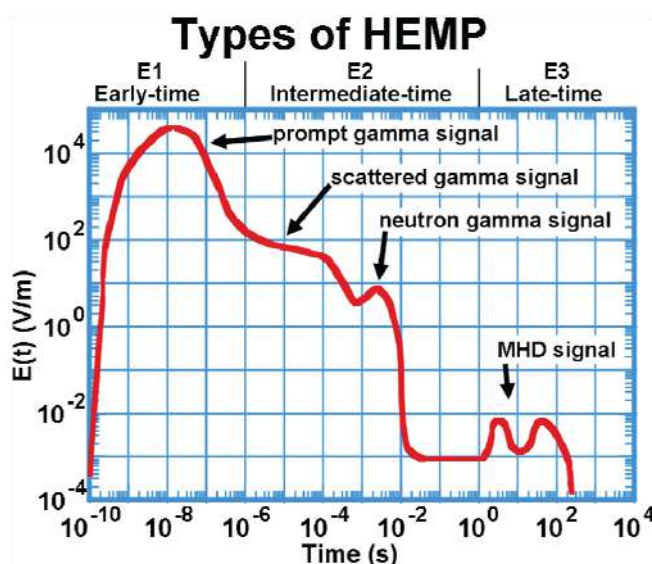


Figure 14: The various generation mechanisms for the HEMP environment.

Figure 15 illustrates the three main waveforms of interest as defined analytically by the IEC.⁷¹ The early-time waveform is referred to in the figure as E1, the intermediate-time waveform is referred to as E2 and the late-time waveform is known as E3. The pulse widths of these three waveforms are ~ 100 ns, 1 ms, and 10s of seconds, respectively. The peak values shown in Figure 15 are 50 kV/m, 100 V/m, and 40 V/km, respectively. An important feature of this

⁶⁸ Greetsai, V.N., A.H. Kozlovsky, M. M. Kuvshinnikov, V.M. Loborev, Yu. V. Parfenov, O.A. Tarasov, L.N. Zdoukhov, "Response of Long Lines to Nuclear High-Altitude Electromagnetic Pulse (HEMP)," IEEE Transactions on EMC, Vol. 40, No. 4, November 1998, pp. 348-354.

⁶⁹ Radasky, W. A., "High-altitude EMP (HEMP) Environments and Effects," NBC Report, Spring/Summer 2002, pp. 24-29.

⁷⁰ Radasky, W. A., J. Kappenman and R. Pfeffer, "Nuclear and Space Weather Effects on the Electric Power Infrastructure," NBC Report, Fall/Winter 2001, pp. 37-42.

⁷¹ IEC 61000-2-9, "Electromagnetic Compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP Environment – Radiated Disturbance," International Electrotechnical Commission, Geneva, Switzerland, February 1996.

waveform is that it can expose a very large area of the Earth (on the order of several million square kilometers) simultaneously, as it propagates at the speed of light. This creates a special hazard for large area networks such as the bulk power system which are, at a minimum, designed to withstand a series of single point failures as long as each failure is recognized in turn. For example, a single high-altitude burst over the U.S., assuming it was not defended by the U.S. military, could expose the entire electrical grid east of the Mississippi River to a severe HEMP transient within one power cycle.

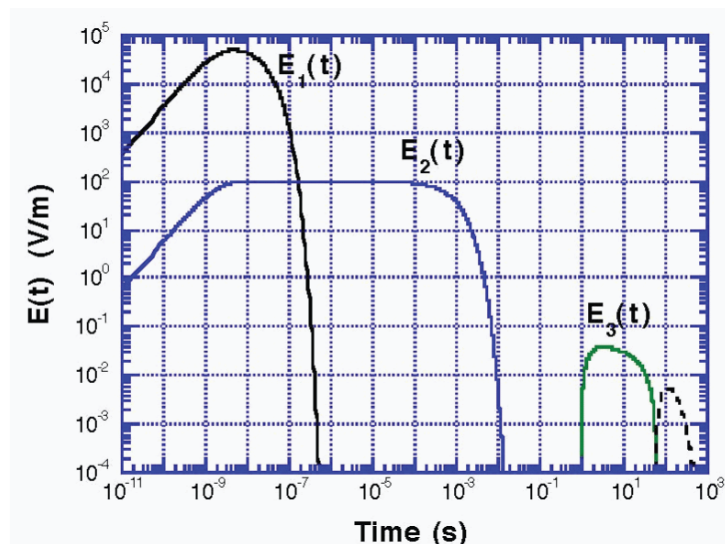


Figure 15: Three portions of the HEMP electric field waveform in volts/meter from IEC 61000-2-9 [41].

While the electromagnetic field waveform is a direct threat to some electronic systems, it is clear that the E2 and E3 waveforms are only of concern for systems connected to very long lines (hundreds of meters to hundreds of kilometers) due to the electromagnetic wavelengths involved. While E2 HEMP may not be a threat by itself, it is possible that since it follows immediately after E1 HEMP, that there could be some additional failures (e.g., surge arresters) due to the E2 HEMP. Additional research may resolve this issue as it is not conclusive at this time.

The early-time E1 HEMP waveform is somewhat different in that it can directly penetrate through apertures in the external case of equipment, such as a computer, and induce significant currents and voltages at the circuit board level. These voltages can create malfunctions in the operation of the equipment and may cause damage depending on the shielding effectiveness of the equipment case. The early-time E1 HEMP waveform also couples efficiently to short lines (1-10 meters) connected to equipment (power, signal lines, etc.) and can induce large voltages and currents that can be conducted to the inside of the equipment. Laboratory E1 HEMP experiments for unhardened (to HEMP) commercial equipment indicate that the coupling to these short lines is the major threat to most commercial equipment. It is also noted that the E1 HEMP can also couple efficiently to overhead power lines producing high currents and voltages that can be a concern to distribution line insulators and transformers.

Natural EM Equivalents to HEMP and Power Grid Concerns

There are natural electromagnetic equivalents to the three HEMP waveforms. For the E1 waveform, its electromagnetic field is very similar to the field generated close to an electrostatic discharge.⁷² The electrostatic discharge field can reach ~10 kV/m at a distance of 10 cm from an arc. It also has a rise time of 0.7 ns and a pulse width of 30 ns. For conducted transients that are naturally observed, most electronic equipment is exposed to the electrical fast transient waveform⁷³ that is generated in electrical substations and propagates to factories and homes through the power network. These electrical fast transient waveforms can reach peak levels of ~4 kV and have a 5 ns rise time and a 50 ns pulse width at the locations of electronic equipment.

To compare to the E2 waveform, the electromagnetic field produced by a lightning ground return stroke is similar in waveshape and can reach levels of 100 kV/m very close (~50 meters) to the stroke, but these fields decrease rapidly with distance from the stroke. The pulse widths of these fields extend from 100 microseconds to as long as 1 millisecond for positive lightning strokes. The E2 fields from HEMP are much lower (~100 V/m), but do not vary significantly with distance. It is unlikely that the E2 fields could be a problem for power lines as the induced voltages are not expected to be very high.

To compare to the E3 HEMP waveform, the fields created by a geomagnetic storm last from a few to hundreds of seconds.⁷⁴ It is known that a large geomagnetic storm can produce electric fields greater than 1 V/km, and levels such as these have caused a regional power grid blackout as experienced in Québec on March 13, 1989.

Given that the three HEMP waveforms have natural disturbance equivalents, it appears that the E1 and E3 HEMP waveform peak values are likely to be larger in magnitude than the natural exposure levels. This is a concern, because it is known from high-frequency electromagnetic compatibility standardized testing that electronic equipment, such as protective relays, remote terminal units, MTUs and communications equipment usually requires some protection to survive the electrostatic discharge and electrical fast transient threats. These electromagnetic compatibility test levels are, however, much lower than the levels produced by E1 HEMP. As discussed above, power grids could collapse due to the occurrence of a severe geomagnetic storm, which produces electric fields with similar waveshapes and area coverage as E3 HEMP; however, the E3 HEMP is likely to have a higher peak field level.

⁷² IEC 61000-4-2, “Electromagnetic Compatibility (EMC) – Part 4: Testing and Measurement Techniques – Section 2: Electrostatic Discharge Immunity Test,” International Electrotechnical Commission, Geneva, Switzerland, April 2001.

⁷³ IEC 61000-4-4, “Electromagnetic Compatibility (EMC) – Part 4-4: Testing and Measurement Techniques – Electrical Fast Transient/Burst Immunity Test,” International Electrotechnical Commission, Geneva, Switzerland, April 2007.

⁷⁴ J. G. Kappenman, W. A. Radasky, J. L. Gilbert, I. A. Erinmez, “Advanced Geomagnetic Storm Forecasting: A Risk Management Tool for Electric Power Operations,” IEEE Plasma Society Special Issue on Space Plasmas, December 2000, Vol. 28, No. 6, pp. 2114-2121.

Vulnerability

E1 HEMP

As part of the EMP Commission activities, a large number of test and analysis studies dealing with the U.S. power grid determined that there are four main areas of concern with respect to HEMP:

1. High voltage substation controls and communications
2. Power generation and control room computers and communications
3. Distribution line insulators
4. Distribution transformers

The primary pathway for the E1 HEMP to reach the electronic equipment that control the operation of the grid is through the coupling of the E1 HEMP fields to cables and wiring, producing conducted transients that can exceed the withstand capability of the connected electronics. In addition, the distribution line insulators and transformers connect to the above-ground electric wires and are thus also influenced by the coupled E1 HEMP fields.

High-Voltage Substation Controls and Communications

High-voltage power substations are especially at risk as many operate without on-site personnel. Many substations will be exposed simultaneously (within one power cycle) to high-frequency electromagnetic fields from a single high-altitude nuclear burst as shown in Figures 16 and 17.

