

Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment

February 5th, 2019
Version 2.2

Developed by the
National Coordinating Center for
Communications (NCC)

National Cybersecurity and Communications Integration Center
Arlington, Virginia

Executive Overview

This document provides guidelines to assist federal, state, and local officials and critical infrastructure owners and operators to protect mission essential equipment against electromagnetic pulse (EMP) threats. It was created to help fulfill the Secretary of Homeland Security's responsibilities to:

- "... provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." [*Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience*]
- "... ensure ... the necessary combination of hardness, redundancy, ... to obtain, to the maximum extent practicable, the survivability of NS/EP {national security/emergency preparedness} communications ..." [*Executive Order 13618, Assignment of National Security and Emergency Preparedness Communications Functions*]
- "... be the focal point within the Federal Government for all EMP technical data and studies concerning telecommunications." [*Title 47 Part 215 of the Code of Federal Regulations (CFR)*]

These guidelines also respond to the U.S. Congressional EMP Commission's recommendation that the "Department of Homeland Security should play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences." [Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures, page 181, 2008]. The Department of Homeland Security (DHS) takes seriously the findings of this Commission, such as:

"The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about an EMP attack generated by a high-altitude nuclear weapon as a tactic by which the Soviet Union could suppress the U.S. national command authority and the ability to respond to a nuclear attack—and thus negate the deterrence value of assured nuclear retaliation. Within the last decade, newly-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the United States. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause widespread, long-lasting damage to critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population." [*Assessing the Threat from Electromagnetic Pulse (EMP), Executive Report, July 2017*]

There are four EMP Protection Levels defined herein, as outlined in Table 1. These levels were initially developed at the request of the federal Continuity Communications Managers Group (CCMG), but are applicable to any organization that desires to protect its electronics and critical infrastructures. For additional background on EMP, a set of reports can be found at "www.firstempcommission.org" that includes information about high-altitude EMP (HEMP), Source Region EMP (SREMP), and Intentional Electromagnetic Interference (IEMI) EMP.

Table 1. Four EMP Protection Levels for Infrastructure and Equipment

Level 1: Lowest cost; longer mission outages permitted	Level 2: Only hours of mission outages are permitted	Level 3: Only minutes of mission outages are permitted	Level 4: Only seconds of mission outages permitted
<ul style="list-style-type: none"> • Unplug power, data, and antenna lines from spare equipment where feasible. • Turn off equipment that cannot be unplugged and is not actively being used. • Use at least a lightning rated surge protection device (SPD) on power cords, antenna lines, and data cables; maintain spare SPDs. • Have either EMP protected backup power or a generation source that is not connected to the grid with one (1) week of on-site fuel or equivalent (e.g., renewable source). • Wrap spare electronics with aluminum foil or put in Faraday containers. • Use priority phone services like GETS, WPS (for cell phones), and TSP; join SHARES if applicable (see Appendix C). • Consider land mobile radios with standalone capabilities, HF radios, and FirstNet. • Store one week of food, water, and other supplies for personnel. • Use battery operated AM/FM/NOAA radios to receive Emergency Alerts. 	<p>In addition to Level 1 ...</p> <ul style="list-style-type: none"> • Use EMP-rated SPDs on power cords, antenna lines, and data cables to protect critical equipment. • Use on-line/double-conversion uninterruptible power supplies (UPS) or a high quality line interactive UPS. • Use fiber optic cables (with no metal); otherwise use shielded cables, ferrites, and SPDs. Note: shielded racks, rooms or facilities may be more cost-effective than hardening numerous cables. • Use EMP protected backup power that is not vulnerable to EMP coupled through the power grid. • Implement EMP protected, high frequency (HF) voice and email for long-distance communications. • Consider geosynchronous (GEO) orbit satellite services, like BGAN. Avoid low-earth orbit (LEO) satellite services. Use terminals that are EMP resilient. • Consider shortwave radio for situational awareness. 	<p>In addition to Level 2 ...</p> <ul style="list-style-type: none"> • Use International Electrotechnical Commission (IEC) EMP and IEMI protection standards (IEC SC 77C series, see Appendix F). • Shielding should be 30+ dB of protection through 10 GHz. • Use EMP shielded racks, rooms, or facilities to protect critical computers, data centers, phone switches, industrial and substation controls and other electronics. • Use “Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures” from EMP Commission for grid and undersea cable protection planning. Use 85 V/km for CONUS E3 threat. • Use EMP tested SPDs and equipment. • Institute IEC level hardness maintenance & surveillance (HM/HS). • Have 30 days of EMP protected power/fuel. • Store 30 days of food, water, and critical supplies and spares. • Use time-urgent EMP resilient comms, like X, Ku and Ka satellite, and either HF groundwave or Automatic Link Establishment (ALE) HF. 	<p>In addition to Level 3 ...</p> <ul style="list-style-type: none"> • Use Military EMP Standards (like MIL-STD-188-125-1 and MIL-HDBK-423), and 80+ dB hardening through 10 GHz. • Use EMP shielding in rooms, racks, and buildings as needed to protect critical equipment. • Use EMP protected double-door entryways. • Validate per Military guidelines, like Test Operations Procedure (TOP) 01-2-620 HEMP. • Have 30+ days of Military Standard protected power and fuel, plus alternate generation source (renewables preferred). • Consider double surge protection on critical external lines entering EMP protected areas. • Consider using communications systems/networks that are designed to meet Military EMP standards, like: Advanced EHF (AEHF) satellite, EMP protected fiber optic networks, and EMP protected radios. • Institute ongoing Military Standard HM/HS programs.

Note: These guidelines do not endorse any referenced product, company, service, or information external to DHS.

Level 1 begins with low-cost methods and best practices to help protect critical infrastructure from severe damage. An important aspect of Level 1 protection is ensuring that personnel have backup power and the food, water, and other essential supplies needed to operate and maintain their mission-critical systems, given that normal services and supply chains are likely to be disrupted in some reasonable scenarios for a week (or longer).

Level 2 guidelines are based on using EMP-capable filters and surge arresters on power cords, antenna lines, and data cables, as well as installing fiber optics and ferrites, where possible, to protect critical equipment. These will mitigate the majority of EMP equipment vulnerabilities when EMP facility shielding is not feasible and are expected to be the most cost-effective approach for hardening limited equipment in facilities. Levels 1 and 2 are for organizations where days or hours of mission interruptions can be tolerated and for which “cost to harden” is a critical factor.

Level 3 guidelines are appropriate for organizations, facilities, and systems that cannot tolerate more than a few minutes of mission outage due to EMP, in order to effectively protect life, health, and security. The International Electrotechnical Commission (IEC) EMP and IEMI protection standards (IEC SC 77C series, see Appendix F), serve as the foundation for planning and protecting critical infrastructures and equipment that are in this category. For EMP Protection Levels 3 (and 4), electromagnetically shielded racks and rooms are used to prevent electromagnetic (EM) fields and currents from reaching mission critical equipment. At Level 3, shielding against high frequency EMP should provide at least 30 dB of protection through 10 GHz (in other words, the EMP field strength should be attenuated by a factor of at least 97% by the shielding).

Level 4 guidelines are for organizations/missions/systems that cannot tolerate more than a few seconds of outage and where immediate life and safety are at stake. U.S. Military EMP Standards supporting critical and time-urgent command, control, communications, computer, and intelligence (C4I) missions serve as the foundation for planning and protecting critical infrastructures and equipment in this category. Examples of missions where this apply are nuclear command and control and Presidential conferencing. However, this level of protection may also be appropriate for non-military related systems and missions, such as nuclear power plant controls, medical life-support systems, and time-critical air traffic control functions. At Level 4, shielding against high frequency EMP should provide at least 80 dB of protection through 10 GHz (in other words, the EMP field strength should be attenuated by a factor of at least 99.99% by the shielding).

Levels 3 and 4 also use hardness maintenance and hardness surveillance (HM/HS) programs to verify that the EMP shields are effective and that the EMP barrier’s integrity is maintained over the life cycle of the system. A properly designed barrier with penetration protection for all power, data and antenna cables will make equipment behind it safe from wide variations of external EM fields, including HEMP, SREMP, and IEMI threats. Level 3 allows the use of commercial standards for designing protection and performing HM/HS in a more cost-effective manner compared to Level 4.

Given the growing risks associated with EMP and IEMI related threats, it is hoped that organizations that support essential functions will quickly achieve at least a Level 1 or 2 capability. The costs of achieving Level 3 or 4 protection are small when compared to the life and mission risks averted. For example, Level 3 protection can be achieved for many sites for far less than 1% of the system cost. Even the most expensive Level 4 protections are only expected to cost 1% to 5% of overall new system costs, if planned from the onset versus retrofitted into existing systems.

Acknowledgements and Authors

The *Electromagnetic Pulse (EMP) Protection Guidelines* were initially developed by Dr. George H. Baker, based on his previous work where he led the Department of Defense program to develop EMP protection standards (such as MIL-STD-188-125, MIL-HDBK-423, and MIL-STD-2169B) while at the Defense Nuclear Agency (DNA) and the Defense Threat Reduction Agency (DTRA). He is currently serving as a consultant to the Department of Homeland Security (DHS) and is Professor Emeritus of Applied Science, James Madison University (JMU). He presently serves on the Board of Directors of the Foundation for Resilient Societies, the Board of Advisors for the Congressional Task Force on National and Homeland Security, the JMU Research and Public Service Advisory Board, and the North American Electric Reliability Corporation GMD Task Force. From 2002-2009 and again from 2016-2017, he also served as a Senior Scientist to the Congressional EMP Commission.

A second principal author is Dr. William A. Radasky. Dr. Radasky started his career as a research engineer at the Air Force Weapons Laboratory (AFWL) in 1968 working on the theory of the EMP. In 1984 he founded Metatech Corporation (www.metatechcorp.com) in Goleta, California where he is currently President and Managing Engineer. He has published over 500 technical papers, reports and articles dealing with electromagnetic interference (EMI) and protection. In 1989, Dr. Radasky began his volunteer work with the International Electrotechnical Commission (IEC) developing reports and standards to protect commercial equipment and systems against the threats of high-altitude electromagnetic pulse (HEMP) and Intentional Electromagnetic Interference (IEMI). He led the development of 22 publications as Chairman of IEC SC 77C since 1991. In addition, he helped to coordinate all of the electromagnetic compatibility (EMC) work of the IEC as Chairman of the Advisory Committee on EMC from 1996 to 2008. He also organized and presented many workshops for the IEC dealing with EMC in general and IEMI. In 2004 he received the Lord Kelvin Award from the IEC for exceptional contributions to international standardization. This award is presented annually to one individual out of 15,000 active participants within the IEC.

Dr. Radasky and his team of EMP experts developed the Electromagnetic Assessment Tool (EMAT) for the Department of Homeland Security. The EMAT and the related Infrastructure Mapping Tool (IMT) were used to develop many of the graphics and assessments in this report.

Dr. James L. Gilbert, who serves as the Chief Scientist at Metatech, has helped to lead Metatech's efforts in the development and use of analytic and numerical techniques to model electromagnetic and plasma effects produced by nuclear and natural radiation. Much of his work over the last 45+ years has dealt with the protection of electronic systems from the EMP effects produced by nuclear explosions. He is the principal developer of the Source Region EMP (SREMP TAPS) and EMAT codes and has served as a consultant to DHS in modeling solar and EMP effects for many years.

Many others have worked to develop the assessments and information used in this document, most notably: Rob Benish and Mark Jones of Jacobs Technology Inc. (past and current editorial support), Dr. Edward Savage of Metatech, Dr. Don Morris-Jones, Mr. Seth Sobel and Mr. Matthew Jackson (who developed many of the EMAT outputs used herein), Mr. Steven Karty (technical contributor), Mr. Bronius Cikotas (a leader in the EMP community for decades and mentor to Dr. Baker prior to passing away in 2014), and Kevin Briggs (the DHS/NCC Project Officer and Principal Editor for this report). Questions on this report should be sent to: Kevin.Briggs@hq.dhs.gov.

Table of Contents

Executive Overview ii

Acknowledgements and Authors v

List of Figures..... vii

List of Tables..... ix

Document Change History x

1. INTRODUCTION 1

 1.1. Document Purpose and Audience 1

 1.2. Scope 4

 1.3. HEMP and GMD Characteristics 5

 1.4. HEMP, SREMP, and IEMI Risks..... 12

2. EMP PROTECTION AND RESILIENCE CONSIDERATIONS 25

 2.1. Prioritizing EMP Mitigation Efforts..... 25

 2.2. IEC Technical Design Standards..... 26

 2.3. Surge Protective Device (SPD) Selection 29

 2.4. Use of Common Building Materials to Increase EMP Shielding..... 31

3. LEVEL 1 EMP GUIDELINES 34

4. LEVEL 2 EMP GUIDELINES 36

5. LEVEL 3 EMP GUIDELINES 41

 Calculated Level 3 Mitigation Effects 42

6. LEVEL 4 EMP GUIDELINES 45

7. HEMP MODEL MITIGATION RESULTS..... 65

 7.1. Model Assumptions..... 65

 7.2. Model Results..... 66

8. NEXT STEPS 70

Appendix A. EMP PROTECTION TEST AND ACCEPTANCE CRITERIA A-1

Appendix B. EMP PROTECTION VENDORS AND SERVICES B-1

Appendix C. PRIORITY SERVICES (GETS, WPS, FIRSTNET, TSP, AND SHARES)..... C-1

Appendix D. EXCERPTS FROM 2017 BRIEF TO INFRAGARD SUMMIT D-1

Appendix E. ACRONYMS AND EXPLANATION OF DECIBELS..... E-1

Appendix F. IEC SC 77C BIBLIOGRAPHY..... F-1

Appendix G. REFERENCES..... G-1

Appendix H. EXAMPLE EMP IMPLEMENTATION FOR HF COMMUNICATIONS SITE H-1

Appendix I. ENDNOTES I-1

List of Figures

Figure 1. Generic HEMP waveform (ref. Meta-R-324)	4
Figure 2. IEC Standard E1 Waveform (ref. IEC 61000-2-9)	5
Figure 3. 100 Year geomagnetic storm – 50 degree GMD scenario (ref. Fig. 3-25)	7
Figure 4. 100 Year geomagnetic storm – 45 degree GMD scenario (ref. Fig. 3-26)	8
Figure 5. Normalized E3 Heave E field waveform from the 150 km burst height scenario	9
Figure 6. Normalized E peak contour pattern from the 150 km burst case	10
Figure 7. B-dot Magnetic Field Peak contour pattern from a 300 km burst case (from EMAT)	10
Figure 8. Frequency ranges of Lightning, HEMP, and IEMI	12
Figure 9. Potential disruption for 100' Ethernet-connected equipment from 100 kT HEMP	13
Figure 10. Potential disruption for 100' Ethernet-connected equipment from 30 kT HEMP	14
Figure 11. HEMP picture from the Fishbowl Starfish Prime at 0 to 15 seconds.	15
Figure 12. Generation of Source Region EMP (SREMP) from a ground burst	17
Figure 13. Potential 10 kT SREMP disruption of AC/DC adapters	18
Figure 14. Potential 10 kt SREMP Upset/Damage to FM Radio Transmission	19
Figure 15. Potential 10 kt SREMP Upset/Damage to Cellular Handsets	19
Figure 16. Typical IEMI interaction of radiated fields	22
Figure 17. DIEHL Munitions damped sine IEMI generator	23
Figure 18. Laboratory hyperband pulse generator used in Russia	23
Figure 19. RADAN 303B hyperband generator used in Sweden	23
Figure 20. High intensity JOLT hyperband generator used in the United States	24
Figure 21. Effect of Building Materials on EMP Attenuation	32
Figure 22. Organization of the current IEC SC 77C publications	41
Figure 23. Protective effects on cordless telephones with recommended 30 dB shielding	43
Figure 24. Protective effects on a 100' Ethernet cable with recommended 30 dB shielding	44
Figure 25. Protective effects on a Plain Old Telephone Service Line with 30 dB shielding	44
Figure 26. Low-risk EMP barrier protection for facilities (per MIL-STD-188-125-1)	47
Figure 27. Typical cable POE protection design	49
Figure 28. Commercial electric power POE protection	50
Figure 29. Power line POE protection using a motor-generator set	51
Figure 30. Entryway using two doors separated by a WBC	51