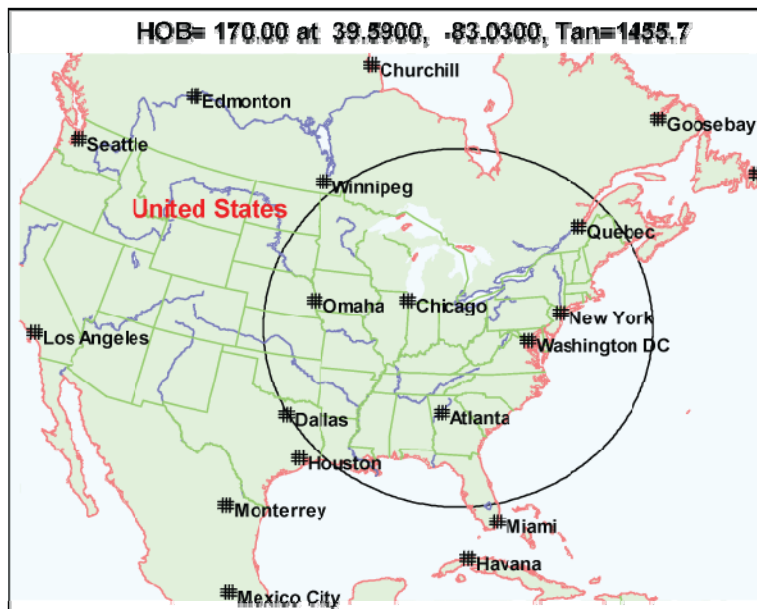


Figure 16: Exposure area for E1 HEMP burst at 170 km over Ohio.⁷⁵

⁷⁵ Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume 1: Executive Report. Commission to Assess the Threat to the United States from an EMP Attack. Washington, DC. April 2008. http://www.empcommission.org/docs/empc_exec_rpt.pdf

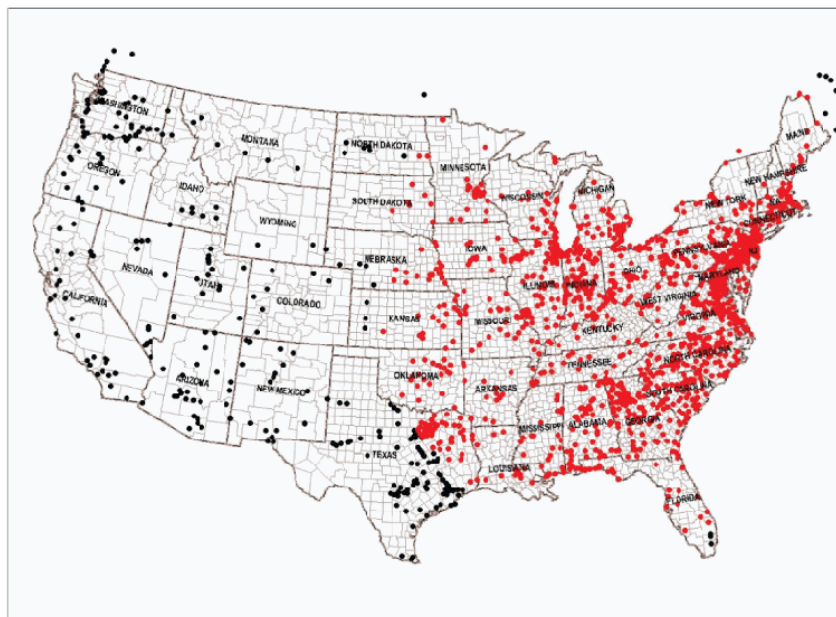


Figure 17: 1765 EHV substations at 345 kV and higher (83%) exposed by the burst in Figure 16.⁷⁶

The most significant E1 HEMP concern within a high-voltage substation is not the high-voltage transmission lines and transformers, but rather the low-voltage sensor and control lines that extend from the transformer yard to the relays and other control electronics in the control building. When these cables are in metallic conduits above ground, these conduits are not effective electromagnetic shields at high frequencies. Currents and voltages coupled to an external conduit are likely to leak into the internal cables at the joints and at connection points to sensors and the controls. These sensor and control cables run back to the control building in underground trays that also are not well shielded in many cases and could allow significant E1 HEMP pickup on the cables themselves.

E1 HEMP currents on the cables will propagate into the control buildings and may propagate further to protective relay and other equipment. Figure 18 shows the grounding process inside the control building where control cables have insulation stripped back and the shields are connected to ground cables. It is noted that the ground cables are on the order of 30 cm long (or longer), which provides a high impedance at high frequencies. While sufficient for lightning frequencies (typically below 1 MHz), this will enable a significant portion of the high-frequency E1 HEMP transients to continue to propagate on the signal wires inside the control facility instead of being directed to ground.

⁷⁶ Source: Metatech Corp.

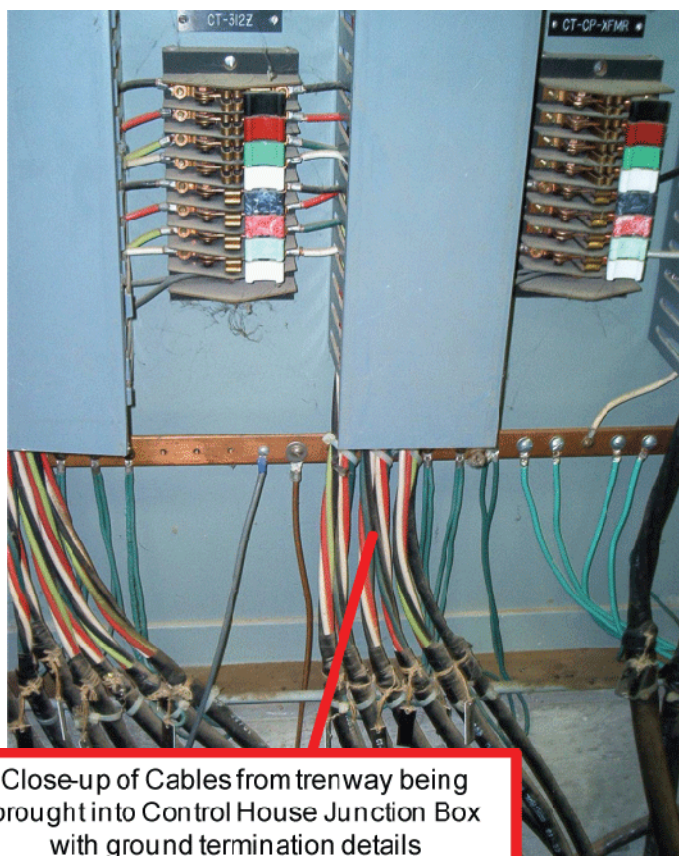


Figure 18: Grounding of control cable shields and j-boxes in control building.⁷⁷

Cables extend from the junction boxes to the individual racks of equipment. These cables will carry any remaining high-frequency transients that were coupled to the cables outside, and they will also carry high-frequency transients coupled from the electromagnetic fields that propagate through the walls of the building. The direct coupling of E1 HEMP fields inside the building is strongly influenced by the construction type of the building. There are strong variations for the penetrating electric fields at frequencies above 10 MHz due to whether the building is made of concrete (with or without reinforced bars), bolted metal, or wood.

While this discussion is provided to give an indication of the scope of the problem, it will be necessary to evaluate many factors that are common or different in various power substations in order to determine the potential impact of an E1 HEMP event and to recommend cost-effective protection techniques.

Based upon coupling calculations it appears that levels up to 10 kV may be coupled to horizontal buried lines in a substation yard (although 20 kV is possible under some scenarios). HEMP voltage levels on the order of 70 kV may also be induced on vertical conduits. While the amount of these voltages that could propagate to the relays and other electronic control equipment is

⁷⁷ Source: Metatech Corp.

extremely variable, the fact that upsets on relays begin at 3.2 kV and damage to programmable logic controllers (PLCs) and personal computers begin at approximately 0.5 kV, indicates a serious concern for the continued operation of the substations.⁷⁸

Even if the cable penetrations to the control building are protected, the penetration of the E1 HEMP fields inside the building and their coupling to the cables just above the electronic cabinets still presents an issue. The level of the field penetrating the building is completely dependent on the type of wall and ceiling construction; however, tests performed in the past on telephone switching centers indicated that voltage levels as high as 10 kV could be induced on internal cables. Depending on the way that the cables enter the cabinets (whether the cable shields are bonded to the cabinet shield or not) will determine if these voltages reach the electronic equipment ports inside.

Generation and Control Center Programmable Logic Controllers and Computers

Generation facilities use PLCs to control the flow of fuel and other aspects of the power generation process. As indicated in previous test programs, damage may occur for E1-like pulses at levels as low as 0.6 kV, although while one manufacturer's equipment failed at that level; the other failed at 3.3 kV.⁷⁹ Since most generation facilities are staffed, upsets may not be as important as damage, however, the damage levels indicated are quite low. In addition, it is not expected that the cabling within the generator facility will be better protected than in a substation, so again levels of induced voltages as high as 70 kV may be coupled to vertical cables and 20 kV for horizontal buried cables in some generation facilities.

Control centers have many communications lines entering and leaving the facility. Though many bulk power system control centers are constructed to high physical resilience and security standards, computer equipment is not always afforded the same level of immunity found in substations or generation facilities. Computers are likely to fail at the communications port due to E1 HEMP at 0.5 kV, and other test data indicates that Ethernet ports are generally vulnerable at low levels. Given that ordinary building protection levels will typically allow up to 10 kV to be coupled to internal cables, this indicates a potential problem.

The location and type of wall construction of control centers can have a significant impact on their relative vulnerability. A control center built below the surface of the Earth has much better natural shielding than one built above grade.

⁷⁸ Savage, E. B., K. S. Smith, M. J. Madrid, J. L. Gilbert and W. A. Radasky, "Fast Pulse Testing of Power System Control Equipment to Determine their Susceptibility to HEMP Conducted Transients," Proceedings of the 16th International Zurich Symposium on EMC, Zurich, Switzerland, February 2005, pp. 377-380.

⁷⁹ See Footnote 39.

Distribution System

Approximately 78% of all electric power delivery to end-users is delivered via 15 kV class distribution lines. The likelihood for an optimum exposure of a segment of the line is high and that at some point along the feeder the maximum E1 HEMP voltage will be induced, creating a possible insulator flashover.

At present, considerable uncertainty exists as to whether the typical insulation capability of these distribution assets will be sufficient to withstand the induced overvoltages due to the E1 environment of a HEMP threat. Prior analysis of the E1 HEMP threat by the EMP Commission indicated that induced overvoltages ranging from 200 kV to more than 400 kV (depending on the scenario) can occur on distribution lines over geographically widespread regions. If large-scale distribution line insulator failure, damage, or flashover occurs, the impacted regions will likely experience outages on the distribution system, especially if many flashovers occur within 1 mile of many substations where the fault current will be high. Concerns also exist relative to distribution-level transformers.

It is noted that under some scenarios, the loss of large numbers of insulators and transformers will result in a sudden loss of load to the bulk power system. Further information on the technical aspects of these vulnerabilities are found Appendix 2.