Figure 31. Sample door with gaskets protecting against EMP threats	52
Figure 32. Typical waveguide-below-cutoff (WBC) piping POE protective design for E1 HEMP	53
Figure 33. Typical waveguide-below-cutoff ventilation POE protective design for E1 HEMP	54
Figure 34. Shield barrier earth electrode system	55
Figure 35. Example receiver protector unit diagram.	58
Figure 36. Special protective volume for piping POE for E1 HEMP	60
Figure 37. Special protective volume for electrical equipment	60
Figure 38. Global barrier vs. box-level protection	62
Figure 39. Box-level hardening techniques	63
Figure 40. EMP protected conduit	64
Figure 41. Potential upset/damage of equipment connected to 100' Ethernet cable with 0 dB protection	67
Figure 42. Reduced damage with 10 dB protection to 100' Ethernet cable connected equipment	67
Figure 43. Localized damage only with 20 dB protection with 100' Ethernet cable	67
Figure 44. No damage with 100' Ethernet cable and 30 dB protection	67
Figure 45. Devastating POTS telephone damage with 0 dB protection	68
Figure 46. Significantly reduced damage with 10 dB protection	68
Figure 47. No POTS telephone damage with 20 dB protection	68
Figure 48. No POTS telephone damage with 30 dB protection	68
Figure 49. Devastating cordless telephone AC/DC adapter damage with 0 dB protection	69
Figure 50. Significantly reduced damage, but still huge with 10 dB protection	69
Figure 51. Only localized damage to cordless telephones with 20 dB protection	69
Figure 52. No cordless telephone damage with 30 dB protection	69
Figure A-1. HEMP Shielding Effectiveness Requirement	A-4

List of Tables

Table 1. Four EMP Protection Levels for Infrastructure and Equipment	iii
Table 2. E3 Heave Electric Field Strengths in V/km	9
Table 3. HEMP and GMD Comparison	11
Table 4. Some Effects of High Altitude Nuclear Detonations on Radio Systems	16
Table 5. Source Region EMP Damage and Upset Planning Factors	20
Table 6. Comparisons between IEMI threats and E1 HEMP	24
Table 7. Considerations for prioritizing infrastructures for EMP Protection	26
Table 8. EMP Induced Surges on Conductors	29
Table 9. Building shielding “rules of thumb” for E1 HEMP	33
Table 10. HEMP Specifications for Cable Runs Between Two Protected Areas	63
Table 11. Modeling Parameters Used to Calculate HEMP Damage	65
Table 12. Example HEMP Model Damage and Upset Mitigation Results	66
Table A-1. Injected Pulse Characteristics	A-1
Table A-2. Residual internal stress limits for classes of electrical POEs	A-2
Table A-3. Injected pulse characteristics and residual internal stress limits for antenna POE	A-3
Table E-1. Explanation of Decibel (dB)	E-4
Table H-1. Level 1 EMP Resilient HF Site Specific Technical Costs	H-2
Table H-2. Level 2 EMP Resilient HF Site Specific Technical Costs	H-3
Table H-3. Level 3 EMP Resilient HF Site Specific Technical Costs	H-5
Table H-4. General, Non-HF Specific EMP Requirements for Levels 1-3	H-7

Document Change History

This table identifies the major changes to the NCC's *EMP Protection Guidelines* since 2016. While the descriptive "long title" of this document has changed several times since Version 1.0 of the original *EMP Protection Guidelines* (9 October 2014), this short title, *EMP Protection Guidelines*, has stayed consistent.

Date	Version #	Change Description
12/22/2016	1.0	Initial release of the <i>EMP Protection and Restoration Guidelines for Equipment and Facilities</i> to the Federal Continuity Community Managers Group, FBI InfraGard EMP SIG Community, Appendix B companies, the reestablished Congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, and others. This document replaced and extensively revised the earlier <i>EMP Protection Guidelines for Equipment, Facilities, and Data Centers, Version 6.0, 11 May 2015</i> .
11/14/2018	2.0	Changed title to <i>Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment</i> . Additional sections were created including an Executive Overview, a Document Purpose, a Problem Background, a Scope, an EMP Protection and Resilience Considerations section, and information about FirstNet.
1/16/2019	2.1	Added or substantially changed several sections, such as: (i) Executive Overview (modifications primarily to Table 1), (ii) HEMP Characteristics (added), (iii) HEMP, SREMP, and IEMI Risks (previously just covered the Problem Background), (iv) Prioritizing EMP Mitigation Efforts (added), (v) Use of Common Building Materials to Increase EMP Shielding (added), and (vi) HEMP Model Mitigation Results (overhauled). Made a number of editorial and consistency improvements. In the appendices, added Appendix D "Excerpts from 2017 brief to InfraGard Summit", included additional vendor information, and updated the FirstNet subsection in Appendix C.
2/5/2019	2.2	Revised the <i>Executive Overview</i> and <i>Acknowledgments and Authors</i> section. Added information on IEMI risks and threats. Added Surge Protection Device guidelines for each level. Added Appendix H: Example EMP Implementation for HF Communication Site.

1. INTRODUCTION

1.1. Document Purpose and Audience

This document was initially developed to respond to: (1) a request by the federal Continuity Communications Managers Group (CCMG) for guidelines to help protect critical communications infrastructures against an EMP attack and (2) as part of the responsibilities of the Secretary of Homeland Security, as the Executive Agent for the legacy National Communications System (NCS), as fulfilled by the National Coordinating Center for Communications, under Title 47 Part 215 of the Code of Federal Regulations (CFR).¹

The purpose of these updated guidelines is to help federal, state, and local officials and critical infrastructure owners and operators to protect essential equipment against electromagnetic pulse (EMP) threats. It was created to help fulfill the Secretary of Homeland Security's responsibilities to:

- "... provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." [Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience]
- "... ensure ... the necessary combination of hardness, redundancy, ... to obtain, to the maximum extent practicable, the survivability of NS/EP {national security/emergency preparedness} communications ..." [Executive Order 13618, Assignment of National Security and Emergency Preparedness Communications Functions]
- "... be the focal point within the Federal Government for all EMP technical data and studies concerning telecommunications." [Title 47 Part 215 of the Code of Federal Regulations (CFR)]

These guidelines also respond to the U.S. Congressional EMP Commission's recommendation that the "Department of Homeland Security should play a leading role in spreading knowledge of the nature of prudent mitigation preparations for EMP attack to mitigate its consequences." [Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Critical National Infrastructures, 2008]. The Department of Homeland Security (DHS) takes seriously the findings of this Commission, such as the following information released by the Department of Defense on 8 May 2018, from the Commission's "Assessing the Threat from Electromagnetic Pulse (EMP) Executive Report":

"The critical national infrastructure in the United States faces a present and continuing existential threat from combined-arms warfare, including cyber and manmade electromagnetic pulse (EMP) attack, as well as from natural EMP from a solar superstorm. During the Cold War, the U.S. was primarily concerned about an EMP attack generated by a high-altitude nuclear weapon as a tactic by which the Soviet Union could suppress the U.S. national command authority and the ability to respond to a nuclear attack—and thus negate the deterrence value of assured nuclear retaliation. Within the last decade, newly-armed adversaries, including North Korea, have been developing the ability and threatening to carry out an EMP attack against the United States. Such an attack would give countries that have only a small number of nuclear weapons the ability to cause

widespread, long-lasting damage to critical national infrastructures, to the United States itself as a viable country, and to the survival of a majority of its population.” [Assessing the Threat from Electromagnetic Pulse (EMP), Executive Report, July 2017]

Finally, this document comports with the DHS “*Strategy for Protecting and Preparing the Homeland against Threats of Electromagnetic Pulse and Geomagnetic Disturbances*”, issued on October 9th of 2018, which states:

Extreme electromagnetic incidents caused by an intentional electromagnetic pulse (EMP) attack or a naturally occurring geomagnetic disturbance (GMD, also referred to as “space weather”) could damage significant portions of the Nation’s critical infrastructure, including the electrical grid, communications equipment, water and wastewater systems, and transportation modes. The impacts are likely to cascade, initially compromising one or more critical infrastructure sectors, spilling over into additional sectors, and expanding beyond the initial geographic regions.

EMPs are associated with intentional attacks using high-altitude nuclear detonations, specialized conventional munitions, or non-nuclear directed energy devices. Effects vary in scale from highly local to regional to continental, depending upon the specific characteristics of the weapon and the attack profile. High-altitude electromagnetic pulse attacks (HEMP) using nuclear weapons are of most concern because they may permanently damage or disable large sections of the national electric grid and other critical infrastructure control systems.

Similarly, extreme geomagnetic disturbances associated with solar coronal mass ejections (when plasma from the sun, with its embedded magnetic field, arrives at Earth) may cause widespread and long-lasting damage to electric power systems, satellites, electronic navigation systems, and undersea cables. ...

For these reasons, the potential severity of both the direct and indirect impacts of an EMP or GMD incident compels our national attention. The Department of Homeland Security (DHS) has been actively analyzing the risk of the EMP-GMD problem set since its inception. *The Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances* (hereafter referred to as the “DHS Strategy”) represents the Department’s first articulation of a holistic, long-term, partnership-based approach to confronting this challenge.

These guidelines provide recommendations to help protect critical electronic infrastructure based upon their mission importance from the following three EMP types:

- (1) High-altitude EMP (**HEMP**), from a nuclear detonation typically occurring 15 or more miles above the Earth’s surface;
- (2) Source Region EMP (**SREMP**), created when a nuclear weapon detonates at lower altitudes, especially when the detonation is at or near the surface of the earth;
- (3) Intentional Electromagnetic Interference (**IEMI**), from nearby sources such as an Electromagnetic (EM) weapon (also known as a Radio Frequency (RF) weapon (RFW)).

Collectively, these will be called by the general term “EMP” in this document, unless one of the specific EM environments is being discussed.

In addition to making recommendations on how to physically protect electronic equipment from different types of EMP, this document provides guidance on how to help ensure communications and information systems (and their supported missions) can continue to function or be rapidly restored after one or more EMP events. Hence, Appendix C contains information on priority service programs (like GETS, WPS, and TSP) as well as on the SHARES alternate communications service that can be used to support critical missions and to facilitate and coordinate restoration activities.

The document supports the concepts of resiliency and recovery. The intention is to provide different levels of protection that should allow less damage and/or loss of data as one moves to a higher level of protection. This also should result in shorter outages of the system mission.

Lastly, it is worth noting that many of the EMP protection methods presented in these guidelines can also help shield against “tapping” or monitoring telecommunications and IT equipment from the weak EM signals that they emit.

Audience

The audience for this document is all governmental and civilian officials and owners and operators of critical infrastructures, particularly those using sensitive electronics for their operations. This includes the 16 critical infrastructure sectors identified under “*Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience.*” PPD-21 advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure in the following specific sectors (see www.dhs.gov/cisa/critical-infrastructure-sectors for more information):

1. Chemical (DHS is the Sector-Specific Agency (SSA) for the Chemical Sector)
2. Commercial Facilities (DHS is the SSA)
3. Communications (DHS is the SSA)
4. Critical Manufacturing (DHS is the SSA)
5. Dams (DHS is the SSA)
6. Defense Industrial Base (Department of Defense (DOD) is the SSA)
7. Emergency Services (DHS is the SSA)
8. Energy (Department of Energy (DOE) is the SSA)
9. Financial Services (Department of Treasury is the SSA)
10. Food and Agriculture (Department of Agriculture is the SSA)
11. Government Facilities (DHS is the SSA)
12. Healthcare and Public Health (Department of Health and Human Services (HHS) is the SSA)
13. Information Technology (DHS is the SSA)
14. Nuclear Reactors, Materials, and Waste (DHS is the SSA)
15. Transportation Systems (DHS and the Department of Transportation are the Co-SSAs)
16. Water and Wastewater Systems (Environmental Protection Agency is the SSA)

1.2. Scope

This document is focused on EMP related protection and resilience of critical infrastructure and electronic assets, including communications, information technology (IT), and supervisory control and data acquisition (SCADA) equipment. Per the 2017 National Security Strategy, resilience “includes the ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks and threats to our economy and democratic system.”²

Following the above definition of resilience, this document covers the below topics for critical infrastructure providers and equipment operators based upon risk management principles:

- Protection from EMP damage
- Quick recovery from an EMP related attack
- Ability to continue to communicate and operate during an EMP event based upon maximum downtime permitted
- Test procedures to evaluate protective EMP measures
- Potential vendor EMP protection equipment
- Additional EMP related information

Route diversity and power resiliency recommendations beyond EMP protection are not covered herein except for a few very high level comments.

This report’s main focus is on protecting systems from E1 (early-time) HEMP (shown in Figure 1), the radiated SREMP, and the IEMI. All of these are fast transient EM fields and can induce voltages on cables that can damage and upset unprotected electronics connected to those cables. The E3 (late-time) HEMP, which is also shown in Figure 1, is covered briefly later in the next section.

The E2 (intermediate-time) HEMP component, between 1 μ s to 1 second in time or 1 Hz to 1 MHz in frequency, is minimally covered in this report. Taking precautions against E1 will help protect against E2 since the devices and techniques that protect against the quick rise E1 pulses typically protect against the longer E2 pulse as well. Further, the precautions that are used to prevent lightning damage are also useful to protect against E2 damage although the E2 pulse magnitude can be higher than lightning at higher frequencies. Therefore, E2 is not as significant a risk as E1 HEMP, SREMP, and IEMI and so will only be briefly discussed.

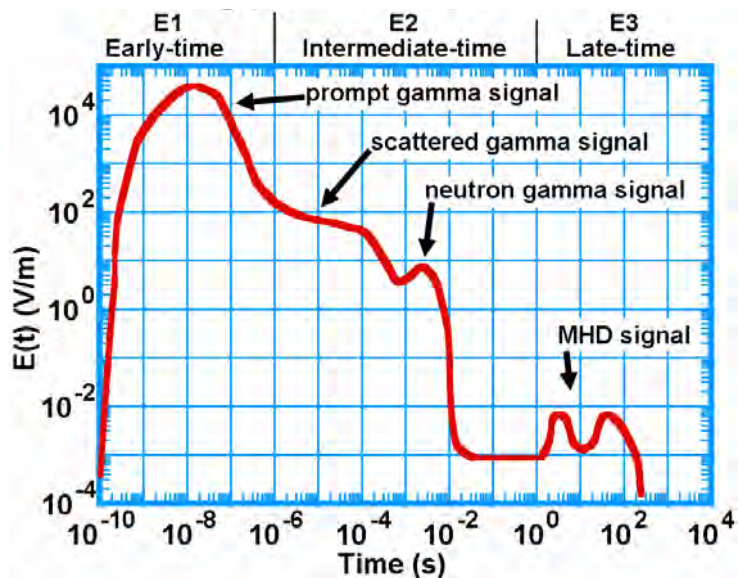


Figure 1. Generic HEMP waveform (ref. Meta-R-324)

1.3. HEMP and GMD Characteristics

E1 HEMP has a pulse that is 1 nanosecond (ns) to 1 microsecond (μs) in time or 1 MHz to several hundred MHz in frequency as shown in the “Generic HEMP waveform (ref. Meta-R-324)” figure above. Additional technical information on the E1 waveform properties from the International Electrotechnical Commission (IEC) is shown in Figure 2 below.

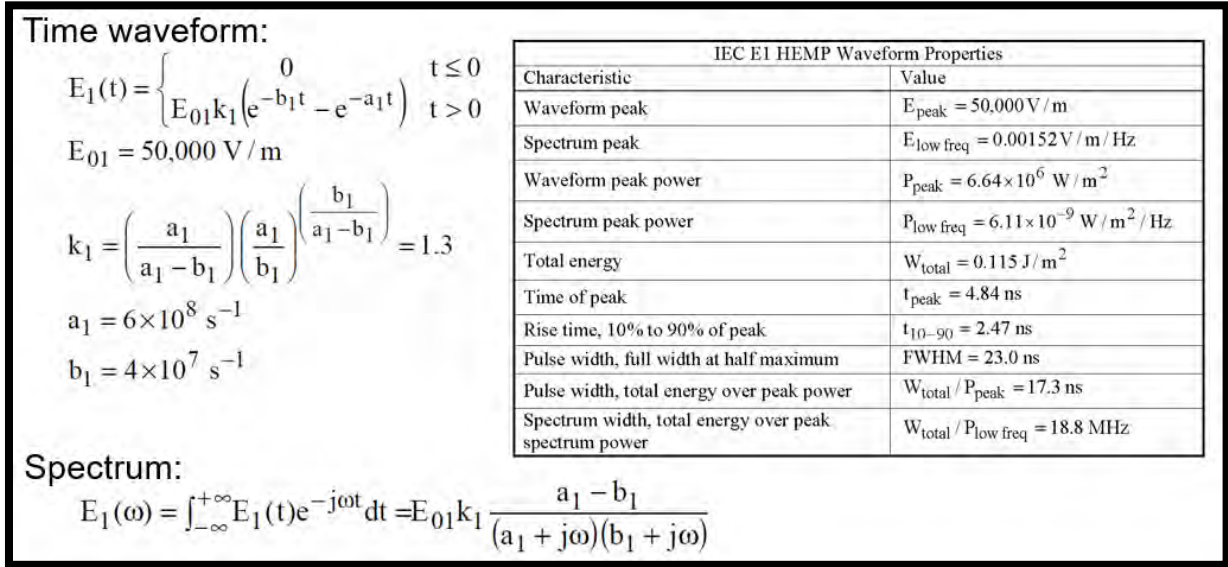


Figure 2. IEC Standard E1 Waveform (ref. IEC 61000-2-9)

E3 HEMP is similar to a larger version of solar geomagnetic disturbance (GMD) and consists of sub-Hertz pulses lasting up to hundreds of seconds. However, a nuclear E3 pulse can be significantly more intense than a solar storm induced GMD pulse. It is a risk both to the grid and undersea cables. E3 HEMP is discussed in detail in Oak Ridge National Laboratory’s (ORNL’s) META-R-321 report, and GMD risks to the electric grid are explained in Meta-R-319. Some key quotes from these reports follow, prior to resuming the discussion on E-3 risks and mitigation planning guidelines.

According to ORNL’s META-R-321 report, E3 HEMP has the following characteristics:

“E3 HEMP is also called Magneto-hydrodynamic or MHD EMP as it arises from the motion of the ionized bomb debris and atmosphere relative to the geomagnetic field. It was first noticed in 1958 in the Teak and Orange exoatmospheric nuclear weapons tests in the Pacific and Operation Argus in the Atlantic the same year, and additional information was obtained in the later exoatmospheric tests of the Fishbowl series, especially the Starfish Prime test in 1962.

Analysis of these tests has shown that the E3 electromagnetic environments are produced by two basically different physical mechanisms for bursts, both producing significant threats to electrical systems.

1. The 1-10 second time period is known as the “Blast Wave”
2. The 10-300 second time period is known as the “Heave”

The first of these, designated E3A or Blast Wave, is the expansion of the fireball, expelling the geomagnetic field and creating a magnetic bubble. At later times, the debris in the bubble flows along geomagnetic field lines and heats and ionizes the upper atmosphere, causing it to expand buoyantly and rise. The rising, conducting patch crosses the geomagnetic field lines, causing currents to flow in the patch and producing magnetic fields on the surface of the earth beneath the patch. This is designated E3B or Heave. The two processes occur in different time regimes and have different geographical distributions of the electrical field at the surface of the earth.”

According to ORNL’s META-R-319 report, geomagnetic storm induced currents have the following characteristics:

“Geomagnetic storms are created when the Earth’s magnetic field captures ionized particles carried by the solar wind due to coronal mass ejections or coronal holes at the Sun. Although there are different types of disturbances noted at the Earth surface, the disturbances can be characterized as a very slowly varying magnetic field, with rise times as fast as a few seconds, and pulse widths of up to an hour. The rate of change of the magnetic field is a major factor in creating electric fields in the Earth and thereby inducing quasi-dc current flow in the power transmission network. Unlike the HEMP threats, geomagnetic storms are a much more frequent occurrence, which also allows for extensive opportunities to fully benchmark each component of the simulation models and therefore provide greater confidence in the analysis of plausible severe threats, such as the threat posed by an extreme geomagnetic storm scenario.

... these types of disturbances could instantly create a loss of over 70 percent of the nation’s electrical service. This could be a blackout several times larger than the previously largest, the North American blackout of 14 August 2003. The most troubling aspect of the analysis is the possibility of an extremely slow pace of restoration from such a large outage and the multiplying effects that could cripple other infrastructures such as water, transportation, and communications due to the prolonged loss of the electric power grid supply. This extended recovery would be due to permanent damage to key power grid components caused by the unique nature of the electromagnetic upset. The recovery could plausibly extend into months in many parts of the impacted regions. Also other space weather environment interactions can lead to loss of, or permanent damage to, satellites, communications, and other infrastructures, as has been widely reported in the space weather community.

... Both HEMP and space weather disturbances, however, can have a sudden onset and cover large geographic regions. They therefore cause near-simultaneous, correlated, multipoint failures in power system infrastructures, allowing little or no time for meaningful human interventions that are intended within the framework of the N–1 criterion. This is the situation that triggered the collapse of the Hydro Quebec power grid on 13 March 1989, when their system went from normal conditions to a situation where they sustained seven contingencies (i.e., N–7) in an elapsed time of 57 seconds. The province-wide blackout rapidly followed, with a total elapsed time of 92 seconds from normal conditions to a complete collapse of the grid. For perspective, this occurred at a disturbance intensity of approximately ~480 nT/min over the region. As previously discussed, an examination by Metatech of historically large disturbance intensities indicated that disturbance levels greater than 2000 nT/min have been observed even in contemporary storms on at least three occasions over the past 30 years at geomagnetic latitudes of concern for the North American power grid infrastructure and most

other similar world locations; on August 1972, July 1982, and March 1989. Anecdotal information from older storms suggests that disturbance levels may have reached nearly 5000 nT/min. Both observations and simulations indicate that as the intensity of the disturbance increases, the relative levels of GICs and related power system impacts will also proportionately increase. Under these scenarios, the scale and speed of problems that could occur on exposed power grids will hit system operators unlike anything they have ever experienced or even imagined in their careers. Therefore, as storm environments reach higher intensity levels, it becomes more likely that these events will precipitate widespread blackouts to exposed power grid infrastructures.

Continued quote from META-R-319: For this scenario, the intensity of the disturbance is decreased as it progresses from the eastern to western U.S. The eastern U.S. is exposed to a 4800 nT/min disturbance intensity, while west of the Mississippi, the disturbance intensity decreases to 2400 nT/min. This simulation was also performed for the two highest impact and likeliest latitude locations at 45° and 50°. ... Figure 3-25 [Figure 3 below] provides the outage regions that would be expected for a disturbance occurring at a 50° latitude, while the regions for a 45° disturbance latitude are shown in Figure 3-26" [Figure 4 that follows].

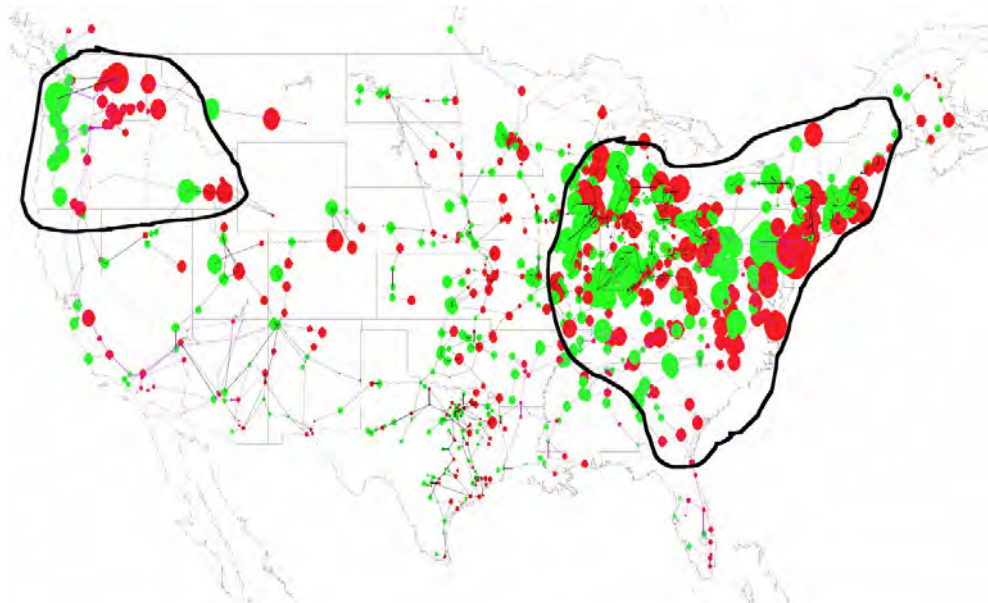


Figure 3. 100 Year geomagnetic storm – 50 degree GMD scenario (ref. Fig. 3-25)

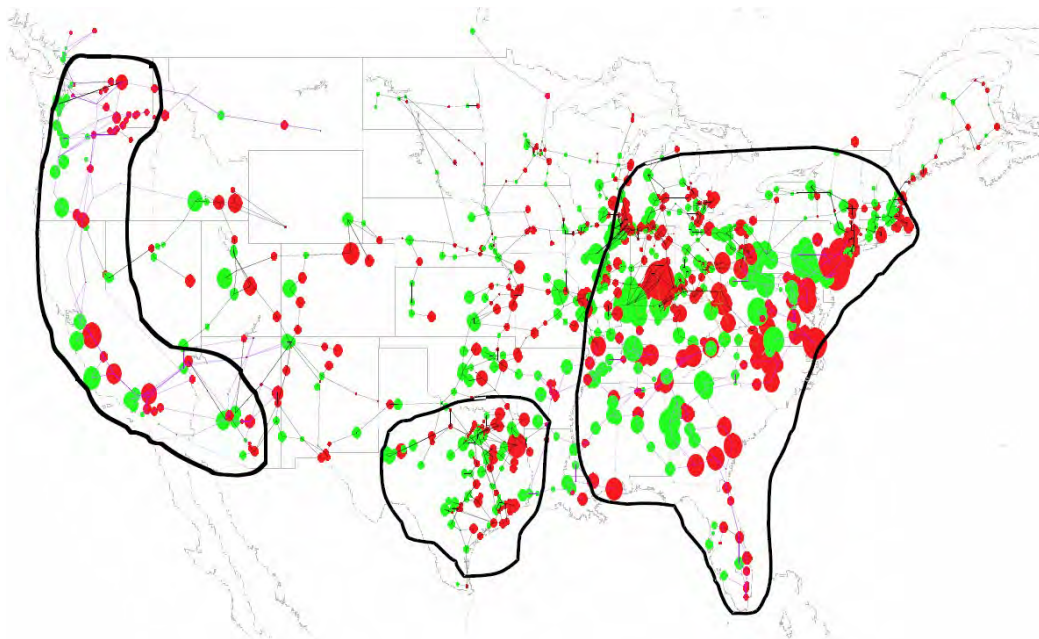


Figure 4. 100 Year geomagnetic storm – 45 degree GMD scenario (ref. Fig. 3-26)

Note that the areas outlined in black are at greatest risks of collapse; cascading outages are likely. Returning now to the topic of low-frequency nuclear EMP variants, only the E3B form of HEMP will be addressed in some detail in the following paragraphs, as there is a need for guidelines on characterizing the E3 HEAVE threat to the grid and other long-line based infrastructures. The most current guidance on the E3 HEAVE threat is from an EMP Commission report released in 2018.

The U.S. EMP Commission published a July 2017 report: “Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures”. In this report, the Commission states:

“... there is a need to have bounding information for the late-time (E3) high-altitude electromagnetic pulse (HEMP) threat waveform and a ground pattern to study the impact of these types of electromagnetic fields on long lines associated with the critical infrastructures. It is important that this waveform be readily available and useful for those working in the commercial sectors.

While the military has developed worst-case HEMP waveforms (E1, E2, and E3) for its purposes, these are not available for commercial use. Therefore, in this report openly available E3 HEMP measurements are evaluated from two high-altitude nuclear tests performed by the Soviet Union in 1962. Using these data waveforms and an understanding of the scaling relationships for the E3 HEMP heave phenomenon, bounding waveforms for commercial applications were developed.

As the E3 HEMP heave field also increases for burst points closer to the geomagnetic equator, the measured results were also evaluated for this parameter. This scaling increases the maximum peak electric field up to 85 V/km for locations in the southern part of the continental U.S., and 102 V/km for locations nearer to the geomagnetic equator, as in Hawaii. The levels in Alaska would be lower at an estimated peak value of 38 V/km ...”
[Page 1 of Volume II, Recommended E3 HEMP Heave Electric Field Waveform for the Critical Infrastructures]

The following Table 2 is derived from the Conclusions of the above EMP Commission report for use as an unclassified reference for determining risks to critical long-line infrastructures to E3.

Table 2. E3 Heave Electric Field Strengths in V/km

Scenarios	Hawaii (Latitude 22° N)	Southern Continental USA (Latitude 35° N)	Alaska (Latitude 65° N)
Altitude: 150 kilometers Yield: 300 kilotons	64 V/km	52 V/km	23 V/km
Altitude: 300 kilometers Yield: 300 kilotons	102 V/km	85 V/km	38 V/km

Note: Assumes uniform ground conductivity of 1 millisiemens per meter (mS/m); estimates the expected maximum E field strength.

Figure 5 below (derived from the Conclusions of the subject EMP Commission Report) provides a normalized waveform that can be used when computing the induced currents flowing in power lines (for example, to determine the amount of heating in transformer hot spots, as the time dependence of the currents are important in determining thermal effects).

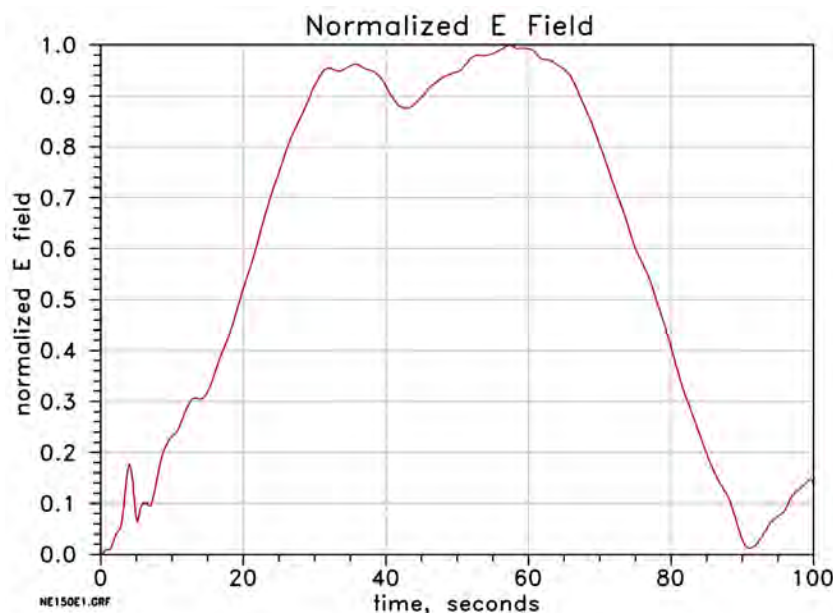


Figure 5. Normalized E3 Heave E field waveform from the 150 km burst height scenario

Figure 6 that follows provides a normalized E field ground pattern resulting from a 300 kT weapon at 150 kilometers altitude, showing the spatial fall-off from the maximum value. Higher yield bursts could lead to even higher maximum fields, although the peak value tends to saturate as yields increase. Larger yields can increase the spatial extent of the high field, and a 300 km burst altitude with a 300 kT weapon also increases the special extent, as shown in Figure 7 (output from EMAT 3 code).

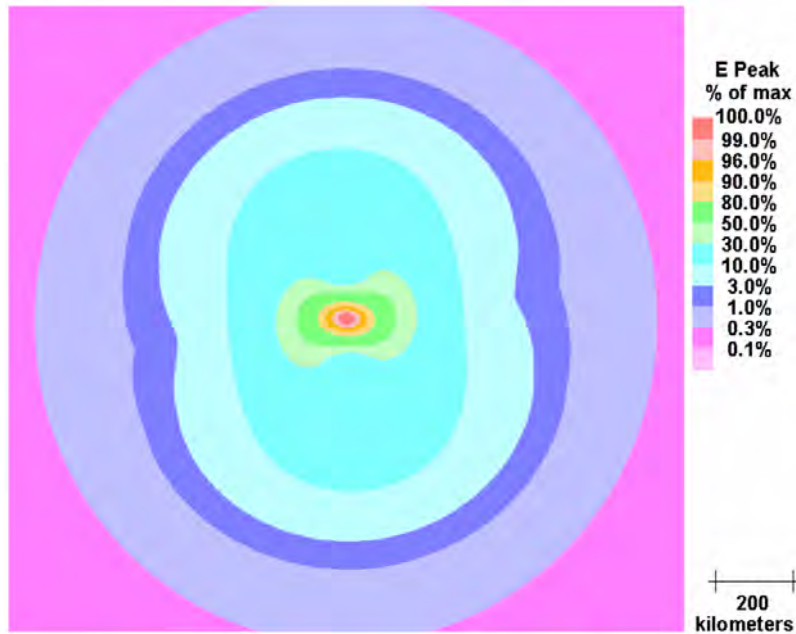


Figure 6. Normalized E peak contour pattern from the 150 km burst case

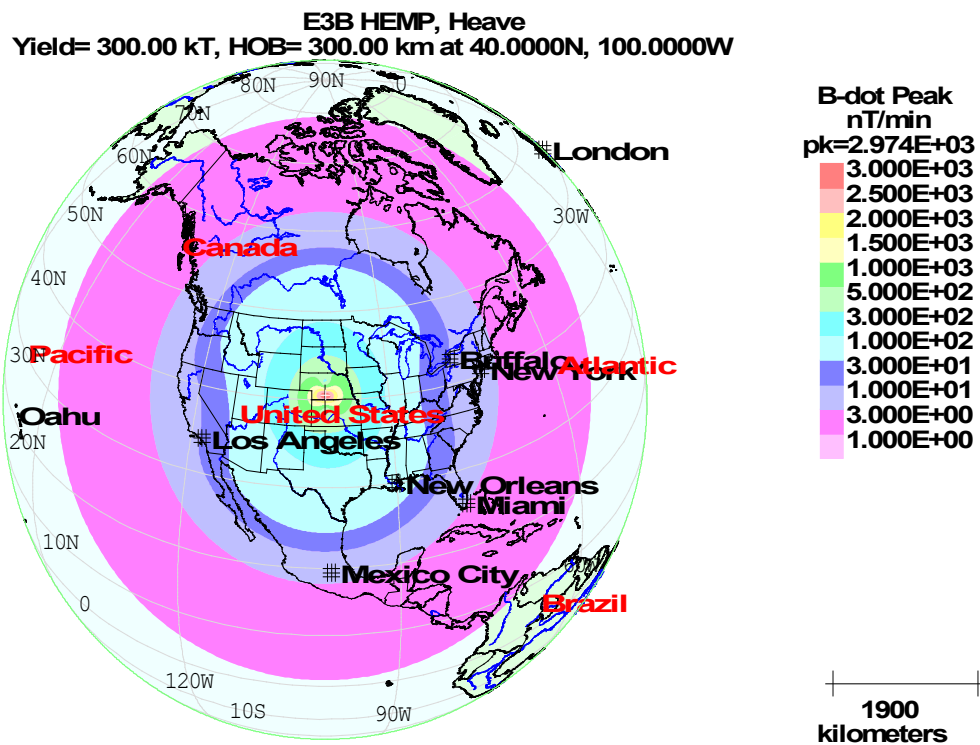


Figure 7. B-dot Magnetic Field Peak contour pattern from a 300 km burst case (from EMAT)

Geomagnetic Storm History and Comparison of HEMP and GMD

As noted in the DHS “Strategy for Protecting and Preparing the Homeland against Threats of Electromagnetic Pulse and Geomagnetic Disturbances”:

“The strongest geomagnetic storm on record is the Carrington Event of 1859 which electrified telegraph lines. The event caused major outages and disruptions in telegraph networks around the world; currents induced in the lines by the event were strong enough to cause sparks and allow some operators to disconnect their systems from batteries and send messages using only the current induced by the storm.