E3 HEMP

As indicated earlier, the E3 HEMP may reach levels of 40 V/km under particular burst scenarios, according to the IEC. The area coverage of large fields on the Earth's surface is on the order of a circle with a radius of roughly 1000 km in radius. In this region, it is expected that induced GIC in EHV power lines could be as high as 1000 A, creating a potentially severe threat to the power grid in that region. As indicated by the EMP Commission under these threat conditions, a blackout is likely. The expected E3 GIC footprint associated with a large-yield device detonated over Columbus, OH is depicted in Figures 19 and 20. The areas of potential resulting power system outages are shown in a separate chart. Also as in the severe geomagnetic storm case, many transformers could be at risk of irreparable damage. Finally before a power blackout occurs, the generation of severe harmonics in the power network is also a threat to computer and other communications facilities due to potential damage to and misoperation of uninterruptable power supply systems.

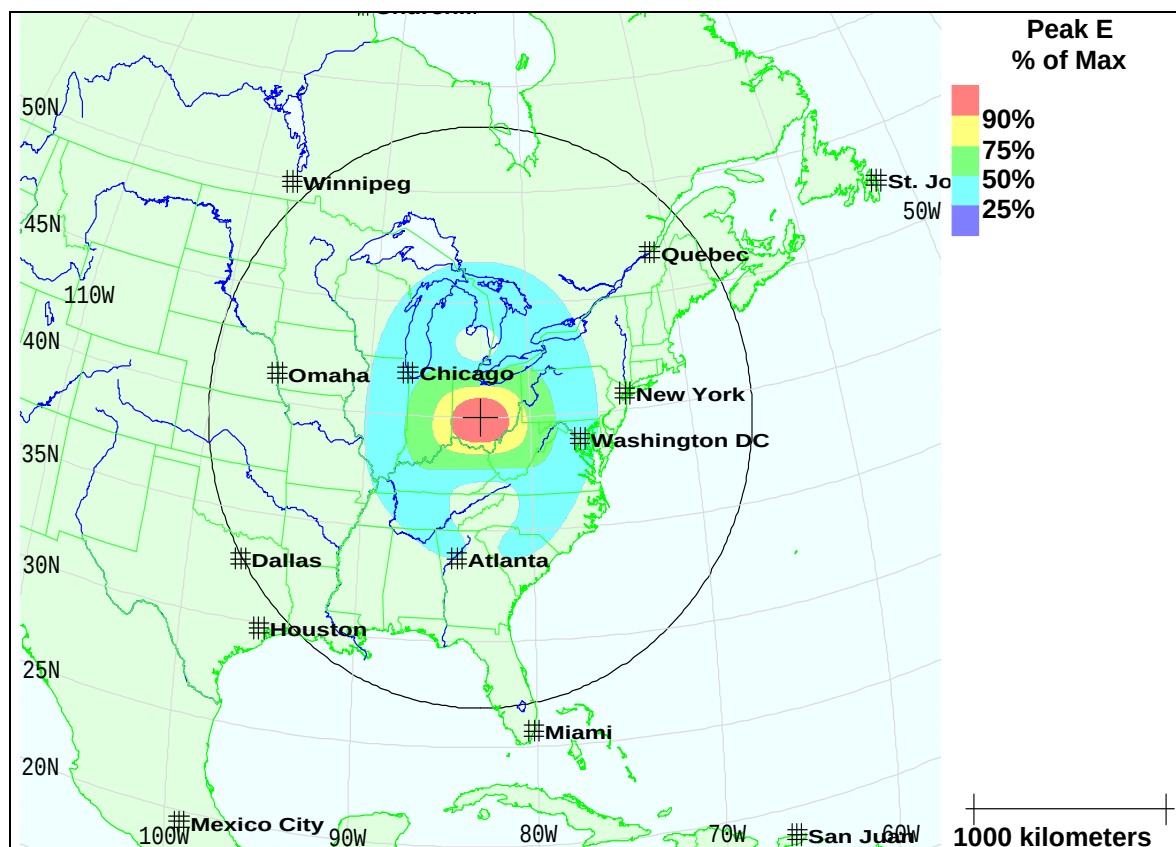


Figure 19: A map showing the E3 Field Pattern from a Large Yield Device positioned over Columbus OH.⁸⁰

⁸⁰ Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Volume 1: Executive Report. Commission to Assess the Threat to the United States from an EMP Attack. Washington, DC. April 2008. http://www.empcommission.org/docs/empc_exec_rpt.pdf

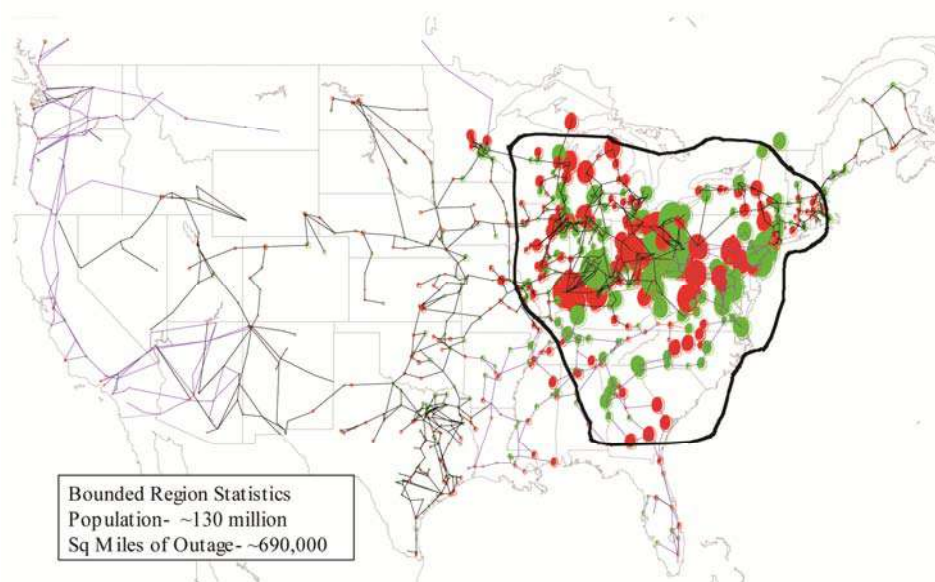


Figure 20: Summary of GIC Flows in U.S. Power Grid for Threat Columbus, OH – Large Yield Device. The outlined region shown above would be expected to experience collapse from this E3 Threat Scenario.⁸¹

As discussed earlier, the relatively limited global manufacturing capability for EHV transformers could pose a significant challenge to restoration efforts were a large number of EHV transformers to be damaged during a single event. Procurement times for these assets typically range between 12 and 24 months and, while some spares are kept on hand, an impact involving irreparable damage to hundreds of transformers could result in certain areas of the system being unable to serve customers for an extended period of time (months or even years). In addition the trend to build higher voltage transmission networks today leads to increased vulnerability from GIC, as discussed earlier.

One aspect of the HEMP is different than geomagnetic storms and that is the fact that the E3 HEMP waveform is preceded by the E1 and E2 HEMP waveforms. If the E1 HEMP causes some of the solid-state safety relays to misoperate in the first microsecond, then it is possible that the E3 HEMP will cause additional damage to transformers as the high-voltage network collapses without the benefit of relay protection.

For details concerning the GIC impacts, the reader should examine the sections of this report dealing with the impacts of geomagnetic storms on the power grid.

⁸¹ Image provided courtesy of Metatech.

Consequence

As indicated by the impacts in the discussion above, an E1 HEMP event could simultaneously (within one power cycle) create malfunctions of electronic control equipment over thousands of kilometers. Traditional probabilistic planning and operating criteria do not provide sufficient protection from such a widespread, simultaneous impact. Restoration may also be complicated by the amount of equipment available to replace damaged assets. It is unknown, for example, the number of protective relays that will be damaged, but without facility-level protection, the number may exhaust current spare parts on hand.

The second consequence is that since the E1 HEMP comes before the E3 HEMP, some relays may not operate properly to protect transformers during an E3-HEMP event. This could increase the likelihood of damage to large EHV transformers beyond that caused directly by GIC impacts.

The programmable logic controllers and computer controls at power generation facilities and in control centers are vulnerable to E1 HEMP upset and damage. Such effects may complicate restoration efforts until this equipment is repaired, replaced, or restored to service. As with the relays, it is possible to protect the existing equipment through a high-frequency facility protection program that involves improved grounding, shielding, fiber optic cabling and/or the addition of surge protection devices.

On the distribution system, the E1 HEMP may damage a small percentage (but still a significant number) of power-line insulators that could require replacement. Pole-mounted distribution transformers may also be damaged by the E1 HEMP. These issues could cause delays in restoration of power to certain customers.

For the E3 HEMP threat to transmission grid transformers and grid collapse, the best approach is to reduce or eliminate the flow of GIC through transformer neutral protection. The E3 HEMP currents flow into the high-voltage network through the neutrals of these high-voltage transformers. This approach will also reduce the harmonics generated in the network. These aspects are discussed in more detail in the section of this report dealing with geomagnetic storms.

Intentional Electromagnetic Interference (IEMI)

Threat

The term IEMI has been defined as: “Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes”.⁸² In general the term refers to the intense electromagnetic fields generated by a repeatable (non-explosive), highly-mobile, high-power generator, which are directed to a target by an antenna.

⁸² IEC 61000-2-13, Electromagnetic compatibility (EMC) – Part 2-13: Environment – High power electromagnetic (HPEM) environments – Radiated and conducted, 2005.

The International Electrotechnical Commission (IEC) has worked intensively in this area for the past 10 years to understand the environment levels that may be generated and the vulnerability of commercial equipment to these types of fields in order to establish protection standards. In addition researchers at recent electromagnetic compatibility conferences have studied different aspects of the threat including the environments, the coupling, the vulnerability of equipment and protection methods. The IEEE electromagnetic compatibility Special Issue on IEMI and HPEM is a useful resource for reviewing IEMI technologies.⁸³

Figure 21 illustrates a frequency-domain comparison of IEMI environments with other high power EM environments, including the E1 portion of HEMP. There are two main categories of IEMI environments: wideband and narrowband. The figure shows one example of a wideband environment and 4 different examples of narrowband environments. The IEMI frequency range of greatest interest is typically between 0.3 and 3 GHz, although higher and lower frequencies may be important in special cases.