Impacts from the storm were limited given the state of technology at the time; modern society is far more vulnerable to the effects of a significant GMD event due to its reliance on electricity and technology. A more recent significant event occurred in 1989, when a geomagnetic storm collapsed the Hydro-Québec power grid in under two minutes, resulting in the loss of electric power to more than six million people for nine hours in Canada.

A Carrington-like event today, which exceeds the magnitude of the 1989 Hydro-Québec event, could even more significantly disrupt and damage electric power grids. A major GMD event could also disrupt radio communications and navigation signals from GPS satellites, and intense events could create significant radiation hazards for astronauts. Due to technological interdependencies, a severe GMD event could create a complex set of cascading effects, including requiring rerouting of air traffic to avoid areas where communication and navigation would be limited by space weather impacts.”

Table 3. HEMP and GMD Comparison

Attribute	HEMP	GMD
Cause	Adversarial threat	Natural hazard
Warning	Strategic: unknown Tactical: none to several minutes	Strategic: 18 to 72 hours Tactical: 20 to 45 minutes
Effects	<i>E1</i> : High peak field – quick rise time <i>E2</i> : Medium peak field <i>E3</i> : low peak field, but quicker rise time and higher field than for GMD (possibly 3 times higher)	No comparable <i>E1</i> wave forms No comparable <i>E2</i> wave forms <i>E3</i> : low peak field – fluctuating magnitude and direction
Duration	<i>E1</i> : less than a 1 microsecond <i>E2</i> : less than 10 millisecond <i>E3 Blast</i> : ~10 seconds <i>E3 Heave</i> : ~1 – 2 minutes	No comparable <i>E1</i> wave forms No comparable <i>E2</i> wave forms <i>E3</i> : hours
Equipment at Risk	<i>E1</i> : telecommunications, electronics and control systems, relays, lightning arrestors <i>E2</i> : lightning: power lines and tower structures – “flashover”, telecommunications, electronics, controls systems, transformers. <i>E3</i> : transformers and protective relays – long run transmission and communication - generator step-up transformers	<i>E3</i> : transformers and protective relays – long-haul transmission and communications – generator step-up transformers
Footprint	Regional to continental depending on height of burst	Regional to worldwide, depending upon magnitude

Table above adapted from: U.S. Department of Energy, “Electromagnetic Pulse Resilience Action Plan,” p.4

1.4. HEMP, SREMP, and IEMI Risks

As mentioned within the *Scope* section, the protection mechanisms for HEMP, SREMP, and IEMI are very similar, so these are covered together within the document and are discussed further below. From an EMP perspective, the HEMP burst is the most serious due to the potential multi-state to continental extent of impacts. A low altitude SREMP burst could also produce significant EMP damage, but only in a city-wide or regional area, causing equipment upset and damage far beyond the range of blast, shock, and prompt radiation effects. An IEMI attack (for example, using a radio frequency weapon) on a single data center or other electronics dependent targets, such as a grid substation, could cause significant localized or regional infrastructure damage or disruption. The primary protection related difference between these three sources of EMP is that IEMI can occur over a wider range of frequencies, as shown below in Figure 8 (see Wideband and Narrowband).

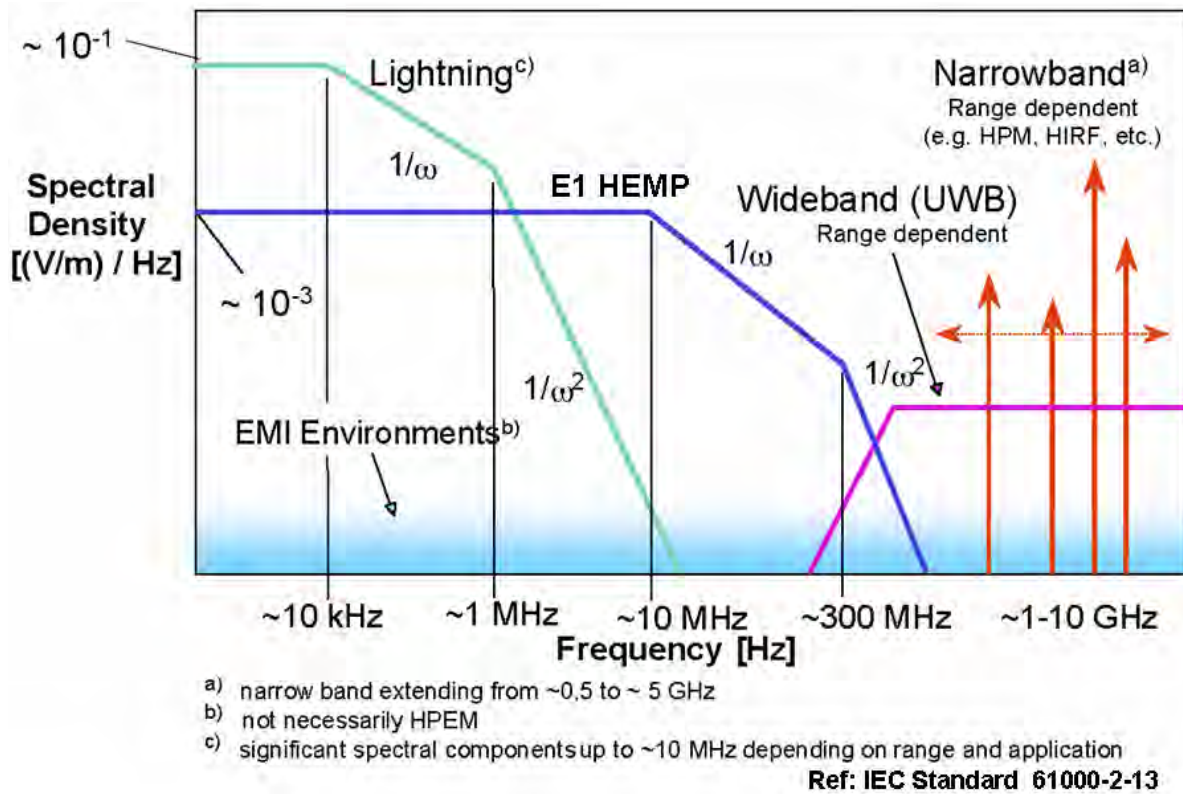


Figure 8. Frequency ranges of Lightning, HEMP, and IEMI ³

High-altitude EMP (HEMP) Risks

HEMP disruption and damage to critical infrastructures can occur across multiple time zones with one or more nuclear bombs exploded at high altitudes in the near-space region. These high altitude nuclear detonations create Compton currents in the upper atmosphere and radiate HEMP pulses downward. A single nuclear burst 250 miles (400 kilometers [km]) above Kansas could destabilize much, if not most, of the U.S. power grid. Likewise, one HEMP burst over North American could significantly disrupt regional or continental data infrastructures, such as the Internet and our television, radio, phone, and cellular networks.

“A nationwide blackout lasting one year could kill millions, perhaps prove fatal to most Americans, by starvation, disease, and societal collapse.”
(William R. Graham, Chairman of the Commission to Assess the Threat to the United States from EMP Attack)

The HEMP pulses could damage or disrupt a significant portion of the equipment connected to power or data lines, if the connections between the cables and the equipment are unprotected. The primary issue is that cables act as antennas to conduct EMP energy to unprotected equipment. And while small electronics without cables, such as cell phones and land mobile radios, are relatively resilient to EMP, their supporting infrastructures are not. Even without long cables, small devices can be disrupted, particularly if they are turned on and/or charging when the EMP occurs.

An example of the potential disruption areas from E1 HEMP (on equipment connected to 100’ Ethernet cables inside of buildings providing 10 dB of protection) is shown in the figure below. As the figure shows, with a 100 kT burst from a generic UNCLASSIFIED warhead at 400 km altitude over the USA, much of the country’s equipment attached to ~ 100’ long Ethernet cables (in this case, running north to south), if not protected against EMP, could be at risk of damage or upset.

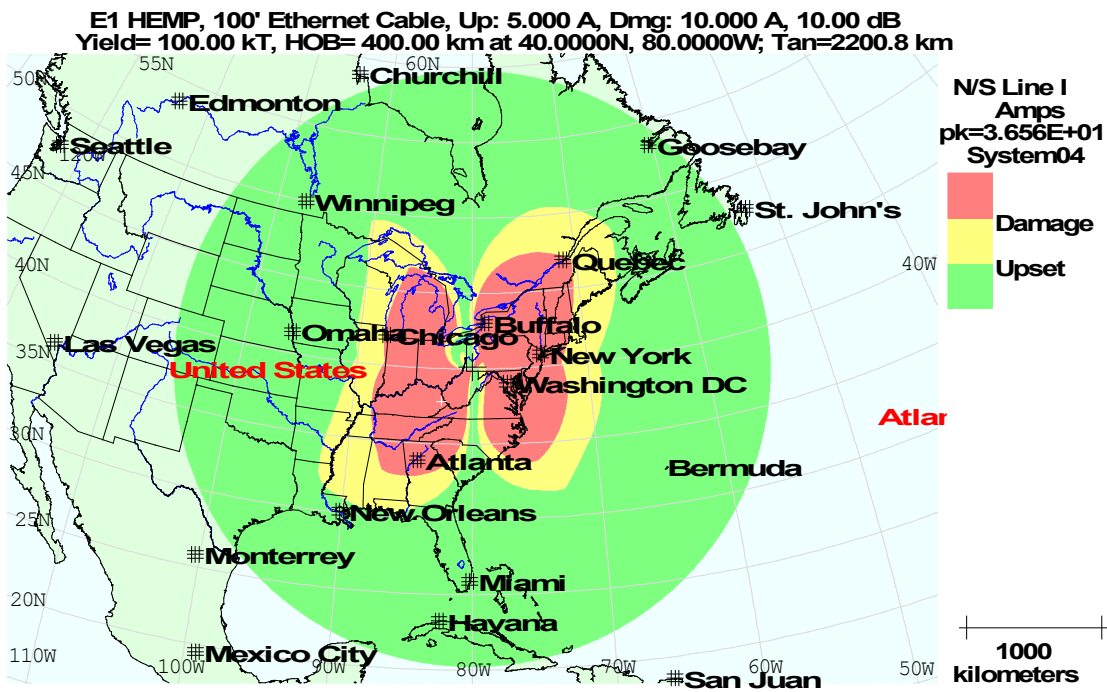


Figure 9. Potential disruption for 100’ Ethernet-connected equipment from 100 kT HEMP

HEMP weapons can be carried by a ballistic missile, a satellite, or a relatively low-cost high-altitude balloon. Intercontinental Ballistic Missiles (ICBMs), Intermediate Range Ballistic Missiles (IRBMs), Medium-Range Ballistic Missiles (MRBM), and Sea Launched Ballistic Missiles (SLBMs) can create significant HEMP, if armed with nuclear warheads that are designed to detonate above the atmosphere.⁴ However, even Short Range Ballistic Missiles (SRBMs), like SCUDs, and high altitude balloons can be used as weapons that carry a nuclear warhead to create significant regional HEMP. The figure below shows the possible HEMP disruption of north/south oriented Ethernet connected equipment inside of buildings providing 10 dB of shielding, from a lower altitude burst (100 km), with a much lower yield than the previous figure (in this case, a 30 kT generic UNCLASSIFIED warhead), as is possible using a shorter range ballistic missile.

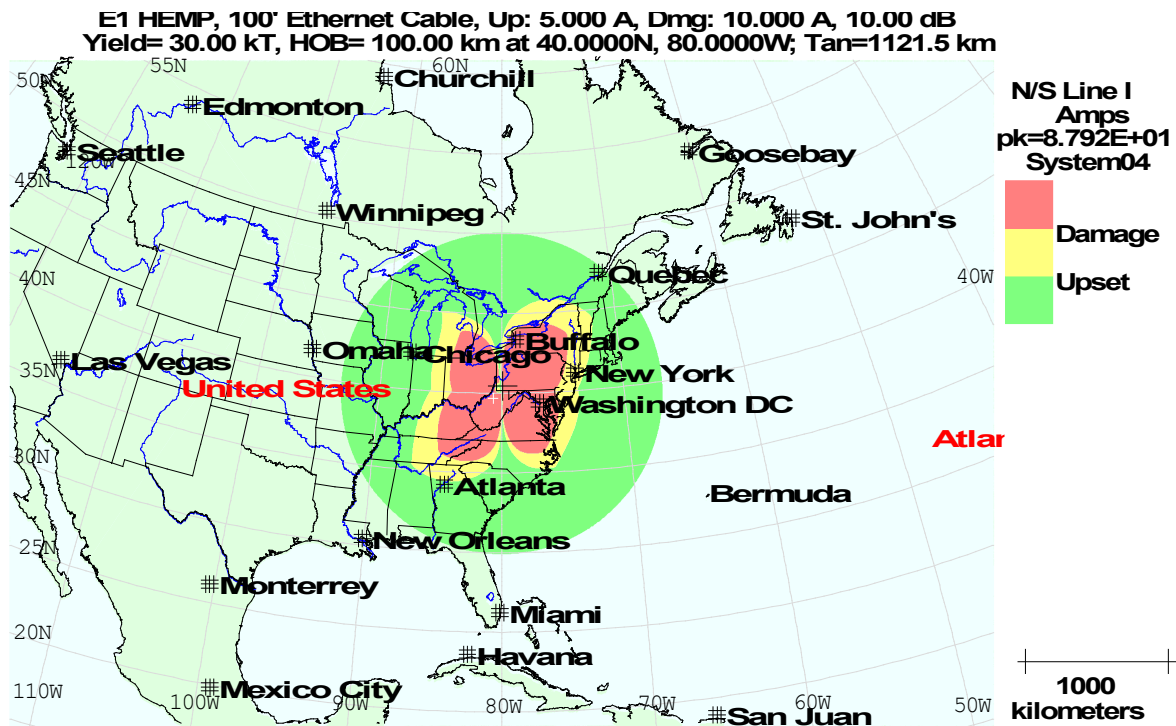


Figure 10. Potential disruption for 100' Ethernet-connected equipment from 30 kT HEMP

The risk associated with a major EMP attack is significant since, as an EMP Commission representative stated, "... many foreign analysts perceive nuclear EMP attack as falling within the category of electronic warfare or information warfare, not nuclear warfare. Indeed, the military doctrines of at least China and Russia appear to define information warfare as embracing a spectrum ranging from computer viruses to nuclear EMP attack."⁵

Shown on the right is a night time photo from Maui Station of the 1962 Fishbowl Starfish Prime HEMP test, which was conducted about 900 miles from Hawaii.⁶ The slide below provides information about some infrastructure impacts from the Starfish Prime test and [Appendix D](#) has extracts from a DHS briefing (that was presented at the Federal Bureau of Investigation’s (FBI’s) sponsored InfraGard Summit in 2017) that provides additional background on EMP risks and mitigation.

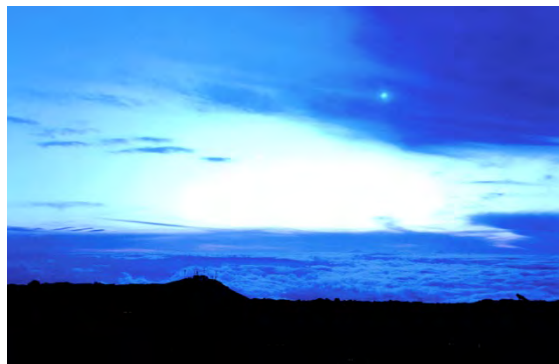



Figure 11. HEMP picture from the Fishbowl Starfish Prime at 0 to 15 seconds.



History of HEMP – USA

1962: U.S. “Starfish Prime” High Altitude EMP (HEMP) Test

- At midnight (9 July) over Johnston Island, a 1.4 MT device was detonated at 400 km (~ 250 miles) altitude ; a ~ 14 kV/meter EMP resulted at Johnston Island
- At 100 nanoseconds, Hawaii experienced a 5.6 kV/m EMP
 - Blew fuses supporting ~ 300 street lights in Oahu (~ 900 miles away)
 - Damaged a microwave link that then shut down telephone service between Kauai to the other Hawaiian islands
 - Other: some car ignition systems fused and burglar alarms went off
- Artificial radiation belt of trapped electrons damaged many satellites
 - Solar panels degraded; most satellites failed (within days to 6 months)
- HF radio was disrupted for minutes to hours in the region; HF equipment damaged

A similar burst over the central USA today would likely shut down commercial power and communications in large regions for months or longer

Kevin Briggs Note: This slide does not present a formalized DHS position regarding EMP risks.

A final set of HEMP-related risks that will be briefly discussed here, that can cause disruptions to long-range radio and satellite communications and navigation, are due to High Altitude Nuclear Effects (HANE). In a similar fashion, large geomagnetic storms can also affect the ionosphere. These communication interruptions can be particularly harmful to longer range wireless communications, such as High Frequency (HF) or satellite. Although this communications interference does not directly harm the infrastructure or equipment, communications resiliency to these distortions of the atmosphere can be a significant problem. See the Table that follows for a summary of some potential HANE impacts on communications (as explained in National Communications System Technical Information Bulletin (NCS TIB) 85-10).

Table 4. Some Effects of High Altitude Nuclear Detonations on Radio Systems

Frequency Band	Degradation Mechanism	Spatial Extent and Duration of Effects	Comments
Very Low Frequency (VLF) (3 kHz – 30 kHz)	Phase and amplitude changes	<ul style="list-style-type: none"> • Hundreds to thousands of miles • Minutes to hours 	<ul style="list-style-type: none"> • Ground wave not affected. • Reduces range and quality of signal. • Lowering of sky wave reflection height causes rapid phase changes with slow recovery. • Significant amplitude degradation also possible.
Low Frequency (LF) (30 kHz – 300 kHz)	Absorption and scattering of sky waves	<ul style="list-style-type: none"> • Hundreds to thousands of miles • Minutes to hours 	<ul style="list-style-type: none"> • Ground wave not affected. • Negative impact is sensitive to burst location and propagation path.
Medium Frequency (MF) (300 kHz – 3 MHz)	Absorption of sky waves	<ul style="list-style-type: none"> • Hundreds to thousands of miles • Minutes to hours 	<ul style="list-style-type: none"> • Ground wave not affected. • Could also prevent AM radio reception where signal is weak or transmitter is hundreds of miles away
High Frequency (HF) (3 MHz – 30 MHz)	Absorption, multipath interference, loss of support for F-region reflection (region 150 km – 800 km above sea level)	<ul style="list-style-type: none"> • Hundreds to thousands of miles • Minutes to hours 	<ul style="list-style-type: none"> • Reduces range and quality of signal. • Could impact HF sky wave, including SHARES and Amateur Radio Operators (AROs). • Daytime absorption is larger than nighttime.
Very High Frequency (VHF) (30 MHz – 300 MHz)	Absorption, multipath interference	<ul style="list-style-type: none"> • Few miles to hundreds of miles • Minutes to tens of minutes 	<ul style="list-style-type: none"> • Reduces range and quality of signal. • 99% of EMP energy is found below 100 MHz.
Ultra High Frequency (UHF) (300 MHz – 3 GHz)	Absorption	<ul style="list-style-type: none"> • Few miles to hundreds of miles • Seconds to few minutes 	<ul style="list-style-type: none"> • Could impact lower frequency satellite services. • Only harms line-of-sight (LOS) propagation through highly ionized regions.

Source Region EMP (SREMP)

Significant SREMP is generated when a nuclear detonation occurs on or near the ground. The SREMP travels through the air and can damage or disrupt equipment connected to Ethernet cables, telephone lines, and power cords out to 70 miles or more. Electronic systems not connected to power cords or communications lines, such as cellular phones, are generally resistant to SREMP but become useless for communicating if the infrastructure that supports them is non-functional.

While SREMP is only a secondary reason a terrorist or nation-state adversary would detonate a nuclear weapon, all ground based (at or near surface) nuclear detonations create SREMP of sufficient magnitude to cause infrastructure disruptions. Although the extent of the overall EMP damage is likely much less with SREMP than with HEMP, the solutions are generally applicable to both types of attacks and therefore SREMP is covered along with HEMP in this document.

For bursts near the Earth's surface (burst heights less than 1,000 meters), the phenomenology of SREMP is well understood. The figure that follows illustrates the basic ground burst geometry and SREMP characteristics. The peak fields occur near the time of the peak prompt gamma ray flux at the observer (retarded time of approximately 10 ns); they are strongest close to the burst and decrease with range. The air becomes highly conducting near the burst, reaching levels of 10 siemens per meter (S/m), which is more conducting than seawater. The Compton current can exceed 1 mega-ampere per square meter, which creates peak electric fields from 1 to 10 million volts per meter (larger fields are generated in the Earth). The prompt ionized source region extends out to a range of 2 - 5 km depending mainly on the device gamma ray yield.

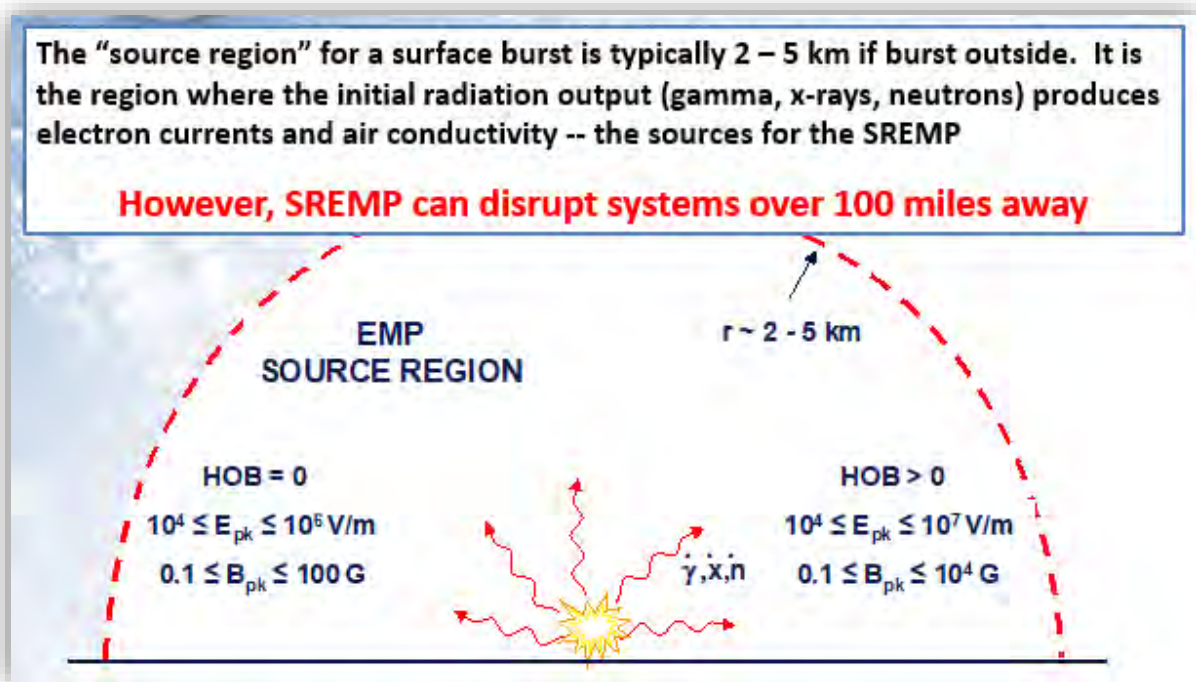


Figure 12. Generation of Source Region EMP (SREMP) from a ground burst

Although the peak early-time SREMP fields are much more intense than HEMP (by up to a factor of 1,000 for some blast-hardened silo systems), the late-time SREMP may be more important for many classes of systems. The neutrons that interact with the air and ground produce gamma rays at later times. The most important interaction is the ground-capture process that produces gamma rays, which leave the Earth's surface, at retarded times from 0.1 to 100 milliseconds. These gamma rays produce Compton currents, air ionization and conductivity and SREMP fields of a few kV/m, which cover the same time frame. These low-frequency fields (in the kilohertz range) propagate with little attenuation into the Earth to depths of 1 km or more (depending on the electrical characteristics of the soil). These fields also couple readily to long buried cables and can induce currents of 200 kA with pulse widths (and therefore energy) 10 times larger than worst case lightning. In comparison, currents coupled due to early-time (E1) HEMP are no more than 5 kA and 1 kA at later times.

During the 1950s to 60s surface burst tests, equipment/cables were damaged by SREMP in over 100 cases at the Nevada Test Site. SREMP can cause long-term regional power outages and can damage electronics in deeply buried structures. SREMP can also cause fires due to wires melting. The figures that follow show the potential disruption zones for: AC/DC adapters, FM radio transmission towers, and cellular handsets due to a simulated 10 kT surface burst in the National Capital Region.

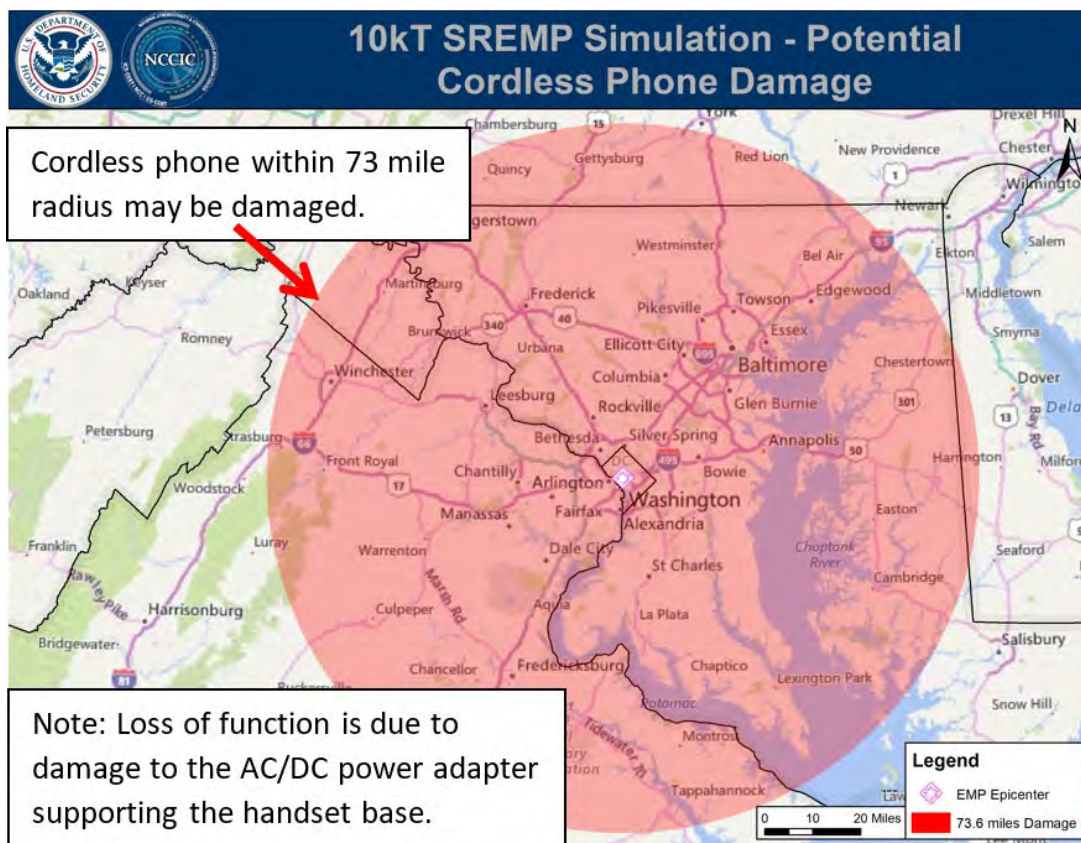


Figure 13. Potential 10 kT SREMP disruption of AC/DC adapters

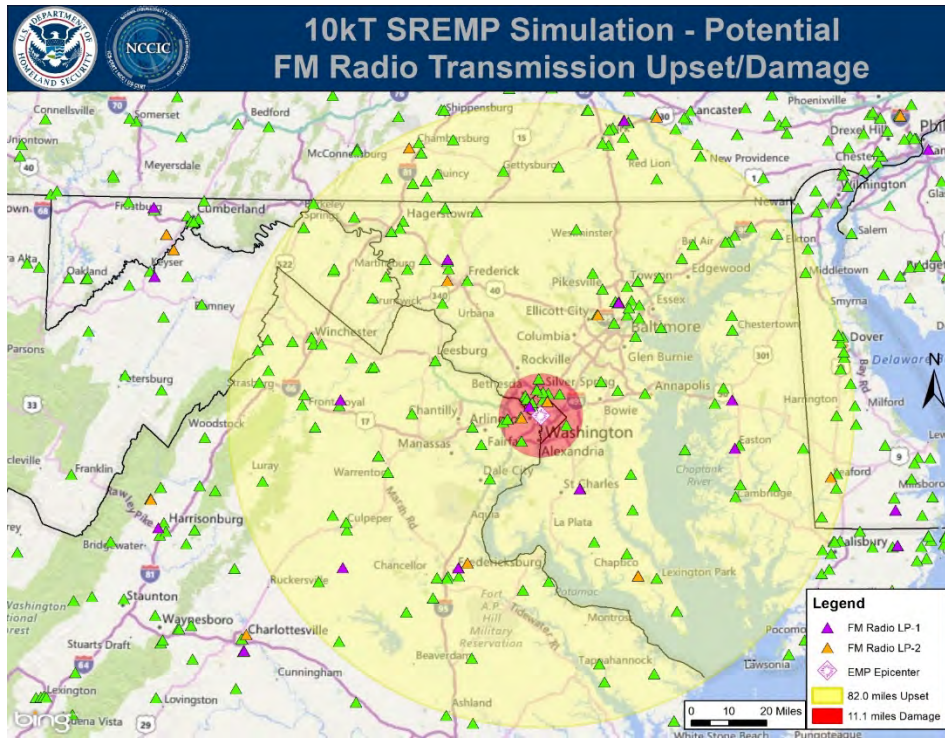


Figure 14. Potential 10 kt SREMP Upset/Damage to FM Radio Transmission

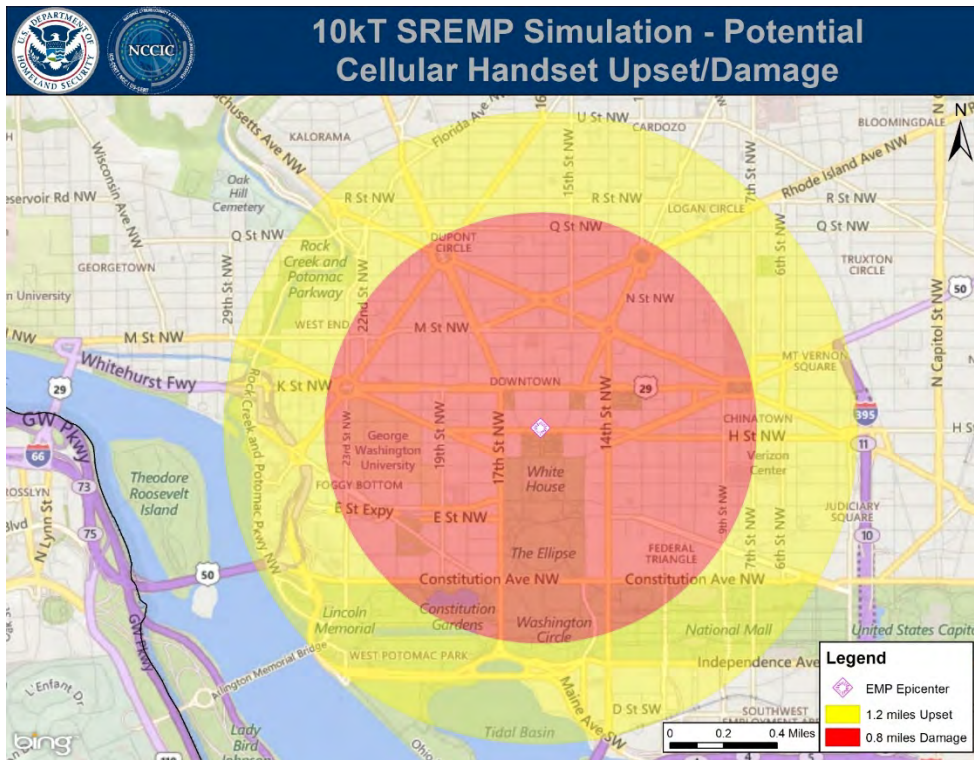


Figure 15. Potential 10 kt SREMP Upset/Damage to Cellular Handsets

Note: These guidelines do not endorse any referenced product, company, service, or information external to DHS.