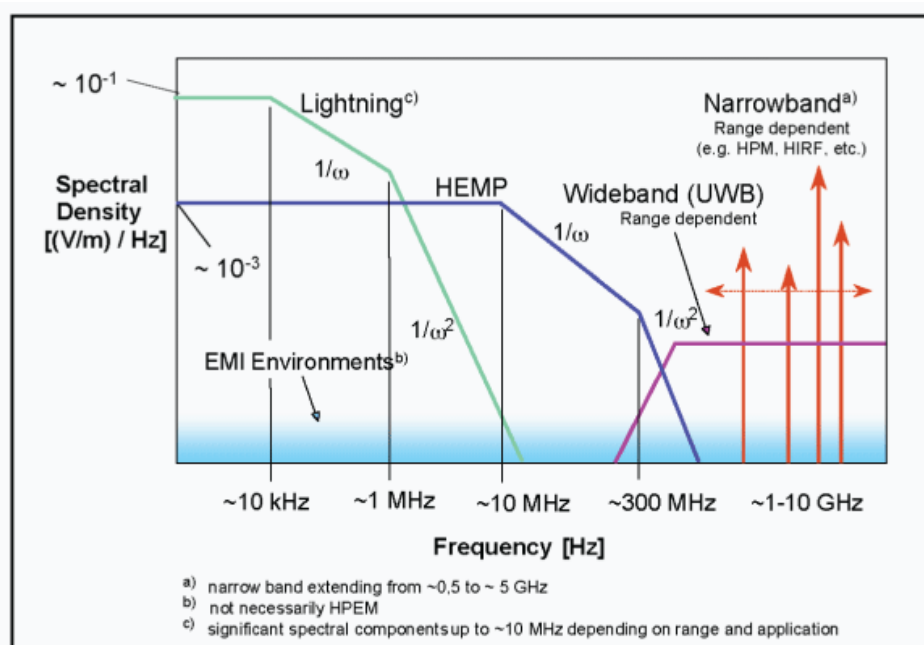


Figure 21: Comparison of IEMI environments to other HPEM environments in the frequency domain [53]

Very fast (hyperband) wideband pulses that have rise times of less than 100 ps and pulse widths on the order of 1 ns are of most concern. These pulses are considerably faster than E1 HEMP and can easily be produced at repetition rates between thousands and millions of pulses per second. At close ranges or for powerful generators, peak fields of nearly 10 kV/m can be

⁸³ Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI)", IEEE Transactions on Electromagnetic Compatibility, Volume 46, No. 3, August 2004.

propagated to the location of critical electronics, and effects on electronics have been noted as low as 1 kV/m for pulsed waveforms.

In addition, certain IEMI threats are produced as narrowband EM waveforms that are generated in a pulse that lasts on the order of 1 microsecond. Narrowband threats require more energy to generate than wideband pulses, but also create damage both through EM interactions and through the damage of integrated circuits directly. Narrowband field levels at 10 kV/m can easily be generated using surplus radar systems and can be damaging to many different types of commercial electronics at levels above a few hundred V/m.

In both cases (wideband and narrowband) the IEMI environments tend to decrease as $1/r$ from the EM weapon source and therefore they are not as efficient as E1 HEMP in coupling to lines longer than 10 meters as the IEMI fields are varying in both magnitude and angle of incidence when coupling to a cable. On the other hand, the IEMI threat can appear inside of a building at close range to sensitive electronics in the situation when the EM weapon fits inside of a briefcase or suitcase. In general, the IEMI threat creates upset and damage to equipment through direct illumination of the equipment itself and the last several meters of cables connected to the equipment.

The IEMI threat is a very local threat compared to E1 HEMP. As the threat is electromagnetic in nature, upset and damage to equipment may occur without any indication of the reasons. An enemy with a powerful electromagnetic weapon could potentially disrupt the operations of multiple facilities by traveling from one parking lot to another over a period of a day.

IEMI Coupling

IEMI coupling to bulk power system assets are generally very similar to those of the E1 portion of a HEMP event discussed earlier in this document, with the exception of coupling to long lines on the order of 100 meters long, for which it is less efficient than E1 HEMP due to the $1/r$ falloff of the fields.

It has been established that at frequencies near 300 MHz the maximum coupling ratio of induced voltage to the electric field is approximately 1.0. This means that an incident IEMI narrowband field of 10 kV/m at 300 MHz can induce 10 kV on a cable. A hyperband waveform with a pulse width of 1 nanosecond would also have the same effectiveness in coupling (1.0) and again a 10 kV/m electric field would induce a peak voltage of 10 kV.

Since the IEMI coupling process is only effective over 10 meter lengths of cable (or shorter), it is likely that the conducted threat is most important for the coupling to cables inside of a substation or a power generator control building. It is also a threat to the sensors mounted in the substation high-voltage yard. IEMI coupling to the control cables outside of the substation control building does not lead to significant vulnerability to the electronics inside, due to the longer cable paths for that geometry and the higher frequency content for IEMI (creating significant attenuation).

The same situation is true for control centers as the external cables leading to the building are unlikely to propagate very high frequency IEMI transients in a common-mode geometry.

For distribution transformer winding insulation or power line insulators, the BIL ratings are typically 100 kV or higher, and the expected induced IEMI voltage levels of 10 kV at frequencies on the order of 1 GHz are unlikely to cause any problems. Reaching a level of 100 kV/m from IEMI weapons is very unlikely.

Figure 22 illustrates a scenario of how IEMI environments can be produced and how they will interact with a building's electronics. In this image, a fiberglass van with a surplus radar system can sit in a parking lot and generate significant fields incident on a nearby building. These fields can directly penetrate the walls and windows of the building and can couple to the wiring outside, creating voltage pulses that then penetrate the building. Of course other scenarios are possible including briefcase weapons taken inside the building by a visitor or disgruntled employee.

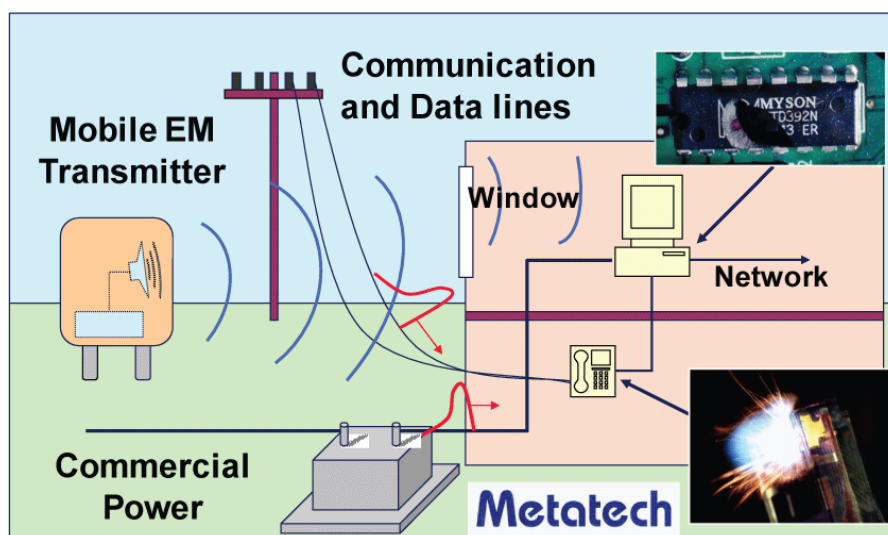


Figure 22: Coupling paths for radiated IEMI fields⁸⁴

The discussion of the threats and impacts of HEMP and IEMI in this report have been directed to the power system assets themselves. It is certainly true in the case of HEMP, that the E3 HEMP is likely to create problems with factory power systems due to the injection of high levels of power harmonics due to the E3 HEMP. Laboratory tests have found that many UPS systems are unlikely to perform well under high levels of power harmonics. In addition the E1 HEMP is a serious threat to business and home computers through the direct coupling of high levels of currents into the power supplies and the Internet wiring. Industrial customers also are likely to have difficulties with control equipment such as programmable logic controllers necessary to run their businesses. As E1 HEMP will also affect communications and transportation, it is likely that many businesses will experience significant impacts lasting several days. As a result, load

⁸⁴ Image provided courtesy of Metatech.

patterns and demand for electricity may deviate significantly from the norm. These effects will complicate operation of the system, as the system is designed to constantly keep supply and demand in balance. The IEMI threat is not a significant threat to the load as the range of the effects are typically less than 1 km, and it is unlikely that much of the load could be impacted.

Vulnerability

High-Voltage Substation Controls and Communications

The most significant IEMI concern within a high-voltage substation is not the high-voltage transmission lines and transformers, but rather the low-voltage sensor and control lines that extend from the transformer yard to the relays and other control electronics in the control building. Coupling to sensors in the transformer yard and with the cables inside of the control building are of most concern, although the last few meters of exterior cables could be a factor for lower frequency IEMI threats.

As in the case of the E1 HEMP, the poor grounding (at high frequencies) of control cables inside of the control building is a problem to be considered. In addition, direct coupling to cables through the walls of the control building is even more important for IEMI as coupling close to the electronics is more effective for IEMI than for E1 HEMP. Like E1 HEMP, the IEMI field penetration inside the building is strongly influenced by the construction type of the building. There are strong variations for the penetrating electric fields at frequencies above 10 MHz due to whether the building is made of concrete (with or without reinforced bars), bolted metal, or wood.

As discussed earlier, it appears that maximum levels of approximately 10 kV may be coupled to horizontal buried lines in a substation yard just before entering the substation building. The amount of these voltages that could propagate to the relays and other electronic control equipment is extremely variable, but upsets on relays begin at 3.2 kV and damage to programmable logic controllers and personal computers begin at approximately 0.5 kV, indicating a serious concern for the continued reliable operation of substations.

The more important problem for IEMI is that, even if the cable penetrations into the control building are protected, the penetration of the IEMI fields inside and coupling to the cables just above the electronic cabinets still presents a problem. The level of the field penetrating the building is completely dependent on the type of wall and ceiling construction; given that field levels inside a poorly shielded control building could be as high as 10 kV/m, up to 10 kV could be induced on cables leading to the electronics. Depending on the way that the cables enter the cabinets (whether the shields are bonded to the cabinets or not) will determine if these voltages reach the electronic equipment ports inside.

Generation Facilities

Generation facilities use programmable logic controllers to control the flow of fuel and other aspects of the power generation process. Damage may occur for IEMI-like pulses at levels as low as 0.6 kV, as one manufacturer's equipment failed at that level while the other failed at 3.3 kV. Since most generation facilities are staffed, upset may not be as important as damage, however, the damage levels indicated are quite low. In addition, it is not expected that the cabling within the generation facility will be better protected than in a substation, so again levels of induced IEMI voltages as high as 10 kV are possible at the locations of control electronics.

Control Centers

Control centers have many communications lines entering and leaving the facility. Though many bulk power system control centers are constructed to high physical resilience and security standards, computer equipment is not always afforded the same level of immunity found in substations or generation facilities. Equipment like the PC will fail at its communications port due to a fast pulse at 0.5 kV, and other test data indicates that Ethernet ports are generally vulnerable at low levels of IEMI. Given that ordinary building protection levels will allow up to 10 kV of IEMI environments to be coupled to internal cables, this indicates a potential problem.

An important factor to consider is the location and type of wall construction of control centers. A control center built below the surface of the Earth has much better natural shielding than one built above-grade.