Version 2.2 – 5 February 2019
Guidelines are subject to change and only represent the views of the NCC.

The table that follows provides some suggested upset/damage planning guidelines related to SREMP.

Table 5. Source Region EMP Damage and Upset Planning Factors

Yield (kT)	10	100	1,000		
	Range to effect in km			Effect Threshold and Notes	
Buried Comms Cable Damage / Upset	21.00 / 26.00	34.91 / 39.98	44.16 / 49.19	100 A / 50 A	Short circuit current, assumed to connect with fireball at early times and cable insulation breaks down, 0.001 S/m ground conductivity, effect of branching not included
Overhead HV Power line Damage/Upset	65.00 / 85.00	110.05 / 143.00	134.16 / 174.00	1000 A / 500 A	Short circuit current, assumed to connect with fireball at early times, 138 kV line used for line parameters, 0.001 S/m ground conductivity, effect of branching not included
0.5 km Offset Overhead HV Power line D./U.	23.00 / 43.00	33.00 / 66.00	44.00 / 84.00	1000 A / 500 A	Short circuit current, assume connect with fireball at late time based on fireball growth, 138 kV line used, 0.001 S/m ground conductivity, effect of branching not included
100' Ethernet Damage / Upset	21.04 / 77.42	23.76 / 86.88	26.40 / 95.84	10 A / 5 A	0.1 m height, current into 100 ohms, aligned radially, max of calculations for 0.01 S/m or 0.001 S/m ground conductivity
Wireline phone / Cordless phone adapter damage	69.19 / 118.50	77.16 / 131.80	87.90 / 149.64	8 kV / 4 kV	Voltage calculation for 1 km radial line. Wireline assumes twisted pair. Cordless telephone base failure due to AC/DC power adapter damage.
1000' T1 Line Damage / Upset	95.26 / 161.8	105.84 / 179.35	115.06 / 194.6	10 A / 5 A	10 m height, current into 100 ohms, aligned radially, max of calculations for 0.01 or 0.001 S/m ground conductivity
200' Cell Tower Shield D./Upset	2.30 / 14.36	2.67 / 15.33	2.99 / 16.25	1000 A / 100 A	Short circuit current at base of 200' vertical monopole
100m FM Tower Shield D./Upset	4.74 / 38.95	5.20 / 42.38	5.49 / 44.60	1000 A / 100 A	Short circuit current at base of 100m vertical monopole
500m FM Tower Shield D./Upset	17.72 / 133.38	21.65 / 160.37	24.57 / 180.06	1000 A / 100 A	Short circuit current at base of 500m vertical monopole
600m DTV Tower Shield D/U	21.18 / 183.31	26.65 / 226.00	30.62 / 256.48	1000 A / 100 A	Short circuit current at base of 600m vertical monopole
200m AM Signal Antenna D./U.	8.43 / 78.97	9.68 / 90.18	10.69 / 99.11	1000 A / 100 A	Current into 50 ohm at base of vertical monopole
HF Vertical Mono. Signal Dam/Upset	2.50 / 15.85	2.81 / 16.72	3.09 / 17.29	10 A / 1 A	7.5 m vertical monopole (1/4 wave antenna), current into 50 ohms, max. of calculations for 0.01 or 0.001 S/m conductivity
HF Horizontal Dipole Signal D/U	1.50 / 2.15	1.77 / 2.42	2.02 / 2.67	10 A / 1 A	15 m horizontal dipole aligned radially (1/2 wave dipole), 15 m above ground, current into 50 ohms
VHF-Hi Antenna Signal D./Upset	1.25 / 1.95	1.54 / 2.22	1.75 / 2.45	10 A / 1 A	1.4 m vertical monopole (modeling j-pole antenna), current into 50 ohms
Cell Tower Ant. Signal Dam/Upset	0.37 / 0.65	0.50 / 0.83	0.57 / 0.95	10 A / 1 A	19 cm horizontal dipole at 200' height (modeling 1/4 wavelength crossed dipoles), current into 25 ohms
Cell or Land Mobile Radio Handset D./Upset	1.30 / 1.90	1.57 / 2.21	1.72 / 2.49	100mA / 10mA	10 cm vertical monopole, short circuit current, coupling dominated by air conductivity

Intentional Electromagnetic Interference (IEMI)

IEMI is 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.”⁷ In general, IEMI is generated by a high power generator that can be hidden in a truck, aircraft, ship, backpack, or suitcase. This weapon could be used to shut down the electronics associated with critical infrastructure, such as a communications site, data center, power substation, or headquarters location.

EMI has been known to cause problems with heart pacemakers, but perhaps the worst incident was in 1967 when an aircraft sitting on board the USS Forrestal was exposed to the ship’s radar and accidentally fired its munitions hitting a fully armed and fueled aircraft sitting on the deck. The explosions and resulting fire caused 134 deaths. “A later investigation discovered that a degraded cable shield termination on the first aircraft was the cause of the accident.”⁸

IEMI has been around since the dawn of wireless communications, causing the Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) to play critical roles to minimize interference. EMI is becoming even more critical as wireless continues to proliferate and becomes more and more important. Due to this wireless growth and as electronic components and circuits continue to become an increasingly integral part of society often with increased sensitivity to EMI, IEMI disturbances and damages have become much more common. Further, devices that can cause IEMI have also become more common and more powerful causing IEMI to gain more and more attention.

The type and amount of IEMI disturbances and damages is dependent on multiple parameters of the IEMI source device:

- **Proximity** to the target, with the EM field decreasing with the square of the distance
- **Power**
- **Frequency** with higher frequencies typically used to damage equipment (in-band frequencies cause the most harm to communications)
- **Duration** is usually a short pulse at high power such that it can destroy equipment (continuous power is used to block wireless communications).

Oak Ridge National Laboratory’s report “Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid”, Meta-R-323, by Dr. Radasky and Dr. Savage, January 2010, provides a detailed technical overview of IEMI risks. Some key excerpts follow:

“In terms of system vulnerabilities, the narrowband threat is usually one of very high power and high energy, since the electrical energy is delivered in a narrow frequency band. It is fairly easy to deliver fields on the order of thousands of volts/meter at a single frequency. Of course each system under test may have a vulnerable frequency that is different from the next. Often the malfunctions observed in testing equipment with narrowband waveforms are those of permanent damage. ...”

“The wideband threat is somewhat different in this respect. Since a time domain pulse produces energy over many frequencies at the same time, the energy density at any single frequency is much less. This means that damage is not as likely as in the narrowband case;

however, it is easier to find a system's vulnerability since many frequencies are applied at the same time. Sources that have been built in the past typically produce repetitive pulses that can continue for many seconds or minutes, thereby increasing the probability of producing a system upset. ..."

"For radiated fields, it seems clear that frequencies above 100 MHz are of primary concern in that they are able to penetrate unshielded or poorly protected buildings very well and yet couple efficiently to the equipment inside of the building. In addition, they have the advantage that antennas designed to radiate efficiently at these frequencies are small. [The Figure that follows] illustrates a qualitative view of how radiated fields may illuminate and couple to system electronics through apertures (e.g., windows) and through building wiring."

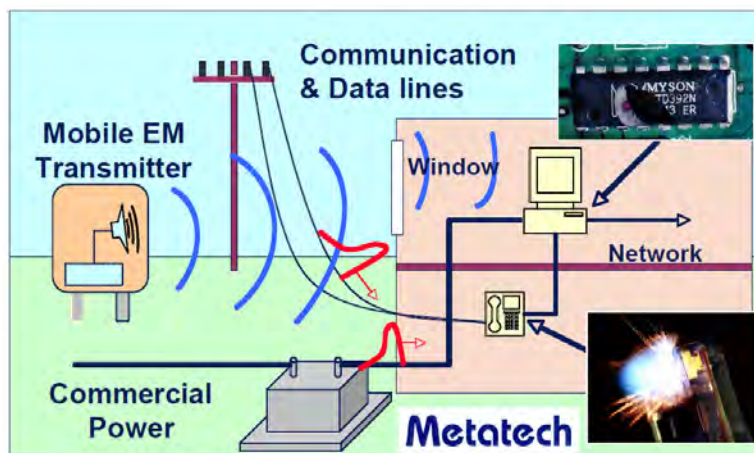


Figure 16. Typical IEMI interaction of radiated fields

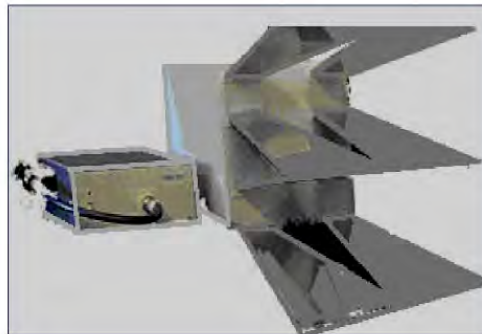
"For conducted voltages and currents, there are some differences in terms of the frequency range of interest. It is well established that if common-mode conducted signals are injected into the power supply or telecom cables outside of a building, that frequencies below 10 MHz (and pulse widths wider than 50 ns) propagate more efficiently than higher frequencies. Experiments by Parfenov et al. have shown that these "lower" frequencies can disrupt the operation of equipment inside a building ..."

"With regard to actual threat "weapons", the following four figures describes some published examples of devices that could be used as weapons. ..."

- Diehl Munitions Systeme is marketing a small interference source (including antenna)
 - 350 MHz damped sine field
 - 120 kV/m at 1 meter (omni-directional antenna)
 - 30 minute continuous operation (5 pulses per second) or 3 hours in bursts
 - 20 x 16 x 8 inches and 62 pounds
- Demonstration in Summer 2004



Figure 17. DIEHL Munitions damped sine IEMI generator



Parameters	Values
Amplitude at 20 m distance	2 kV/m
Pulse duration	0.2 ns
Pulse repetition rate	Up to 1000 Hz
Antenna aperture	0.35 m x 0.35 m

Source: Dr. Yuri Parfenov, Russia

Figure 18. Laboratory hyperband pulse generator used in Russia

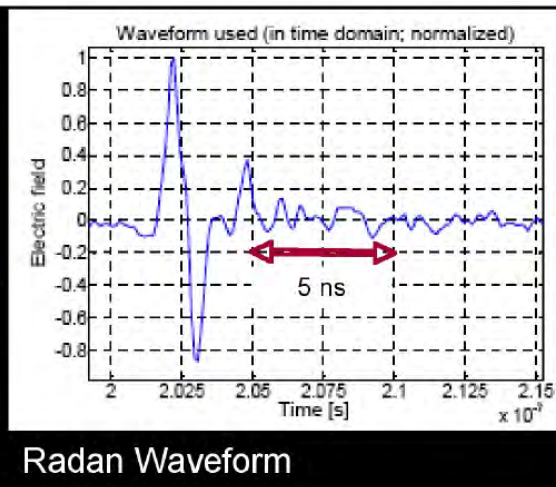


Figure 19. RADAN 303B hyperband generator used in Sweden

AFRL has developed an extremely powerful IRA system that produces UWB pulses

- E*R = 5.3 MV
- pulse width ~100 ps



Figure 20. High intensity JOLT hyperband generator used in the United States

“... For wideband radiated threat waveforms, buildings can be exposed externally to hyperband waveforms with peak field levels on the order of 10 kV/m. For briefcase devices, the same level of peak field in the hyperband to the mesoband range can be delivered and should be considered. The frequency range of these devices is from 100 MHz to 10 GHz.

For narrowband radiated threat waveforms, buildings can be exposed externally to radar type waveforms again in the range of 10 kV/m. Small internal narrowband generators have not been observed beyond the level of cellular phones or walkie-talkies at very close ranges (~100 V/m) or weapons made from microwave ovens (~1 kV/m).

For conducted IEMI threats, the induced conducted voltage from a 10 kV/m peak field (narrowband or wideband) is on the order of 10 kV. The typical injected capability is also on the order of 10 kV, although there are newer pulsers that may exceed this level.”

Table 6. Comparisons between IEMI threats and E1 HEMP

Threat Environments	
Threat	Description
E1 HEMP	IEC 61000-2-9 E1 HEMP Peak = 50 kV/m Rise time (10% - 90%) = 2.5 ns Pulse width (FWHM*) = 23 ns Number of pulses = 1 or 2
Severe IEMI	JOLT-like Peak rE = 5 MV Rise time (10% - 90%) = <100 ps Pulse width (FWHM*) = <1 ns Number of pulses = ~600/s
Moderate IEMI	1/10 th of Severe IEMI Peak rE = 500 kV Rise time (10% - 90%) = <100 ps Pulse width (FWHM*) = <1 ns Number of pulses = ~600/s

2. EMP PROTECTION AND RESILIENCE CONSIDERATIONS

This EMP guidance document provides a range of protection and resilience levels that are based on the criticality of the EMP sensitive electronic infrastructure and equipment as well as the amount of down time that can be tolerated. This section discusses basic requirements and design principles that are applicable across all mission critical levels of importance and budgets.

2.1. Prioritizing EMP Mitigation Efforts

Each federal, state, and local critical infrastructure owner or operator can prioritize EMP protection efforts by determining their infrastructure's overall importance by (1) assessing the risk to society if their infrastructure is disrupted and (2) by comparing their infrastructure's role in supporting one or more of the eight National Essential Functions defined in Presidential Policy Directive 40, National Continuity Policy.⁹ The infrastructure's importance, together with the amount of downtime that can be tolerated, can then be used to determine which level of EMP Protection should be achieved for that infrastructure. It is recommended that for any infrastructure supporting life or safety or the economic well-being of society, at least a Level 1 EMP Protection capability should be attained as a near-term goal. If the loss of a particular infrastructure will likely result in a significant loss of life or health or economic well-being, then an EMP Protection Level of 2 or 3 is recommended. Few infrastructure owners/operators will need to meet EMP Protection Level 4 guidelines, as these protections are more expensive and were developed mainly for Presidential support or strategic military missions.

For non-federal entities, the four National Essential Functions that are most often supported are:

- Protect and stabilize the Nation's economy.
- Protect against threats to the homeland and bring perpetrators to justice.
- Provide for critical national health, safety, and welfare needs of the United States.
- Respond to and recover from domestic consequences of an attack.

The federal government provides a leading role overall in the above functions, but typically has an even more important role in the following with support from non-federal entities:

- Ensure the continued functioning of the three separate branches of government
- Maintain and foster effective relationships with foreign nations
- Provide leadership visible to the Nation and the world
- Defend the Constitution against all enemies, foreign and domestic

Table 7 that follows provides some additional guidelines to consider when prioritizing critical infrastructures for EMP protection.

Table 7. Considerations for prioritizing infrastructures for EMP Protection

Step	Decision	Explanation
1	Rank importance of critical infrastructure (CI)	<ul style="list-style-type: none"> • How many people are likely to die if this infrastructure is disrupted? • How many people are likely to suffer significant health risks if this infrastructure is disrupted? • What is the economic impact, measure in dollars of loss, if this infrastructure is disrupted? • Is a National Essential Function put at risk if this infrastructure is disrupted?
2	For the most important critical infrastructures, prioritize end-to-end substructures needed to meet essential needs and maximize benefits	<ul style="list-style-type: none"> • After prioritizing the high-level critical infrastructure’s importance, then assess the end-to-end substructures needed to effectively support the most important CI. Remember that a CI is only as resilient as its weakest link. Organizations may need to develop internal backup systems for supporting infrastructures outside of their normal mission. For example, both power and communications and personnel support systems are typically required for every CI. • Do not rely on unprotected commercial power and communications networks. If your CI does not have resilient back-up power and communications, then consider what the most cost-effective alternatives for obtaining these are. • After determining the key substructures, prioritize each supporting system and independent subsystem to provide the most value per dollar spent on EMP Protection. Different substructures and systems and subsystems are likely to require different EMP Protection Levels. • Example: A wireless vendor’s IT team may have determined in Step 1 that their overall network is a Level 3 EMP priority. To meet this overall Level 3 goal, they classified the primary core control system and some sites in key locations as Level 3, but most sites were classified as Level 2 or Level 1, and some sites that overlap with others were considered not as critical.
3	Prioritize components and develop plans for protecting the end-to-end functions	<ul style="list-style-type: none"> • Breakdown the above systems and subsystems from Step 2 into the major components. • Prioritize the various components within each prioritized system and subsystem and assign an EMP Protection Level goal. • Continue the above process until down to the individual component level that can be protected, such as a rack of equipment or a cable connecting two components, and what resilient supporting systems are needed.

The following section provides an overview of the Technical Design Standards that most organizations can use to help them achieve their EMP protection goals.

2.2. IEC Technical Design Standards

The International Electrotechnical Commission (IEC) is the world’s leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies. It has been producing HEMP and IEMI protection standards for commercial

electronics since 1989. These standards provide protection guidelines both against radiated fields that can penetrate inside of a building and against transients induced on cables either entering a building from the outside or induced on cables inside a poorly shielded building (where the internal fields create the induced transients). Many countries have mandatory standards based upon these IEC standards.

IEC Subcommittee 77C developed their HEMP and IEMI protection standards by considering that normal commercial electronic equipment must survive everyday transient currents and voltages that are induced on cables that flow into equipment. The two most important IEC 61000-5-10 tests are the following:

- **Electric Fast Transient (EFT)** – This EMC conducted test protects against an EFT pulse with a rise time of 5 ns and a pulse width of 50 ns, which is nearly the same as the waveshape of E1 HEMP induced voltages (with a rise time of 10 ns and a pulse width of 100 ns).
- **Lightning Induced Transient** – This transient is caused by lightning surges that are characterized by a voltage pulse rise time as fast as 1 μ s and a pulse width of \sim 50 ms. Typical commercial EMC peak test levels for these voltage pulses are 0.5 to 1 kV for EFT and 1-2 kV for surge (first number is for data lines and the second is for a power line).

The IEC has also developed standard waveforms and levels for the coupling of HEMP and IEMI fields both to long external cables such as commercial power lines and for short cables as found inside of a building. Worst case E1 HEMP external above ground power system cable voltage levels are \sim 300 kV and the worst-case internal induced cable voltages are \sim 20 kV when there is no building shielding from the penetrating fields (the reduction is because the wiring inside of a building is not perfectly straight for hundreds of meters). The levels for IEMI coupling are significantly less as those fields do not couple efficiently to wires and cables and have radiated losses. But IEMI is a significant threat to the internal electronics since its frequency content above 1 GHz can penetrate the cases of most equipment. Both of these threats are covered in this document, but the E1 HEMP cable tests are the most severe for equipment, so more emphasis is placed on the protection of power, data, and antennas cables.

Since the E1 HEMP standards of the IEC (as well as most military standards) use a single worst-case electric field pulse waveform (the IEC identifies a peak field of 50 kV/m), these waveforms are considered a reasonable worst-case tool for the design of resilient infrastructures. (Note that while 50 kV/m peak field is used by the IEC and military standards, some Chinese and Russian authorities have said “super-EMP” weapons can generate E1 levels as high as 100 kV/m to 200 kV/m, respectively, as reported in the EMP Commission’s 2017 “Chairman’s Report” pages 21 and 31.) It is possible, as in the case of the Starfish test in 1962, that the HEMP peak fields can be smaller than the worst case, depending on the location of the burst and the location of the infrastructure relative to the burst. Therefore, even for a building with no shielding for E1 HEMP, the voltages coupled to the wiring leading to equipment may be lower by a factor of 5, for example. This means 4 kV could be induced for fields oriented perfectly for cable coupling (assuming no building attenuation). As the equipment can tolerate a peak EMC transient (EFT) of 500 V for a data line entering an electronic equipment and probably more (testing safety margin)

Peak voltage on a cable from HEMP only needs to be reduced between a factor of 4 and 8. This enables inexpensive solutions to be deployed that can also be used for lightning protection.

the amount of reduction required in the peak voltage on a cable is between a factor of 4 and 8, which is not usually a problem for a typical SPD.

Also the IEC EMC test requirements are that no upsets occur during the certification testing, so the damage immunity level is likely higher by at least a factor of 2. (Note: An upset is when the system must be restarted, either by turning the equipment “off and on” and may sometimes even require disconnecting equipment from the battery circuit (as was the case for some vehicles during testing done by the EMP Commission)). Therefore, even standard lightning protection surge protection devices (SPDs) will provide some reduction in the E1 HEMP conducted transients inside of a building. If the building has some natural protection level (say 10-20 dB) then the induced voltages inside are not likely to cause problems for equipment. Based on details in IEC 61000-5-10, if building shielding is to be used, a level of 30 dB or higher is recommended, so this supports the suggested levels of protection for Level 3.

For the external lines coming into a building (both power and data lines), if these lines enter the building above ground (drop wires), much higher voltages can be induced by E1 HEMP than inside the building, and a building level lightning SPD should be used to avoid large voltages entering the building. A better solution for a commercial building is to ensure that the power and communications lines enter the building below ground as the earth will reduce the coupling to those external cables by more than a factor of 10. If this is done, then the main concern is for the coupling to the cables inside the building by fields penetrating the poorly shielded walls of typical building construction, but even this may be a minimal issue if the cable inside the building is short enough.

Given the above, the first two levels of protection recommended in this document rely heavily upon using inexpensive SPDs. Level 1 recommends using lightning protection SPDs. Level 2 suggests the use of EMP SPDs for all critical equipment including power cords, data lines and antenna connections. The EMP performance of an SPD has to do with the amount of peak voltage that can pass through the SPD based on the rise time of the conducted E1 HEMP pulse. The lightning voltage transient has a rise time of about 1 μ s, while the E1 HEMP and the propagated SREMP will rise in approximately 10 ns, and the IEMI conducted transient will rise in about 1 ns. Our focus here is on the E1 HEMP, which rises 100 times faster than a typical lightning voltage pulse. So lightning SPDs will not be as effective in limiting the pass-through voltages as an EMP SPD, but the energy of the EMP pulses passing through the SPD will be much lower than the lightning-pass-through energy.

To summarize, IEC 61000-5-10 provides detailed information concerning the use of SPDs to limit the EMP voltages flowing to equipment in Levels 1 and 2 and how to set the shielding levels for a building (as recommended for Level 3 for at least 30 dB) based on the criticality of the function of the facility and the nature of the equipment inside the building. The standard also recommends simple test methods to establish the natural shielding effectiveness of an existing building, which can be used in the hardening process. The level 4 EMP protection recommendations are presented in this document for missions that cannot allow more than a few seconds of outage, and therefore require the approach provided in MIL-STD-188-125-1, which requires an 80 dB shield and the test procedures defined in the military standard. The basic details of that standard are included in this document.

2.3. Surge Protective Device (SPD) Selection

Many surge protective devices have been designed to withstand the peak-induced voltages (and currents) on cables connected to equipment from a nearby lightning stroke. Of course lightning fields from nearby groundstrokes vary substantially, so the level of induced cable voltages can vary a great deal. The IEC and other organizations have set requirements for typical equipment from 1 – 2 kV for a surge type pulse (1 μs rise time). A large direct strike to an above ground power line entering a building will be much higher than this. In fact, most of the electronics inside the building will be destroyed during a direct strike. But this is a low probability event. SPDs are designed to reduce peak lightning-induced voltages to levels that won't harm most equipment.

The issue, as discussed above, is that E1 HEMP and the propagated SREMP electric fields have a rise time as fast as 1 ns (see Table 8 below). This means that nearly all SPDs designed for lightning will allow higher peak voltages to bypass the voltage “clamping” or “protection” level identified. While metal oxide varistors (MOVs) and transient voltage suppressors (TVSs) have the best performance for waveforms rising faster than a typical lightning pulse, often the peak voltages bypassing the SPD (including gas discharge tubes or GDTs) can be a factor of 3 higher than the voltage identified with the SPD. This is because for GDTs the voltage is a DC level, and for MOVs the voltage indicated is the “firing” level for an AC-type waveform. Therefore, a fast-rising voltage pulse that gets by the SPD will always have a higher peak value than the “rated” value.

Table 8. EMP Induced Surges on Conductors ¹⁰

Type of Conductor	~ Rise Time	Peak Voltage	Peak Current
Long unshielded wires (power lines, large antennas)	10 ns – 100 ns	100 kV – 5 MV	1 kA – 10 kA
Unshielded telephone line at wall plug	10 ns – 1 μs	100 V – 10 kV	1 A – 100 A
Unshielded AC power line at wall plug	100 ns – 10 μs	1 kV – 50 kV	10 A – 100 A
HF antennas	10 ns – 100 ns	10 kV – 1 MV	500 A – 10 kA
VHF antennas	1 ns – 10 ns	1 kV – 100 kV	100 A – 1 kA
UHF antennas	1 ns – 10 ns	100 V – 10 kV	10 A – 100 A
Shielded cable	1 μs – 100 μs	1 V – 100 V	0.1 A – 50 A

The best way to reduce this overshoot for EMP type pulses is to use an SPD followed by a low pass filter (for power lines). An alternative approach is to take the typical 120 V power supply voltage, multiply it times 2 for an operating safety margin (use a 240 V clamping voltage), and then accept another factor of 3 for the EMP overshoot. The good news is that the 720 V peak computed would still be lower than the normal EMC EFT immunity test level (1 kV) for commercial equipment for the power cable attached to the equipment. Experience indicates that MOVs are the best choice for power lines but care must be taken to ensure that the MOV does not overheat if the EMP pulse keeps it in a short-circuit firing mode, permitting the power line current to heat up the MOV. The newest UL standards identify characteristics of the MOV packaging to make them “fire-safe.”

The situation for data lines could be similar by taking the normal operating voltage level of a data line, apply a safety margin and then multiply by 3 for the EMP overshoot, which in most cases will

still be below 500 V (the normal EFT test level for commercial equipment data lines). While MOVs are a good choice for power, for data lines their capacitance may create problems for a high frequency data rate. In this case a TVS is likely a better choice. Note that the TVS will not provide protection from lightning surges.

EMP rated SPDs are available from several manufacturers. See the [Level 2 EMP Guidelines](#) section and [Appendix B, EMP Protection Level 2](#) for more information. Where possible, it is recommended to use SPDs that have their HEMP or NEMP testing results available for review.

For antenna lines, the SPD voltage level must be set well above the transmitter peak voltage level, including the modulation levels and the higher voltage levels created from standing waves due to impedance mismatches (voltage standing wave ratio (VSWR)). To decrease the risk from an EMP event or a lightning strike partially given this SPD peak voltage limitation, the following RF related EMP risk mitigation procedures should be implemented:

Level 1

- **Grounding** – Should comply with “*R56 Standards and Guidelines for Communication Sites*”¹¹ or other recognized grounding standard. The book “*Grounding and Bonding for the Radio Amateur*” available through the National Association for Amateur Radio (ARRL) is also helpful¹².
- **Antenna line** – Use a shielded/braided, double shielded/braided cable, or equivalent. Ground the shield per R56.
- **RF SPD** (or RF Transmission SPD, sometimes also called an antenna SPD) – Connect an RF SPD to the antenna line at the building egress (within 2 ft.). If electronics are at the antenna, also connect an SPD near the antenna prior to the electronics.
 - For HF antennas, it is recommended that an easily replaceable GDT be used (these are also inexpensive).
 - The RF SPD should be replaced per the manufacturer’s recommendations or when there is a known extreme surge (nearby lightning strike or EMP event).
 - The RF SPD should have a ground wire run to it, which will also ground the antenna shield.
- **Antenna mount** – Ground the antenna mount.
- **Robust Transmitter** – Select a transmitter that can tolerate high levels of voltage transients.

Level 2

- **Ferrites** – A ferrite choke should be used prior to the RF SPDs to help dampen and slow the EMP.
- **Secondary RF SPD** – If the antenna line is run straight for more than a few meters inside a facility with poor EMP shielding (e.g., it’s made out of wood), the line should be connected to a secondary RF SPD near its termination point.

Level 3

- **Metal Conduit** – The external portion of the shielded antenna line should be run through a grounded metal conduit to the extent possible.

Level 4

- **EMP Transceiver Testing** – The transceiver should be tested to ensure that it can tolerate higher levels of EMP transients that bypass the selected voltage level of an SPD.
- **SPD Redundancy** – Double surge protect critical external lines entering EMP protected areas assuming that the failed surge protector is designed to continue to allow voltage to pass through upon failure. As an example of why this is necessary can be shown if there is a double EMP event. The first burst could take out the first SPD, which leaves the equipment vulnerable if there is a second EMP burst or a nearby lightning strike. SPD redundancy can occur by connecting a primary SPD to a cable at the building egress and then connecting a secondary SPD to that cable immediately prior to it entering the EMP area.

As an SPD typically degrades over time, it should provide an audio or visual status warning when it is no longer able to effectively protect equipment. Otherwise, a subsequent lightning strike or EMP pulse could destroy the equipment. If the SPD does not alert the operator, then the SPD should be replaced as frequently as every year or two depending upon the location and the number of nearby lightning strikes, which will generally cost more money than using an SPD with alerts. Note that even if a cable is well shielded, an SPD is used both because the shielding won't be perfect and an EMP or lightning pulse could arc over an air gap to cause damage.

2.4. Use of Common Building Materials to Increase EMP Shielding

As discussed above, SPDs reduce EMP surges that travel via cables. These cables are most vulnerable when part of the cable is above ground and external to a building (i.e., it is not covered). Within buildings, the amount of protection required for cables is heavily dependent upon the building material between the cable and the EMP E1 burst as shown in the figure below.

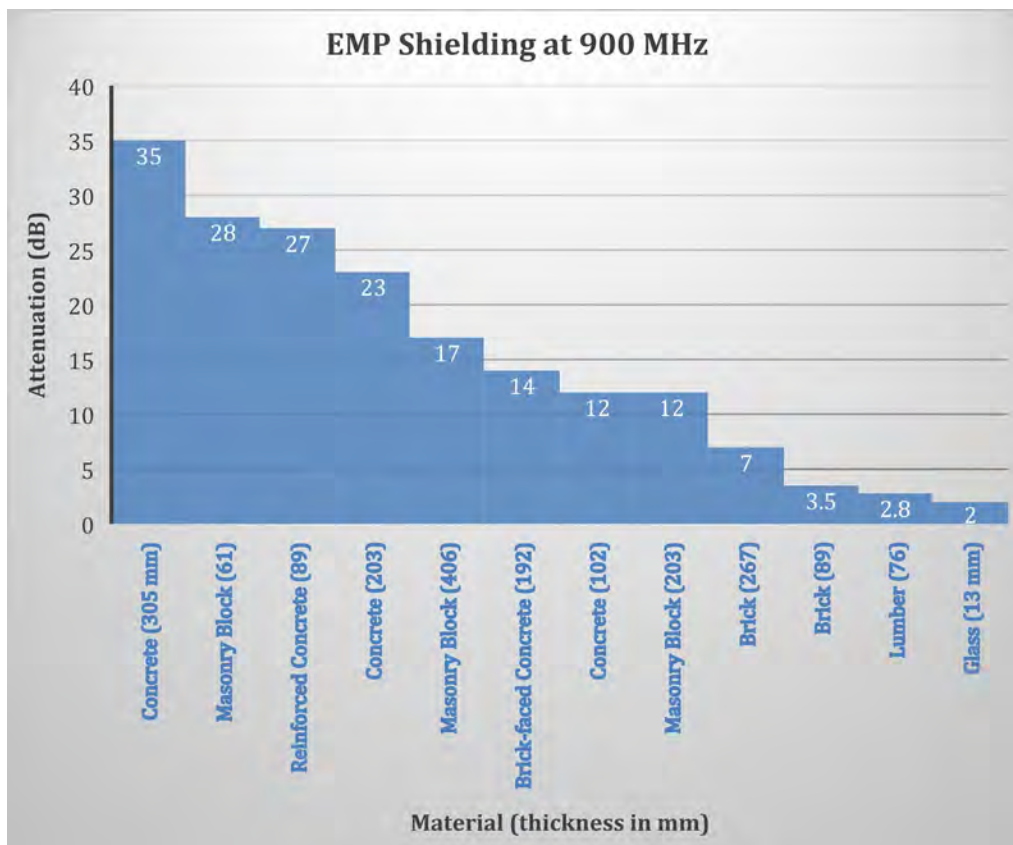


Figure 21. Effect of Building Materials on EMP Attenuation¹³

The attenuation in the above figure is only at 900 MHz, but materials such as reinforced concrete also attenuate signals at lower E1 frequencies as well. In addition to the above, natural barriers such as dirt and rocks can significantly help reduce E1 pulses. Thus, burying a cable a few feet underground can substantially reduce the EMP pulse that hits the cable although the amount is very dependent upon the ground type (moist topsoil is much better than dry sand) and the length of the run.

There are also manmade materials that can be used to significantly attenuate the RF signal, such as EMP paint and other conductive coatings that are inexpensive. These generally don't work equally across all frequencies of concern, but they can still significantly attenuate EMP bursts. Simple tests can be run to determine how much they will help or the manufacturer can be contacted to provide these specifications.