Distribution Line Insulators

As previously described, flashover of distribution insulators begins for BIL levels of about 100 kV. For E1 HEMP, the levels can be higher due to a narrower pulse width, which requires longer times for arcs to close around the insulators. For IEMI the faster waveform will require even more time. Also the fact that it is extremely difficult to generate a peak voltage pulse greater than 10 kV makes it clear that IEMI is not a real threat to distribution class insulators.

Distribution Transformers

The Oak Ridge National Labs power system studies during the 1980's examined the possibility of E1 HEMP damage to distribution step-down transformers found in the U.S. power grid. This testing included 19 samples of 7.2 kV/25 kVA power distribution transformers, using E1 HEMP like pulses. Damage that occurred was usually from pinhole damage and dielectric breakdown within the windings.

Failures occurred during the test when the peak fast pulse voltage was between 264 and 304 kV. For IEMI the likely maximum induced voltage level is about 10 kV, which is much lower than the levels required to damage this type of distribution transformer. It is therefore unlikely that IEMI is a serious threat to distribution transformers.

Consequence

The primary concern of IEMI is based on the high levels of fields generated and the low field levels of failures observed on electronic equipment under test (including solid-state computer and control equipment), with upset being more likely than damage. This upset may be severe, requiring the device to power down and restart, making IEMI a more significant threat to unmanned facilities, such as substations. Because of the use of large numbers of computers in control centers, these facilities are also at risk for disruption, even though they are staffed.

IEMI testing performed in laboratories has indicated that computer forensics are not likely to be available to indicate the cause of failure after a crash of several PCs as multiple subsystems within a single computer are usually affected by the IEMI at the same time. In some cases it has been necessary to reload the system software to restart a PC that has malfunctioned due to IEMI.

Mitigations

The High-Impact, Low-Frequency Event effort is helping to promote a better understanding of GMD, HEMP and IEMI risk across the electric sector. As these risks are better understood, efforts should continue to develop and study potential mitigations to assess their viability, both in terms of efficacy and economic feasibility.

The GMD threat, while more widely understood, is gaining renewed attention across the sector as new predictions suggest that more severe storms could occur and potentially reach lower geographic latitudes than formerly expected. While the electric sector made important improvements in this area after the March 1989 storm, more work is needed to evaluate new protections and reliability considerations associated with future geomagnetic storms.

With respect to a HEMP threat, the inherent limitations in fully protecting this massive infrastructure from a HEMP event should be understood and appreciated. In its 2008 report, the EMP Commission found that it is not practical to try to protect the entire electrical power system or even all high value components from damage by an EMP event. The number and variety of components installed across the system make the time and cost of such an effort prohibitive. The EMP Commission recommended an approach designed to reduce the recovery and restoration times and minimize the net impact from the attack.⁸⁵

The primary proposal for action from the workshop was that work should continue to better understand these threats, assess their likelihood, and identify viable mitigations. Consideration should be given to efficacy, financial implications, resource requirements, and the length of time that would be required to implement potential protections. Specifically, NERC should create a task force to continue these efforts and build consensus around appropriate mitigation options for industry. The task force could consider developing a full “defense plan” for these risks—covering all considerations from system design implications to hardening existing assets to system restoration. The task force should also consider the need for mandatory standards on its findings, whether related to equipment specifications or Reliability Standards. The concepts outlined in the sections below should be considered by the task force in their work, but do not represent recommendations to industry, government, or NERC.

⁸⁵ “Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures,” April 2008.

Proposal for Action

GMD/EMP 1

NERC, working with its stakeholders, the U.S. DOE, and appropriate government authorities in Canada should create a task force of industry, equipment manufacturers, and risk experts to evaluate and prioritize mitigation and restoration options for Geomagnetic Disturbances (GMD), High-altitude Electromagnetic Pulse (HEMP) events, and Intentional Electromagnetic Interference (IEMI) threats, while recognizing the similarities and differences of these three severe electromagnetic threats. Focus should be given to identifying the prioritized “top ten” mitigation steps that are cost-effective and sufficient to protect the power system from widespread catastrophic damage due to each of these threats. The task force should consider the options and concepts discussed in this workshop report, including:

- Acting jointly with the U.S. DOE, National Oceanic and Atmospheric Administration (NOAA), and other appropriate U.S. agencies and authorities in Canada, develop the design of an event monitoring network that can better capture the occurrence of a GMD event with sufficient detail (geographically-dispersed monitoring sites) to correlate an event to power system and equipment issues that arise, and that measures and captures the time-rate-of-change of magnetic flux that is critical to the electric sector. Develop a data sharing and funding plan that includes appropriate cost sharing by the North American governments and affected industries.
- Define the protection environment for each of the electromagnetic threats, considering the work recently completed by the U.S. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (U.S. EMP Commission), the National Academy of Sciences, FERC and the Federal Emergency Management Agency (FEMA).
- Focus mitigation strategies on “high-impact” electric power facilities, wherein the loss of functionality will adversely and perhaps severely impact the delivery of power to the largest number of people for the longest period of time. Specifically consider remedial design corrections to reduce the vulnerability of the existing bulk power system. Focus should be given to the highest voltage portions of the transmission system and considering the growing vulnerability as this system is expanded.
- Consider the tradeoffs of economic efficiency and reliability of the power system with regard to these electromagnetic threats using risk-based analysis. Cost estimates of potential mitigations provided by the EMP Commission should be revisited to appropriately account for labor, engineering, installation, and associated operating costs.
- Identify the primary interdependencies with the other critical infrastructures that will impact restoration and reconstitution, with focus on telecommunications and fuel supply and delivery. Encourage cross-sector coordination to ensure the response of these assets to a GMD or HEMP attack is understood and that appropriate protections are put in place.
- Evaluate the role of spare equipment and sharing programs, such as NERC’s Spare Equipment Database.
- Evaluate the effectiveness of existing blackstart procedures, and the need for exercises for a case where the blackout area is extremely large and other infrastructures have been damaged. Develop new procedures if required.
- Consider the need to develop a full “defense plan” that considers prevention, blackstart analysis, restoration, etc. to establish a model checklist/procedure for sector entities to deal with each of the threats.

Participation from high-level government officials in both the U.S. and Canada will be important to help in building consensus among business leaders on the appropriate level of investment in mitigating these threats when considered among the many other investment priorities facing the electric sector. Coordination with, and participation by, state and provincial regulators will also be an important component of these efforts.

Proposal for Action

GMD/EMP 2

Governmental authorities in the U.S. and Canada should continue to support industry efforts to address these risks. An executive order from government leaders, such as the President of the United States, would give additional weight to the importance of these issues relative to other priorities in both the public and private sectors.

Planning

As discussed in earlier sections, the bulk power system is generally highly-resilient and designed to withstand the loss of one and a half times the single largest asset on the system without affecting reliability. Certain key nodes, if damaged or destroyed, however, would have a greater impact on restoration efforts than others. Key loads, such as military installations and other critical infrastructure components (i.e. major natural gas hubs or telecommunications facilities), are other important elements of the system from a societal perspective that could be considered. Just as these assets should be prioritized for protection from a coordinated attack, so could these assets be prioritized for protection from GMD, HEMP, and IEMI threats.

Likewise, other infrastructures should take electric sector needs into consideration as their response plans are developed. Ultimately, a holistic approach will provide the most effective protection to North America's critical infrastructures. Protection goals and risk-based planning thresholds could be defined and developed in a cross-sector framework, taking interdependencies into account.

The strengthening and expansion of backup equipment sharing programs may be a critical component of improvements, particularly with respect to extra-high-voltage transformers. Though some limited manufacturing capacity exists in North America, nearly 100 percent of these assets are currently manufactured offshore and procurement can take 12-24 months. The "Spare Transformer Equipment Program" (STEP) run by the Edison Electric Institute and DHS S&T's Recovery Transformer Project are important steps, and ongoing efforts to improve these programs should continue. Ultimately efforts could be considered to bring more of the supply chain and manufacturing base for these critical system components back to North America.

Adequately hardening assets will require close coordination with technology vendors and developers. Ensuring protections are "built-in" to system components purchased by asset owners as opposed to requiring a "bolt-on" solution after installation in the field will significantly

enhance the resiliency of the system to these threats, although due to the significant number of installed components, it is likely that facility protection will be higher priority in the short term. Equipment and facility protection standards have been developed by the IEC Subcommittee 77C and could be more widely adopted.

Focus is needed to identify protections specific to substations, generation facilities, and control centers. Dubbed “hardening,” bolt-on protections should be considered for installed assets. Emphasis should be given to preventing catastrophic failures of key infrastructure assets, particularly EHV transformers. This would require an engineering approach in particular to modify the power grid to block, reduce, or in some other manner mitigate (e.g. preventive tripping) GIC and E3 HEMP effects in key EHV transformer assets. This would entail remedial design measures to the existing infrastructure. Various options such as transformer neutral resistors (as reviewed by the EMP Commission) appear to be feasible and reasonably cost-effective, though further analysis of the cost implications and specific application to the system as a whole is needed. Importantly, these solutions must not result in any unintended reliability consequences.

Consideration should also be given to applying high-frequency ($f > 1$ MHz) shielding, grounding, bonding and cable protection technologies for control and communications cables within substations and generation facilities. Further analysis is needed to evaluate the best and most cost-effective means to apply these technologies in generation facilities. The design and geometry of networks in bulk power system control centers should be more thoroughly evaluated as potential mitigations and protections for these environments are prioritized. Detailed cost estimates, including time and labor (which are not sunk costs for the industry), for these measures should be developed and included in the evaluation of feasibility.

Additional efforts are also needed at the distribution level to evaluate, develop, and deploy appropriate and cost-effective protections for the distribution system. The task force referenced above should reach out to distribution engineers and equipment manufacturers, potentially through IEEE and other technical groups considering the issue.

Long-term research, development, and deployment efforts should also be evaluated for new equipment and infrastructure components. The approach to protecting the system from these threats should embrace new technologies, placing emphasis on hardening new smart grid components.

Proposal for Action

GMD/EMP 3

Appropriate government authorities (to potentially include the U.S. DOE, FERC, DHS, NOAA, and National Aeronautics and Space Administration (NASA), and appropriate government authorities in Canada) should work with research organizations and the private sector to consider a roadmap for long-term research, development, and deployment on mitigating options for these threats. These efforts should be coordinated with NERC and the electric sector.

New restoration procedures should also be considered. An “ultimate blackstart” scenario could be developed to guide system restoration when all generation is completely shut down and a significant number of assets face some degree of physical damage. Consideration of the availability of the fuel source should also be included in this scenario, as would an analysis of what kinds of loads would be most affected by a HEMP event.

The implications of current system design trends, which have led to the development of highly-efficient and reliable high-voltage transmission lines, could also be evaluated to ascertain whether new criteria could be applied that would lessen the potential vulnerability to GMD and E3 HEMP events.

Operations

Input from operations will be crucial to the success of many of the efforts discussed in the planning section above. For example, creating an “ultimate blackstart” scenario should be a joint effort between planners and operators. Scenarios involving physical damage to key nodes, significant loss of load due to an E1 HEMP event, and recovery from complete loss of equipment should be considered. Once these scenarios are developed, operators would need to regularly train and drill responses to ensure they are prepared were an event to occur.

Many system operators already have plans in place to operate the system in a conservative state should a major GMD event be expected. These plans include steps such as:

1. Discontinue maintenance work and restore out-of-service lines to service. Avoid any removal of long lines from service
2. Maintain system voltage well within the acceptable range, since voltage swings may occur
3. Adjust the flows on HVDC lines to between 40% and 90% of nominal ratings
4. Reduce the loading on any generators operating at full capacity in order to provide reserve power and reactive capacity margins
5. Consider the possibility that shunt capacitors connected to the grid and static VAR compensators may be lost and prepare for such an event
6. Dispatch reserve generation to manage system voltage and tie line loadings to distribute reserve generation
7. Bring on-line any equipment capable of synchronous condenser operation to provide reactive power reserve
8. Notify adjacent control areas of GIC problems⁸⁶

These plans were developed after the 1989 GMD event and were improved and drilled extensively during the Y2K transition in 1999. When in such a state, reserve capacity is increased and units are backed down from full output so that more units are carrying the load of the system and are available to instantly ramp up to meet demand were units to unexpectedly trip

⁸⁶ Evaluation Report for “Integrated forecasting system for mitigating adverse space weather effects on the Northern American high-voltage power transmission system”; NASA Goddard Space Flight Center in partnership with the Electric Power Research Institute; p 8.; 1/10/2008

offline. In severe scenarios, market-based purchasing and selling decisions can be suspended. More regular sector-wide drills of this capability could be considered to ensure smooth transitions in and out of this state.

Improved options for space weather forecasting should be considered to ensure adequate, timely, and actionable information is provided to system operators across the sector. The K-index approach presently used by NOAA to rank the severity of solar weather should be revised or amended to consider more thoroughly the severity of GMDs and the regional coverage of the anticipated storms. Private forecasting services could be more broadly used by industry or publicly sponsored so the most accurate information available is put in the hands of those who need it most. Communications channels could be strengthened so that information is reliably provided to all asset owners and operators. The communications aspect is also important for HEMP and IEMI as elevated threat levels for either of these threats could be rapidly transmitted to the asset owners and operators if an emergency communications system were developed.

Proposal for Action

GMD/EMP 4

NERC, the U.S. FERC, DOE, DHS, NOAA, and NASA, and appropriate government authorities in Canada, together with subject matter experts, should work together to recommend the development of advanced methods to ensure system operators are given region-specific, timely, and accurate information regarding the expected duration, intensity, and geographic footprint of impending geomagnetic disturbances. Focus should be given to both extreme events and long-duration, low-intensity storms.

Proposal for Action

GMD/EMP 5

The U.S. DOE, DHS and appropriate government authorities in Canada, together with subject matter experts, should work together to establish an alert procedure to inform the electric sector that threat levels of an HEMP or IEMI attack have increased or that an attack is imminent. The communications method developed to distribute information concerning an impending geomagnetic storm or other critical infrastructure protection information could be used to disseminate these notices.

Efforts Already Underway

A number of reports have recently been published on the impacts of GMD, HEMP, and IEMI to civilian infrastructure. These include the 2008 EMP Commission's report⁸⁷ and the 2009 National Academies report on space weather⁸⁸. The electric sector is largely aware of these reports, but further work is needed to formally consider the issues raised therein from the asset owners' perspectives. The task force recommended earlier in this section should consider these reports in their work.

Work continues to raise awareness of GMD, HEMP, and IEMI threats through the High-Impact, Low-Frequency effort. As part of the effort, NERC and the U.S. DOE conducted a Technical Conference in March 2010 that provided industry participants the opportunity to ask questions and dive into the technical details of the issues with some of the world's premier experts on the effects GMD, HEMP, and IEMI on power systems. Roughly 130 people attended the closed, two-day session. Topics presented included threat environments, anticipated effects, and potential mitigations.

Electrical Power Research Institute's (EPRI) SUNBURST network is an ongoing effort to measure GIC events and their effects and to continue research studying the cause, effects and mitigation of GIC impacts on electrical power systems. The data collected supports research into prediction models, mitigation techniques and advanced modeling prior to a storm. The SUNBURST network consists of a consortium of member utilities where near-real-time continuous monitoring of large power transformers is performed to assess the impact of impinging solar storms on the grid. Due to the nature of this network, it is not intended to represent a comprehensive view of the entire system, but does provide an important data point in evaluating these risks and impacts. By measuring these GICs along with current and voltage harmonics—the SUNBURST system helps to communicate the breadth, intensity, and localized transformer saturation impact as these storms occur.

⁸⁷ *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*. Commission to Assess the Threat to the United States from an EMP Attack. Washington, DC. April 2008. http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

⁸⁸ *Severe Space Weather Events--Understanding Societal and Economic Impacts: A Workshop Report*. National Academies Press. Washington, DC. 2008. http://www.nap.edu/catalog.php?record_id=12507

Appendix 1: HEMP Impacts on Distribution Infrastructure

Insulator Flashover and Failure

Approximately 78% of all electric power delivery to end-users is delivered via 15 kV class distribution lines. Figure 23 illustrates a typical distribution feeder geometry that indicates the variation of the orientation of the lines for a single feeder. This shows that the likelihood for an optimum exposure of a segment of the line is high and that at some point along the feeder the maximum E1 HEMP voltage will be induced, creating a possible insulator flashover.

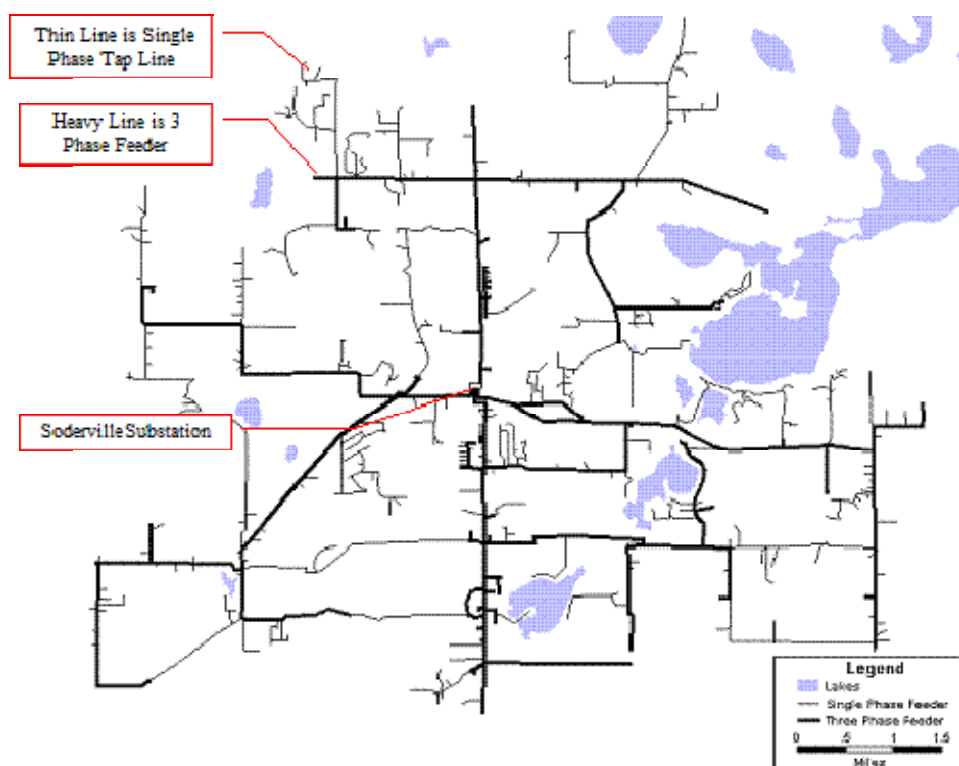


Figure 23. A typical above ground 15 kV distribution geometry in the U.S.⁸⁹

At present, considerable uncertainty exists as to whether the typical insulation capability of these distribution assets will be sufficient to withstand the induced overvoltages due to the E1 environment of a HEMP threat. Prior analysis of the E1 HEMP threat by the EMP Commission indicated that induced overvoltages ranging from 200 kV to over 400 kV (depending on the scenario) can occur on these distribution lines over geographically widespread regions, and that if large scale distribution line insulator failure or flashover occurs, the impacted regions will likely experience power grid collapse, especially if many flashovers occur within 1 mile of many substations, where the fault current will be high.

⁸⁹ Image provided courtesy of Metatech.

Appendix 1: HEMP Impacts on Distribution Infrastructure

Typical insulation designs for distribution feeders usually are based upon testing of the 1.2 μ s rise time impulse due to lightning (with a 50 μ s pulse width). For these lightning impulses, typical pin insulator withstand generally starts at BIL levels of ~100 kV. It has generally been observed that the shorter duration pulse widths of the E1 HEMP threat will increase the level of the flashover voltage for these insulators, but the amount of increase was not well substantiated until further testing was performed.

Two sets of experiments and results are summarized here. The first is work done by Prof. Stan Gryzbowski from Mississippi State University (MSU), using standard insulator test techniques and testing of a wide variety of insulators found in the U.S. power grid. He also examined variations due to polarity of the impulse and other factors such as wet insulators. All of the testing was performed without power on the insulator, which is the usual method for testing insulators in the United States.

The MSU test results are summarized in Table A-1-1, showing both the ratio of the peak critical flashover (CFO) levels of the steep front flashover to the standard lightning tests. It is noted that in most cases the E1 HEMP related tests indicate that the peak HEMP voltage required is often less than a factor of 50% higher than the lightning BIL tests, and with negative polarity it is only about 10% higher. The polymer suspension insulator appears to be more robust to E1 HEMP waveforms. It is also recognized that apparently peak CFO voltages of much less than 200 kV are a concern for flashover.

Table A-1-1. Ratio of peak CFO voltage for steep front, short duration pulse to lightning impulse [12].