Building Shielding

To get to the internal cabling, the HEMP must get through the building – the walls and roof. Generally some amount of “shielding” (attenuation of the EM transient) is provided by the building. The amount of attenuation varies with several factors, and building material type is an important one. (Windows do not provide much EM attenuation, and can ruin the shielding provided by the wall materials.) As a simplification, we might use categorized building types, such as listed in the table below. The factor “dB” translates to a reduction in the HEMP by the logarithmic value $10^{-dB/20}$

(every increase by 20 dB means a factor of 10 smaller in field amplitude; see Appendix E, page E-4 for more information).

The table below provides some additional general engineering “rules of thumb” that can be used when estimating how much inherent E1 EMP protection results from a facility’s design.

Table 9. Building shielding “rules of thumb” for E1 HEMP

Building Shielding		
dB	Type	Example
0	Transparent	Wood
5	Poor	Masonry
10	Moderate	Concrete, no windows
20	Good	Metal siding, no windows
30	Very Good	All metal, no windows

3. LEVEL 1 EMP GUIDELINES

Level 1: Lowest cost; longer mission outages permitted

- Unplug power, data, and antenna lines from spare equipment, where feasible.
- Turn off equipment that cannot be unplugged and is not actively being used.
- Use at least a lightning rated surge protection device (SPD) on power cords, antenna lines, and data cables; maintain spare SPDs.
- Have either EMP protected backup power or a generation source that is not connected to the grid with one (1) week of on-site fuel or equivalent (e.g., renewable source).
- Wrap spare electronics with aluminum foil or put in Faraday containers.
- Use priority phone services like [Government Emergency Telecommunications Service \(GETS\)](#), [Wireless Priority Service \(WPS\)](#) (for cell phones), and [Telecommunications Service Priority \(TSP\)](#) programs to improve your chances of phone call completions and rapid restorations during EMP crises; and join the [SHared RESources \(SHARES\)](#) program if applicable (see [Appendix C](#) for more information on all of these programs).
- Consider land mobile radios with standalone capabilities, High Frequency (HF) radios, and FirstNet.
- Store one week of food, water, and other supplies for personnel.
- Use battery operated AM/FM/NOAA radios to receive alerts from the Emergency Alert System (EAS) and other networks like the NOAA Weather Radio All Hazards networks.

1. Turn off and unplug equipment.

The easiest and quickest way to reduce equipment vulnerabilities to EMP is to turn off non-essential equipment and then unplug this equipment from all metallic lines, such as power cords, telephone lines, Ethernet cables, and antennas/coaxial cables. Battery packs should be removed from small electronics as these batteries can work in conjunction with EMP to provide damaging energy into equipment circuits. Where possible, the cords themselves should also be disconnected from the equipment, not just unplugged at the wall or other distant connection point. The rationale here is that these power cords and data cables will still act as antennas for picking up EMP signals even if they are disconnected from a wall outlet or router or external radio or TV antenna. As an extra precaution, you should also disconnect your non-essential computer(s) from any wired external keyboard or mouse. You should unplug all cords and cables at the point where they actually connect to the equipment, such as at the back of a computer or desktop phone or equipment rack. If you cannot unplug the equipment from a long metallic cable, then coil the cable near the equipment, if possible, so as to minimize its effective length and hence reduce its ability to pick up EMP energy. For wireless devices such as cell phones and other battery operated devices (like portable radios and walkie-talkies), you should turn them off and unplug them from any charging station or adapter. If items need to be charged, be sure to use power cord surge protectors that have a 10 ns or better response time (which can be found at popular retail stores).

2. Use a power surge protector device (SPD) that provides fire protection.

Use at least a “low fire risk” lightning SPD for all electronics with cables connected. Many surge protectors use metal oxide varistors (MOVs) that can be a fire risk when they fail. Some manufacturers provide fire-proof MOVs. If the power SPD is not fire-proof, it should be placed in an area free of combustibles.

A spare SPD should be kept on hand in case one needs to be replaced. A spare transceiver fuse should also be kept on hand in case the fuse is blown due to excessive power that might be caused by a nearby lightning strike or an EMP event.

3. Use heavy-duty aluminum foil or inexpensive Faraday bags/cases.

For small electronics that are spares or backups, you can put these in a plastic or paper bag or other insulating material and then wrap the item with an outer layer of heavy-duty aluminum foil. If power or data cables are permanently connected to the equipment, you should also place these inside the bag before wrapping the item with aluminum foil. You should ensure the aluminum foil completely covers the item and that all seams overlap. If possible, protect the equipment with two or more complete layers of aluminum foil. If you decide to use a Faraday bag, be sure that it is not just a standard Mylar food bag which provides little protection. Metal trash cans do not usually provide reliable EMP protection for items placed inside of them, unless they have been modified to block radio waves from entering through the gaps in the lid, handles, and sometimes at the base. Microwave ovens can serve as expedient Faraday cages for small electronics, but should be tested with a cell phone and/or AM/FM radio to see if there is reception inside of the oven (obviously, these “ovens” should never be turned “on” with equipment inside). In general, small handheld electronics are relatively immune to EMP effects, unless they have long antennas or power cords attached, and so the need for Faraday cages is of secondary importance.

4. Ensure your backup generation system is not directly connected to commercial power (unless it has very good EMP surge protection on the connecting line).

While many companies will recommend connecting your backup diesel or other generator to commercial power in order to provide an automated transfer to backup power when commercial power is lost, you should avoid this unless excellent EMP surge protection is provided. The relatively long commercial power line leading to your facility or organization provide an excellent path for EMP energy and may destroy your backup generator’s electronics if they are wired into an automated transfer switch.

Using a natural gas power generator also reduces risk since the natural gas itself will not act as an antenna. Likewise, natural gas pipeline providers should use natural gas powered compressor stations instead of electrically powered compressor stations. Other potential energy sources are discussed in an upcoming DHS Power Resiliency Guidelines document.

5. Use battery operated AM/FM/NOAA radios to receive alerts

Battery operated radios are relatively resilient to EMP. The national level Emergency Alert System (EAS) has many radio stations across the USA with some protection against EMP. Hence, listening to handheld (or car) radios may be the principle means of receiving information from the government on what is happening in your area and on what actions are recommended.

4. LEVEL 2 EMP GUIDELINES

Level 2: Only hours of mission outages are permitted

In addition to Level 1 ...

- Use EMP-rated SPDs on power cords, antenna lines, and data cables to protect critical equipment.
- Use on-line/double-conversion uninterruptible power supplies (UPS) or a high quality line interactive UPS.
- Use fiber optic cables (with no metal); otherwise use shielded cables and ferrites and/or SPDs. Note: shielded racks, rooms or facilities may be more cost-effective than hardening numerous cables.
- Use EMP protected backup power that is not vulnerable to EMP coupled through the power grid.
- Implement EMP protected, high frequency (HF) voice and email for long-distance communications (if required).
- Consider geosynchronous equatorial orbit (GEO) satellite communications, like Broadband Global Area Network (BGAN). Avoid low-earth orbit (LEO) satellite supported services, unless EMP protected. Use terminals that are EMP resilient.
- Consider shortwave radios for additional situational awareness.

1. Use of EMP-rated surge arresters on power cords and phone/data cables

Many commercially available power strips have surge protection built in. These should be used to protect all essential equipment although the SPDs in the power strips also provide some protection against fast rising transients. Many commonly available power strips use fire-protected MOVs (UL 1449 3rd Edition) and if spaced and grounded at distances of every 20 feet or so, can help mitigate MOV and spark-induced fires from EMP as well as protect against lightning. See “*Surge Protective Device (SPD) Selection*” under Section 2 for more information concerning the characteristics of SPDs adequate for EMP protection.

2. Use of ferrites

Cable ferrites are often used to attenuate unwanted high-frequency cable signals. Ferrites use materials that interact with the magnetic field of the cable signal. Type 61 material ferrites are recommended in that they can attenuate pulses with faster rise times than those made with older ferrite materials, such as Type 43 ferrites. These are simple and inexpensive – they simply snap around the cable (preferably near the vulnerable equipment end).

Ferrites effectively introduce a complex impedance onto the cable. There is signal attenuation because:

- Impedance mismatch relative to the normal cable impedance means some signal is reflected back down the cable,
- And the imaginary part of the impedance means that energy is absorbed.

The impedance is frequency dependent, with a typical peak of hundreds of ohms. This impedance affects only common mode cable signals, such as HEMP. It does not impact differential mode, which are the normal cable signals. The protection is additive with each extra bead snapped on. There is approximately 1 to 2 dB protection per ferrite, so their use with multiple beads is usually good for obtaining ~10 dB of attenuation.

3. HF and other radio equipment protection

HF and other radios need three types of protective devices – (1) those for HF or other radio antenna connections, (2) those for power connections and (3) those for low voltage DC connections such as antenna rotators. Protective devices must be well grounded using low-inductance grounding cables that are as short as possible.

4. Coaxial Cable RF (Antenna) Surge Protectors

Nothing can protect equipment from a direct lightning strike. Antenna surge protectors are designed to reduce antenna-induced voltages resulting from nearby lightning voltage discharges. A HEMP's coupled current rise time is between 5 and 10 ns while IEMI currents will have a rise time on the order of 1 ns. An HF antenna and feedline will slow these rise times down to longer than 10 ns. Most antenna surge protectors contain gas discharge tube (GDT) devices.

Antenna surge protectors should be installed at both ends of the antenna feedline with one near the radio equipment (within 2 meters) and one by the building egress unless the feed line is extremely short. Each surge protector should be grounded directly through a separate low inductance wire or cable (not just through the coaxial cable outer conductor) because an ungrounded protector provides only limited differential mode protection. The feedline should be run as close to metallic surfaces (if available) as possible.

Each protector is installed in series with the antenna feedline. The GDT inside the protector is connected from the center conductor to the shield so that the GDT element is in parallel with the feedline. A GDT is a voltage-sensing device that is typically open (does not conduct). When the voltage is sufficiently high, the gas inside the GDT ionizes and conducts which reduces the voltage on the center pin with respect to the outer shield. If the peak surge is large enough, an arc inside the GDT develops further reducing the voltage. The GDT returns to an open state after the power being shunted through it decreases to a low level.

GDTs wear out with each surge event and usually fail by becoming either permanently open or shorted. It is easy to detect when a GDT shorts because the transmitter will shut down from high Voltage Standing Wave Ratio (VSWR), but not when it opens. What happens when a GDT opens is the gas inside will not ionize anymore, but there is no easy way to predict when that will occur: RF signals will pass through the GDT just as usual but the GDT won't conduct, so it no longer provides any protection.

Antenna surge protectors that are easy to remove and replace without opening their housings are recommended because GDTs wear out and need to be replaced regularly to ensure continued protection. A replaceable GDT typically fits into or beneath a small cap that screws into the protector housing. Unscrewing an old GDT from its existing installed housing and replacing it with a

new GDT is easier and more convenient than replacing the entire housing. It is less expensive to replace a few dollar GDT instead of the complete protector.

GDTs used in surge protectors wear out depending on how many times they have been triggered. Worn out GDTs provide little or no protection. Since it is dangerous to test GDTs to determine their characteristics, and because GDTs cost so little, it is a good idea to replace GDTs every few years or after major thunderstorms when there have been close proximity lightning strikes. Another advantage of using protectors with replaceable GDTs is that different GDTs are available with different voltage ratings to customize the protection level depending on the VSWR and power level. GDTs are triggered not only by voltage induced from an EMP or a nearby lightning strike, but also by the VSWR resulting from reflected transmitter power.

Surge protectors with replaceable GDTs can be easily converted for other power output levels by replacing their GDTs. But the VSWR should first be measured to determine where it is highest (worst) throughout your operating frequencies. The worst VSWR must be known to calculate the highest voltage level so that the voltage rating can be specified for the replacement GDT. Lower voltage rating GDTs provide better protection as long as their voltage ratings are high enough so that the GDTs will not fire under normal operating conditions. Much lower GDT voltage ratings could be used if only low transmit powers are used into a perfectly impedance matched antenna).

GDTs respond to voltage levels, which are functions of both power and VSWR, and the VSWR changes as a function of frequency. Therefore, a much larger selection of GDT voltage ratings is required to match different power levels and VSWRs. Fortunately, there are several companies making GDTs at a variety of different voltages. Several brands of low-cost GDTs (less than \$3) are available. Although many manufacturers list power levels for their surge protectors, the voltage ratings of their GDTs are much more meaningful.

Antenna surge protectors are available from Alpha-Delta, PolyPhaser, Huber+Suhner, Fischer Custom Communications, Amphenol® EMI/EMP Protection Connectors, and ETS-Lindgren. Bourns manufactures GDT elements for other companies to repackage into protective devices. The following URLs provide more information about using protective devices.

Gas Discharge Tubes (GDT)

[http://www.bourns.com/resources/training/circuit-protection/gas-discharge-tubes-\(gdt\)/gas-discharge-tubes-\(gdt\)](http://www.bourns.com/resources/training/circuit-protection/gas-discharge-tubes-(gdt)/gas-discharge-tubes-(gdt))

Telecommunications Application Schematics

<http://www.bourns.com/applications/telecommunications>

Network Communications PortNote® Solutions

<http://www.bourns.com/applications/network-communications>

5. Uninterruptible power supply (UPS) considerations

120 VAC protection from various power systems is best accomplished with a UPS since modern switched-mode power supplies (SMPS) contain microelectronics potentially sensitive to fluctuations. Note that the UPS itself will need protection from AC power feed transients, as the

UPS may be vulnerable to low frequency EMP (E3) or geomagnetic disturbance (GMD) caused power service transformer harmonics. UPSes made by APC, CyberPower and Tripp are available in suitable power ratings throughout the range from 200 W to 1200 W. It is not clear without testing whether protection is needed for the antenna rotator circuit, as the excitation will be common mode while the operation is differential mode, but if testing proves it necessary, the installation of MOVs appropriate for the operating level of the specific rotator should suffice.

When selecting a UPS for protecting equipment from EMP, a true on-line, double-conversion type of UPS is recommended although a high quality line interactive UPS with good surge suppression and noise filtering can be used unless the equipment is extremely sensitive. Less expensive UPS units provide insufficient protection in that they allow voltage spikes to reach equipment before the battery is switched into the circuit, which can take as long as 25 milliseconds (ms). The more expensive on-line, double-conversion UPS ensures that the battery is always connected so that no power transfer switches are needed and voltage spikes will not damage the equipment. A high quality line interactive unit will take 2-4 ms to transfer power to the battery source, which easily meets the specifications for all common modern equipment.

6. Cable layouts, entry, and the use of shielded cables

Cable layout techniques to reduce the coupling of EMP signals at the equipment include:

- Run location: Run the cable along metal structures, such as metal walls or I-beams.
- Cable bundles: Put multiple cables into tight bundles – on average all the cables are helping to short out the E field seen by any individual cable. If one cannot run along metallic structures, periodically ground the bundle to the internal grounding system with low inductance grounding braids or plates.
- Metal cable tray: If cable trays are used to hold the cables, be sure the tray is metal instead of plastic or fiberglass; and ground it often along the run.
- Metal cable conduit: It is even better to have the cables in enclosed metal conduits, which are well grounded at least on the ends, and at other points if possible. The best end connection is a circumferential ground bond onto a metal building wall.

Cable entry into a facility best practices include:

- Use underground cable runs, at least for the part nearest the building (underground cables have reduced HEMP, SREMP (radiated fields) and EM weapon field coupling, and higher attenuation of signals that are flowing toward the building).
- Short out the external conductor at the entry point to the building – it is especially good to use shielded cables, with the shield circumferentially bonded to a metal external wall.
- If the building has an ANSI/TIA/EIA-607 Telecommunications Bonding Backbone (TBB) installed, entry cable shielding should be bonded to the TBB.
- Metal pipes also count as conductors – they should be shorted at the metal wall or the current on them will flow inside and radiate fields, which can be picked up by other wiring.
- Terminal Protection Devices (TPD) may be needed on power and signal wires.

- Antennas need special attention, and possibly special surge protectors as discussed above under *“Coaxial Cable RF (Antenna) Surge Protectors.”*

Considerations with shielded cables include:

- Using shielded cables is very common in EMP protection, and it is easy to procure shielded network cables.
- The protection provided depends on the quality of the shield, but also on the handling of the cable ends. While circumferentially bonded connectors are the best, for some levels of EMP protection, shield clamping to the external wall of a building can provide 20-40 dB of shield current attenuation.
- Common shielded network cabling has simple foil shields. Better and generally more expensive cables use high-coverage braided shields. Although cable vendors often identify cables with shields, it is important to obtain shielding effectiveness data for the range of frequencies ranging from 1 MHz up to 1 GHz.
- The cable plugs must have metal sheaves, firmly grounded to the cable shields.
- The matching cable jack must also be configured to accept the shielded plug – typically with metal tabs. These tabs are not equivalent to circumferential shields, but provide some protection.
- Typical network equipment do not always have shield-ready jacks, so in these cases shielded network cables will not be of value.