Configuration	Typical Application Line Voltage	POSITIVE POLARITY		NEGATIVE POLARITY	
		DRY	WET	DRY	WET
ANSI 55-4	13.2 kV	2.7	-	1.04	-
ANSI 55-3	11.5 kV	1.7	-	1.06	-
ANSI 52-1	13.2 kV	1.2	-	1.32	-
ANSI 52-9	13.2 kV	1.3	-	1.36	-
Polymer Suspension	≤ 15 kV	2.6	-	1.93	-

As the Soviet Union indicated that some distribution insulators were damaged (resulting in power lines dropping to ground) during their high-altitude nuclear tests in 1962, the Russians developed the capability to perform power-on tests on power line insulators. This testing is very difficult, but it was decided by the EMP Commission that such testing should be done for E1 HEMP waveforms.

Appendix 1: HEMP Impacts on Distribution Infrastructure

Lab experiments with fast rising (E1-like HEMP waveforms) were performed for a set of Russian glass and porcelain insulators. The main emphasis for these experiments was the fact that the tests were performed, both with no power on the insulators and also with the insulators energized, with a portion of an AC waveform up to 1,000 amperes. Tests performed power off showed fairly repeatable results for multiple pulses. When power on testing was performed a few of the insulators were physically damaged by the follow-on power. In addition there was substantial degradation of the performance of the insulators even after one test shot as shown in Table A-1-2.

Table A-1-2. Peak voltage of flashover for insulators under operational voltage [13].

Number of insulator	Voltage of overlapping, kV			Notes
	First overlap	Second overlap	Third overlap	
1	370	360	340	-
2	400	390	360	-
3	360	360	330	Destroyed after third test
4	370	320	280	-
5	380	360	330	-
6	390	380	340	-

It is likely that the mechanism for destruction has to do with small defects in the manufacture of the insulators. The Russian experimental team tried to determine whether these defects were present before the testing, but they were not able to find a simple way to evaluate this aspect.

An important aspect of the multiple flashover testing under power is that while large numbers of E1 HEMP pulses are not expected to expose the U.S. power grid, lightning pulses occur in many locations in the U.S. and could therefore expose many insulators to previous impulses without causing noticeable failures. Thus a future E1 HEMP pulse could be the second or third pulse that some insulators will observe.

While this Russian test data is very dramatic, the tests were performed on Russian-manufactured insulators, and statistical damage data were not obtained due to limitations in test time and funding. More work is needed to determine whether the damage aspect is a real concern in the U.S., and if so, with which types of insulator designs. It is clear however, that flashovers of U.S. insulators can occur at E1 HEMP voltage levels much lower than previously thought, and therefore some consideration of mitigation measures are needed, especially near the substations where the follow-current will be high.

Distribution Transformers

During the ORNL power system studies during the 1980s, tests were performed to examine the possibility of E1 HEMP damage to distribution step-down transformers that can be found in the U.S. power grid. This testing included 19 samples of 7.2 kV/25 kVA power distribution transformers, using E1 HEMP like pulses. Damage that occurred was usually from dielectric breakdown within the windings – pinhole damage.

The ORNL test results indicated that failures occurred when the peak fast pulse voltage was between 264 and 304 kV. No damage occurred for peak pulses of 290 and 296 kV, so there appears to be some variability within the group of 19 transformers, although the variation is not that great. When lightning surge arresters were added to the transformers, no damage was noted up to the capability of the pulser (which was 1000 kV). The conclusion reached by the test team, however, indicated that standard surge arresters mounting procedures often include a long wire lead to the transformer, and this method of mounting might not allow for the lightning surge arrester to protect the transformer from fast pulses. Also, not all areas of the U.S. use lightning protection on distribution transformers (e.g. coastal California).

Failure levels beginning at 264 kV for this type of distribution transformer are fairly high as many of the E1 HEMP transients are expected to be in the range of 200 to 300 kV. The presence of surge arresters for lightning should certainly raise this level substantially, so the main issues are to evaluate the different types of surge arresters used in the U.S. and how they are mounted on distribution transformers.

Appendix 2: High Frequency Protection Concepts for E1 HEMP and IEMI

This section examines the impacts to the power system due to E1 HEMP and IEMI and indicates in general how high frequency protection concepts can be applied to harden power system assets against both threats.

High Voltage Substation Controls and Communications

The control building contains critical electronic equipment, such as safety relays, for ensuring the proper operation of a substation. These buildings and the cables that run from these buildings to the sensors and circuit breakers in the high-voltage yard are ideal for applying standard high frequency ($f > 1$ MHz) shielding, grounding, bonding and cable protection technologies.

The major effort suggested here is to determine the most cost-effective means of providing this protection against E1 HEMP and IEMI. It is clear that the best approach for the existing grid assets is to apply facility protection as opposed to purchasing new equipment hardened directly against the highest environment levels expected for E1 HEMP and/or IEMI.

Power Generation Facilities

Power generation facilities are very similar to high-voltage substations except that these facilities are manned, providing the ability to deal with malfunctions on a more rapid basis. They also will have additional types of electronics that are similar to industrial controls for moving fuel and controlling the generation of electricity. These controls may well be more sensitive to high-frequency transients such as E1 HEMP or IEMI than the electronics in a high-voltage substation.

In order to evaluate this category of facility, it is recommended that several specific types of generation plants (nuclear, coal, natural gas, etc.) be evaluated in terms of the coupling of E1 HEMP into above ground and buried control cables with major attention given to the generator control centers. This will enable more realistic evaluation of the E1 HEMP and IEMI voltages and currents expected at electronics controlling the power generation processes.

When the analyses are completed, standard high-frequency protection methods will be evaluated to determine which methods are most cost-effective for application to an actual generation facility.

Power Control Centers

Power control centers are considerably different than locations containing high-voltage transformers and controls. In the control centers, PCs are used to monitor, control and communicate with the substations and power generators that control the operation of the grid. These facilities resemble computer centers with networked PCs and real time displays.

The major concerns for these centers include the coupling of significant E1 HEMP transients on power and communications cables entering the facility from the outside. In addition, attention must be directed to the penetration of E1 HEMP and IEMI fields into the control center itself. Based on the design and geometry of typical control centers, a program of measurement of shielding effectiveness should be done. In addition the geometry of cables with power and communications entering the facilities should be analyzed. After this information is obtained, assessments of the vulnerability and the need for hardening will be completed.

Distribution Line Insulators

For the threat of E1 HEMP on distribution line insulators, additional research is required before the final approach for protection can be considered. First it is necessary to obtain statistical test data on the flashover and damage of U.S. power line insulators for E1-like voltage pulses while the insulators are powered by a typical supply voltage and current. The data obtained from the Russian testing is interesting, but may not be relevant to the vast majority of insulators in place in the U.S. at this time.

The lead option for protection of these distribution insulators is the placement of line to ground lightning surge arresters within 1 mile of the substation to ensure that the fault currents sensed at the substation are small enough to avoid tripping. In order for this protection approach to be effective, it will be necessary to test the efficiency of typical 100 kV BIL arresters for E1 HEMP voltage waveforms.

There is no protection activity required for IEMI related to power line insulators.

Distribution Transformers

Based on the E1 HEMP injection testing done by Oak Ridge in the 1980s, the main issue regarding the vulnerability of distribution transformers is whether lightning protection was present. In addition an issue had been raised concerning the mounting of the lightning protection and whether the effectiveness of the lightning surge protectors for E1 HEMP would be impacted by the mounting procedure.

A laboratory test program is recommended to examine the effectiveness of standard distribution transformer lightning surge arresters against E1 HEMP waveforms. This testing should also examine whether there are any issues involved in the mounting methods for lightning that could affect the protection afforded to E1 HEMP.

There are no activities required for the protection of distribution transformers from IEMI.

Appendix 3: Framework for Determining Pandemic Response Actions Based on Severity

The World Health Organization uses six phases to describe the extent of geographic spread of the virus. However, even at the highest, Phase 6 pandemic, the current A/H1N1 outbreak has a moderate degree of severity in the vast majority of cases, and does not require that response plans be implemented at the highest levels. It has become apparent that a measure of severity, in addition to geographic spread, is needed to help ensure our response plans are triggered at the appropriate times. Health authorities are being urged to develop such a severity measure.

In the meantime, this Advisory provides a framework for implementing plans under mild, moderate, and severe scenarios.

The following describes the typical actions entities would take to respond to a pandemic scenario, grouped into 5 general categories.

Typical Response Actions	
Monitor Situation	Monitor the global situation, and impacts on the local community and employees. Monitor employee absentee rates. Decide response actions. Train additional staff in preparation to maintain essential operations
Communicate	Communicate with employees, suppliers and customers, stakeholders, other interdependent critical infrastructure sectors, state, provincial, and local health authorities. Consider the impact on employee families.
Control Infection	Limit the spread through personal hygiene, workplace screening and cleaning, personal protective equipment, work from home capability, social distancing (e.g. workplace screening, visitor and travel restrictions, return to work policies), anti-virals and vaccine.
Support Employees	Provide guidance to managers and staff, provide medical and psychological support. Consider the impact on employee families and measures to support them.
Maintain Essential Operations	Defer or cease non-essential work, re-deploy staff. Monitor and adjust response actions as required. Plan for subsequent waves.

Appendix 3: Framework for Determining Pandemic Response Actions Based on Severity

Table 1 below maps these response actions against 4 stages that would prompt increasing levels of action as the pandemic worsens:

- Routine
- Enhanced
- Advanced
- Full Activation

TABLE A-3-1: Typical Response Actions

	Monitor Situation	Communicate	Control Infection	Support Employees	Maintain Essential Operations
Routine	Normal	Normal	Normal	Normal	Normal
Enhanced	Periodic updates from health authorities	Periodic updates to all staff Limited sector-wide notifications from NERC	Consider enhanced procedures	Consider enhanced support for managers to make decisions	Normal
Advanced	Frequent updates from health authorities Monitor employee absentee rates	Frequent updates to all staff Periodic sector-wide notifications from NERC	Confirm anti-viral priorities and consider distribution in consultation with health authorities Confirm vaccine priorities to support essential business	Enhanced support for managers to make decisions re: staff and their families, close contact situations	Essential business plus regulatory requirements only
Full Activation	Daily updates from health authorities Monitor employee absentee rates	Daily updates to all staff Frequent sector-wide notifications from NERC	Decide anti-viral distribution in consultation with health authorities Prepare to support requirements by state, provincial and local agencies/governments to identify critical workers for prioritized distribution of vaccine when available	Enhanced support for managers to make decisions re: staff prioritization	Essential business only

Table A-3-2 describes how the response actions in Table 1 would be implemented through mild, moderate and severe absenteeism scenarios. The table is intended to help guide decisions to take the right action at the right time. Implementing response actions too early may seem like the prudent thing to do, but it will consume resources that might best be held until they are really needed. It can also reduce overall capability as time goes on. For example, maintenance activities cannot be deferred indefinitely. Implementing response actions too late can also have negative consequences. Employees may be placed at greater risk or may feel neglected, particularly as they learn of other companies taking action.

While Table A-3-2 has been developed with a pandemic scenario in mind, entities may find it to be a useful framework for managing any emergency that could affect the availability of staff needed to maintain continuity of operations. Table 2 illustrates how the severity scenarios correspond to increasing levels of worker absenteeism, recognizing that absenteeism is influenced by a number of complex factors, such as:

- The likelihood of worker contact with the virus, either in the community or at work (e.g. rate at which the virus is spreading, contagion period)
- Severity of the illness (intensity, duration, extent to which hospitalization is required)
- Mortality rate (provided by the Center for Disease Control as the vertical axis of Table 2)
- Worry and fear
- Social distancing measures (e.g. limiting visitors and non-essential staff in the workplace, school closures, travel restrictions)

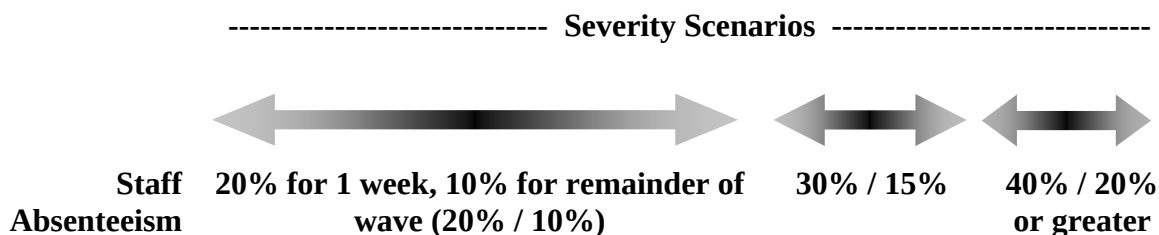
The absentee rates are grouped into 3 scenarios. Health authorities may soon develop a science-based quantitative severity index to measure these scenarios represented by the horizontal axis of Table 2. While this will be helpful, emergencies are managed locally and entities will need to decide appropriate response actions by considering local circumstances affecting their community and the potential impact on workers and their families.

- MILD: Absentee rates of up to 20% for a week of the pandemic wave, 10% for the rest of the wave.
- MODERATE: Absentee rates of up to 30% for a week of the pandemic wave, 15% for the rest of the wave.
- SEVERE: Absentee rates of up to 40% or greater for a week of the pandemic wave, 20% for the rest of the wave.

Appendix 3: Framework for Determining Pandemic Response Actions Based on Severity

TABLE A-3-2: Pandemic Influenza Response Triggers

CDC Mortality Rate (% Case Fatalities)	SEVERE ≥ 2.0%	5	Full Activation	Full Activation	Full Activation	Full Activation	Full Activation
	MODERATE 0.5% - < 2.0%	4	Advanced	Advanced	Advanced	Advanced	Full Activation
		3	Advanced	Advanced	Advanced	Advanced	Full Activation
	MILD < 0.5%	2	Enhanced	Enhanced	Enhanced	Advanced	Full Activation
		1	Routine	Routine	Enhanced	Advanced	Full Activation
				MILD			MODERATE



Appendix 4: Additional References on GMD Events

1. P. R. Barnes and J. W. Van Dyke, "Potential Economic Costs From Geomagnetic Storms," Geomagnetic Storm Cycle 22: Power System Problems on the Horizon, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0357-4-PWR, 1990.
2. V. D. Albertson, "Geomagnetic Disturbance Causes and Power System Effects," Effects of Solar-Geomagnetic Disturbances on Power Systems, Special Panel Session Report, IEEE PES Meeting, 90TH0291-5 PWR, July 12, 1989.
3. Dan Nordell et al., "Solar Effects on Communications," Geomagnetic Storm Cycle 22: Power System Problems on the Horizon, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0357-4-PWR, 1990.
4. Robert J. Ringlee and James R. Stewart, "Geomagnetic Effects on Power Systems," IEEE Power Eng. Rev. 9(7), (July 1989).
5. P. R. Gattens et al., "Investigation of Transformer Overheating Due to Solar Magnetic Disturbances," Effects of Solar-Geomagnetic Disturbances on Power Systems, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0291-5 PWR, 1989.
6. J. D. Aspnes and R. P. Merritt, "Effect of DC Excitation on Instrument Transformers, Geomagnetically Induced Currents," IEEE Trans. Power Apparatus and Syst. PAS-102 (11), 3706-3712 (November 1983).
7. D. H. Boteler et al., "Effects of Geomagnetically Induced Currents in the B. C. Hydro 500 kV System," IEEE Trans. Power Delivery 4(1), (January 1989).
8. IEEE Power System Relaying Committee, Working Group K1.1, "The Effects of Solar Magnetic Disturbances on Protective Relaying," Geomagnetic Storm Cycle 22: Power System Problems on the Horizon, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0357-4-PWR, 1990.
9. D. Larose, "The Hydro-Québec System Blackout of March 13, 1989," Effects of Solar-Geomagnetic Disturbances on Power Systems, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0291-5 PWR, 1989.
10. D. A. Fagnan, P. R. Gattens, and R. D. Johnson, "Measuring GIC in Power Systems," Geomagnetic Storm Cycle 22: Power System Problems on the Horizon, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0357-4-PWR, 1990.

Appendix 4: Additional References on GMD Events



11. V. D. Albertson, “Measurements and Instrumentation for Disturbance Monitoring of Geomagnetic Storm Effects,” Effects of Solar-Geomagnetic Disturbances on Power Systems, Special Panel Session Report, IEEE PES Summer Meeting, IEEE Publication 90TH0291-5 PWR, 1989.
12. L. Bolduc et al., “Currents and Harmonics Generated in Power Transformers By DC Polarization,” presented at the meeting of the IEEE T&D Working Group on Geomagnetic Disturbances and Power System Effects, IEEE PES Summer Meeting, Minneapolis, Minn., July 18, 1990.

HILF Steering Committee and Task Force Rosters

High-Impact Low-Frequency Event Workshop Steering Committee

Executive Sponsors

William Bryan	Deputy Assistant Secretary	U.S. Department of Energy
Michael Assante	VP and Chief Security Officer	NERC

Chairs

Scott Moore	Vice President of Transmission	American Electric Power
Robert Stephan	Former Assistant Secretary for Infrastructure Protection in the National Protection and Programs Directorate	U.S. Department of Homeland Security

Members

Stuart Brindley	<i>Former</i> Manager - Training & Emergency Preparedness	IESO
Tom Bowe	Executive Director, Reliability Integration	PJM Interconnection
Tom Burgess	Director, FERC Policy & Compliance	FirstEnergy
Jerry Dixon	Director of Analysis	Team Cymru Research
Michael Frankel	Executive Director	U.S. EMP Commission
Sam Holeman	System Operating Center	Duke Energy Corporation
John Kappenman	Principal	Storm Analysis Consultants
Robert McClanahan	Vice President, Information Technology	Arkansas Electric Cooperative
Julie Palin	Partner	Business Recovery Solutions LLC
William Radasky	President and Managing Engineer	Metatech Corp.

Special Advisors & Keynotes to the Workshop

Melissa Hathaway	Former Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils	Office of the President of the United States (Former) Hathaway Global Strategies (Present)
------------------	---	---

Staff

Aaron Bennett	Engineer of Reliability Assessments	NERC
Kenneth Friedman	Senior Policy Advisor	U.S. Department of Energy
Mark Lauby	Director, Reliability Assessments and Performance Analysis	NERC
Kelly Ziegler	Project Manager – HILF Effort	Consultant to NERC

High-Impact Low-Frequency Event: Coordinated Attack Ad Hoc Task Force

Chairs

Michael Assante	Vice President and Chief Security Officer	NERC
Robert Stephan	Former Assistant Secretary for Infrastructure Protection in the National Protection and Programs Directorate	U.S. Department of Homeland Security / Dutko Worldwide

Members

Jeff Dagle	Chief Electrical Engineer	Pacific Northwest National Labs
Larry Bugh	Chief Security Officer	ReliabilityFirst Corporation
Howard Lipson	Senior Member of the Technical Staff	CERT/SEI, Carnegie Mellon University
Philip Muhlmeister	Co-Chairman, Energy, Climate, and Transportation	ICF International
Zachary Tudor	Program Director	SRI International
Joe Weiss	Principal	Applied Control Systems
Jeff Rosenberg	Senior Research Associate	Dutko Worldwide

Staff

Aaron Bennett	Engineer of Reliability Assessments	NERC
Rhonda Dunfee	Control Systems Security Analyst	U.S. Department of Energy
Mark Lauby	Director of Reliability Assessments and Performance Analysis	NERC
Matthew Light	Infrastructure Systems Analyst	U.S. Department of Energy
Kelly Ziegler	Project Manager – HILF Effort	Consultant to NERC

High-Impact Low-Frequency Event: Pandemic Ad Hoc Task Force

Chair

Julie Palin	Partner	Business Recovery Solutions
-------------	---------	-----------------------------

Members

Dave Francis	Director Business Continuity	MISO
David Baumken	Manager, Emergency Preparedness and Line of Business Risk Assessment	HydroOne
Sam Holeman	System Operating Center	Duke Energy
Kenneth Flechler	VP Environmental Health & Safety	Pike Energy
Thaddeus Kwiatkowski	Manager Business Recovery Services	American Electric Power
Joel Wise	Manager, Reliability Operations	Tennessee Valley Authority

Staff

Kelly Ziegler	Project Manager – HILF Effort	Consultant to NERC
Aaron Bennett	Engineer of Reliability Assessments	NERC
Robin Henderson		U.S. Department of Energy

High-Impact Low-Frequency Event: GMD/EMP Ad Hoc Task Force

Chairs

John Kappenman	Principal	Storm Analysis Consultants
William Radasky	President and Managing Engineer	Metatech

Members

Nick Abi-Samra	Senior Technical Executive	EPRI
Michael Frankel	Executive Director	U.S. EMP Commission
Mark Kuras	Senior Engineer	PJM Interconnection
Steven Naumann	Vice President, Wholesale Market Development	Exelon
Barry Lawson	Manager, Power Delivery	NRECA

Staff

Michael Assante	Vice President and Chief Security Officer	NERC
Aaron Bennett	Engineer of Reliability Assessments	NERC
Kenneth Friedman	Senior Policy Advisor	U.S. Department of Energy
Mark Lauby	Director of Reliability Assessments and Performance Analysis	NERC
Kelly Ziegler	Project Manager – HILF Effort	Consultant to NERC

